Hao Dinh  
22 August 2016, Delft

Training Senior-Managers for Cyber Crisis  
Designing a Simulation Game for Decision-making under Uncertainty
Training Senior-Managers for Cyber Crisis
Designing a Simulation Game for Decision-making under Uncertainty

**Author**

<table>
<thead>
<tr>
<th>Name</th>
<th>Hao Dinh</th>
</tr>
</thead>
<tbody>
<tr>
<td>Student number</td>
<td>1516752</td>
</tr>
<tr>
<td>Email</td>
<td><a href="mailto:c.h.dinh@student.tudelft.nl">c.h.dinh@student.tudelft.nl</a> / <a href="mailto:h.c.dinh1@gmail.com">h.c.dinh1@gmail.com</a></td>
</tr>
<tr>
<td>Faculty</td>
<td>Technology, Policy &amp; Management, Delft University of Technology</td>
</tr>
</tbody>
</table>

**Graduation Committee**

<table>
<thead>
<tr>
<th>Chairman</th>
<th>Prof. dr. ir. A. Verbraeck</th>
</tr>
</thead>
<tbody>
<tr>
<td>First Supervisor</td>
<td>Dr.rer.soc. H.K. Lukosch</td>
</tr>
<tr>
<td>Second Supervisor</td>
<td>Dr. ir. Wolter Pieters</td>
</tr>
<tr>
<td>Third Supervisor</td>
<td>R. Djwalapersad Msc. LLM.</td>
</tr>
</tbody>
</table>

**Final Version**

<table>
<thead>
<tr>
<th>Date</th>
<th>August 22nd, 2016</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Keywords</strong></td>
<td>Cyber crisis, Simulation Game, Decision-making, Uncertainty, Situational Awareness</td>
</tr>
</tbody>
</table>
Executive Summary

In the last couple of years, data breaches and other information security incidents seem to be recurring headliners of major newspapers. These situations involving information systems can be called “cyber crises”, and have internal as well as external consequences that need to be dealt with by the senior-managers within these organizations.

Crisis management planning sets in place predetermined plans and/or resource to restore the system back to normalcy after an unexpected event, interruption or incident. These planning and preparation steps make it possible to handle a crisis situation efficiently. However, they often lack flexibility to address these crises effectively. It is believed that insufficiency of the crisis management plan comes from the contradiction of terms. How can we prepare for a phenomenon that is complex in itself? This makes it a big challenge for crisis managers to handle, let alone prepare for them. But given the rare nature of such events, how can practitioners then prepare for cyber crises? Simulation games can offer a solution to this problem. Specifically, simulation games can be used to invite participants to an imaginary world and experience unknown situations without the negative consequences.

A review on the crisis and cyber simulation literature provides three gaps: 1) practical cyber security game design is poorly explained, conceptualized or justified, 2) Existing cybersecurity simulation games focus on preventive training and awareness, not on crisis response, and 3) the target group for cyber simulation games are mostly teenagers and children and not senior-management level. Taking these gaps into consideration, there is a need for a well-documented simulation game design specifically preparing senior-managers for cyber crisis, which creates awareness. Therefore, the goal of this research is defined as: To design a simulation game focused on preparing senior-managers for cyber crisis, which offers participants a safe environment to practice decision making and creates awareness. Specifically, the game focuses on two main aspects: 1) the simulation game creates awareness for the concepts and consequences of cyber crisis decision making and 2) offers a realistic simulated environment for participants to practice decision making under crisis characteristics like time-pressure and uncertainty.

Given the above perspective, this research focuses on answering the main research question: How to support senior-managers in preparing for cyber crisis decision-making by means of crisis simulation games? The design research approach combines methods and models from both Knowledge Base and Application Domain, to inform the simulation game design and ensures both scientific rigor as well as practical relevance during the simulation game design. The main theories used in building the simulation game are: Situation Awareness, Recognition Primed Decisions and Source of uncertainty. Additionally, numerous inputs are derived from the cybersecurity theory, interviews with experts as well as a case of cyber crisis to build that realistic simulated environment for participants.

The design of the simulation game can be summarized as: A crisis team needs to steer their organization out of the crisis situation and take crucial decisions. The game revolves around a fictitious company in which cyber crisis occurred. The game takes five decision makers through the process of crisis and crisis management. Uncertainty is very high, with information coming from everywhere. The game leans heavily on interaction between participants and the 'outside world', creating chaos and inducing the feelings involved in crisis situations. These characteristics mimic models from concept as well as from reality.

From interviews with both crisis management experts as well as cybersecurity experts, it can be concluded that crisis definitions do not differ that much from the general crisis model. Importantly, the experts note that cyber is merely the domain in which crisis takes place or originates from. Subsequently, a simulation game specifically designed for cyber crisis decision making, might in essence not be that different from a “regular” crisis simulation game, except for the simulated environment and processes which the game represents.
After testing the prototype, there is one key design variable that was most important during the design: *realism versus control*. The realism is created by a combination of many elements in the game and is praised by participants. Key elements are the *information system, role descriptions, coins* and *pressure from outside*. Included in the realism are the *complexity, interactivity and flexibility* that the configuration of the game elements bring. However, this choice leads to a *loss of control*. Especially over what participants actually learn. In other words, even though there is learning involved, there are no insights in which aspects are actually learned. Therefore, only an assumption exists that when participants note they have learned something, the game has served its goal.

In conclusion, the presumption used in this thesis is that cyber crises have characteristics that challenge the translation into a crisis management simulation game. However, as earlier described, according to experts, cyber crisis is not different from regular crisis except for the environment in takes place in or originates from. In this case, it is cyberspace. This of course does not mean that cyber crises do not have their own characterizing aspects to take into consideration, but after the initial trigger event takes place, regular crisis management activities are conducted by organizations. When supporting senior-managers in preparing for cyber crisis decision making by means of crisis simulation games, the simulation game design requires 1) components of crisis decision-making under uncertainty like situation awareness and recognized primed decisions, 2) learning components like the Kolb cycles, debriefing and the use of narratives and 3) scenarios, events and tasks that are geared towards cyber crises. However, the complexity of designing the proposed simulation game lies creating a realistic as possible environment, without losing control over the game. It is the combination of the game elements, that pull participants into the world of cyber crisis and its chaos.

The evaluation of the test sessions yielded a couple of findings which offer possible insights for future designs when supporting senior-managers for cyber crisis by means of a simulation game that display its complexity:

**Participants enjoy a challenging game.** All ten participants marked the simulation game as enjoyable. On the other hand, they marked their performance as low as well as challenge to be high. Challenging aspects of the game were: *new experience containing many aspects, tough due to the interactivity, a lot of changes within the game and managing people.*

**Interactivity is crucial in a complex decision-making game.** The interactivity; including the phone calls, messages, pressure from outside and the group decision making; disrupts the decision-making at hand. It also adds to a dependency among participants and adds chaos to the situation. This interactivity mimics 1) situation awareness, enabled by the information system, 2) team situation awareness, by adding secrecy as well as personal phone calls to the game and 3) sources of information, for which different stakeholders, systems are simulated like the newspapers, external parties, hackers etc.

**Elements that challenge group dynamics disrupt decision-making during play.** The combination of elements that have been added to challenge group dynamics have proven very effective. These elements include the role descriptions, coins, action list, leaked information, information system and events. These elements have the potential to disrupt the status quo and possibly change the state of the environment.

**Measuring awareness for cyber crisis concepts requires more than a self-evaluation.** One of the goals of this simulation game is to raise awareness for the cyber crisis decision making concepts. Important to know is that it is not logged nor discussed which of the concepts or aspects are learned by the participants, merely if they perceive it to have happened or not. With the taken approach it is not possible to track the concepts that have been learned by the participants.

**Incorporating flexibility increases realism, but has a price.** Incorporating flexibility in the simulation game proves to be very helpful. By doing this, the responses are in line with what the participants expect.
This increased realism has a price, the game is very facilitator intensive, and requires extensive briefing of these facilitators.

By taking a design approach that builds a simulation game model that consists of multiple smaller models, the simulation game is completely geared towards the problem at hand. This modular approach gives game designers the opportunity to mix-and-match parts that are less relevant for their research and replace them with components that are suitable for their purpose. The research community can use, adjust and complement the existing game as well. Its use includes testing hypotheses or theories as well as observing team dynamics, decision making and communication efforts, without duplicating the design process.

As a result of playing the game, participants are more aware of the concepts and consequences of their decision-making within the cyber crisis domain. Ideally, senior-managers are better prepared for cyber crises by practicing decision making in this specific domain and therefore are well-equipped to keep consequences to a minimum.
Contents

Executive Summary ................................................................. 2
List of Figures and Tables .......................................................... 7

1. Introduction .............................................................................. 8
   1.1 Background and Motivation ....................................................... 8
   1.2 Research questions, Research objective and Contributions .............. 9
   1.3 Research Methodology .............................................................. 11
   1.4 Research Strategy ................................................................. 13
   1.5 Structure of the Thesis ............................................................. 14

PART I: Knowledge Base .............................................................. 17

2. The need for training: cyber crisis simulation games ...................... 17
   2.1 Dealing with crisis: crisis management and its phases ..................... 17
   2.2 Preparation: Crisis Management Planning and its limitations ............ 18
   2.3 Preparing senior-managers for crises ......................................... 19
   2.4 Cybersecurity simulation games ............................................... 20
   2.5 Conclusion: the need for a Cyber Crisis simulation game .................. 23

3. Theoretical Framework: Simulation Games, Situational Awareness and Decision-making under uncertainty ........................................... 25
   3.1 Simulation Games .................................................................... 25
   3.2 Simulated Models from Theory .................................................. 34
   3.3 Conclusion: theoretical concepts and their influence on design ........ 47

PART II: Application Domain ......................................................... 52

4. Concepts and models from the Cyber and Crisis domain .................. 53
   4.1 The Crisis Model ................................................................. 53
   4.2 Characterizing Cybersecurity for a simulation game ....................... 56
   4.3 Lessons Learned from a Cyber Crisis in light of the Media ............... 68
   4.4 Conclusion: Concepts and Models from the Cybersecurity and Crisis domain ................................................................. 76

5. The Practitioners view on Cyber Crisis ........................................ 77
   5.1 Method ............................................................................... 77
   5.2 Cyber Crisis According to Experts .............................................. 78
   5.3 Decision-making and SA questions during a Cyber Crisis ................ 80
   5.4 Stakeholders derived from interviews ......................................... 82
   5.5 Processes and Mechanisms during Crisis Management .................... 85
   5.6 Emotions during Crisis .......................................................... 88
   5.7 Integral Schema .................................................................... 88
   5.8 Conclusion: The Practitioners view on dealing with Cyber Crisis ........ 90

6. Requirements for a Cyber Crisis Simulation Game .......................... 94
List of Figures and Tables

FIGURE 2: STEPS OF THE CYBER CRISIS SIMULATION GAME DESIGN RESEARCH ................................................................. 14
FIGURE 3: THESIS OUTLINE, INSPIRED BY HEVNER (2007) ................................................................................................. 16
FIGURE 4: SIMULATION GAME AS MODEL CONSTRUCTION (p. 43) ................................................................. 26
FIGURE 5: LEARNING FROM A SIMULATION. ADAPTED FROM (THATCHER, 1990, p. 269) ................................................................. 29
FIGURE 6: GENERAL OUTLINE OF THE SIMULATION GAME ................................................................................................. 34
FIGURE 7: MODEL OF SITUATION AWARENESS IN DYNAMIC DECISION-MAKING. ADAPTED FROM (ENDSLEY, 1995, p. 36) ................................................................. 37
FIGURE 8: TEAM SITUATION AWARENESS (ADOPTED FROM (ENDSLEY, 1989)) ................................................................. 39
FIGURE 9: SOURCES OF SA INFORMATION (ADOPTED FROM (ENDSLEY AND ROBBERTSON, 2000)) ................................................................. 40
FIGURE 10: SIMULATED MODELS FROM THEORY ................................................................................................. 47
FIGURE 11: CRISIS MODEL, COMBINING BOTH VIEWS ON CRISIS ................................................................................................. 56
FIGURE 12: THE RELATIONSHIP BETWEEN IT-, INFORMATION- AND CYBER SECURITY (VON SOLMS & VAN NIEKERK 2013, p.101) ................................................................. 59
FIGURE 13: THREAT MODEL ................................................................................................................................. 62
FIGURE 14: MESSAGE SONY RECEIVED FROM GOP ................................................................................................................................. 70
FIGURE 15: SONY CORP. STOCK PRICES GENERATED FROM YAHOO FINANCE ................................................................................................................................. 74
FIGURE 16: STAKEHOLDER MAP DURING CYBER CRISIS ................................................................................................. 85
FIGURE 17: PHASE I: DISCOVERY & FIRST RESPONSE ................................................................................................. 89
FIGURE 18: PHASE II: MANAGING THE MEDIA ................................................................................................................................. 90
FIGURE 19: GAME FORMAT ................................................................................................................................................................. 105
FIGURE 20: TIMELINES WITH EVENTS (EXAMPLE) ................................................................................................................................. 112
FIGURE 21: DECISION TREE CRISIS TEAM ................................................................................................................................................................. 116
FIGURE 22: ROOM SETUP DURING PLAY ................................................................................................................................................................. 119
FIGURE 23: INFORMATION SYSTEM VIEWS ................................................................................................................................................................. 138
FIGURE 24: THREE CYCLE VIEW OF DESIGN SCIENCE RESEARCH (HEVNER, 2007) ................................................................................................................................................................. 162
FIGURE 25: ADR METHOD: STAGES AND PRINCIPLES (SEIN ET AL., 2011) ................................................................................................................................................................. 163

TABLE 1: OBSERVATIONS VALIDATED WITH THREE LITERATURE REVIEWS ................................................................................................................................................................. 22
TABLE 2: REFERENCE FOR THE THEORETICAL CONCEPTS ................................................................................................................................................................. 48
TABLE 3: CYBERSECURITY CONCEPTS ................................................................................................................................................................. 67
TABLE 4: EXPERT PERCEPTION CONSIDERATIONS ................................................................................................................................................................. 91
TABLE 5: REQUIREMENTS FOR THE SIMULATION GAME ................................................................................................................................................................. 99
TABLE 6: COMPARISON OF TWO DESIGN-RESEARCH APPROACHES ................................................................................................................................................................. 165
1. Introduction

1.1 Background and Motivation

With the increase of dependency on information from our applications and services, many information systems have been linked together forming complex networks. In the last decade, data breaches and other information security incidents seem to be recurring headliners of major newspapers (Campbell et al., 2003).

One example is the hack on US bank JPMorgan, in which 83 million accounts were leaked. Reuters (2014) reported that names, addresses, phone numbers and email addresses of account holders were breached. This incident also harmed JPMorgan in their reputation and trust from customers. The New York Times reported that a list of the applications and programs that run on JPMorgan’s computers were acquired (Silver-Greenberg, Goldstein & Perrot, 2014). Uncertainty is raised during such events, both internally and externally. This includes uncertainty about the contents of the leaked data, if important stakeholders are affected, if hackers remain on the systems, and especially about what these adversaries are capable of doing.

A second example is one of the biggest data breaches in history: The Target breach. Target is the second largest convenience store in the United States. During this breach 40 million credit and debit cards were skimmed at the stores during busy seasons, together with about 70 million names, e-mail addresses and phone numbers (Welch, 2015). Target’s CEO Gregg Steinhafel resigned several months after the breach. This shows the impact that an information breach can have on the highest echelons of an organization. Even though the breach happened over two years ago, Target still battles out lawsuits over losses today. Reuters (Ax, 2015) reported that the retailer was in court with credit card companies Visa and MasterCard and was settled for $19 million. Additionally, a consortium of banks has filed a lawsuit against Target (Lecher, 2015).

These examples are situations of organizational crises involving information systems and can be called cyber crises. Crisis terms are often used in a negative sense, in ways to describe situations, which are “unwanted, unexpected, unprecedented, and almost unmanageable, causing widespread disbelief and uncertainty” (Rosenthal, Boin & Comfort, 2001). The above mentioned examples of cyber crises show that even though they have to be solved internally, multiple external factors have impact on the organization and need to be considered. Crises are especially associated with negative consequences, which heavily disrupt a system in which it takes place. Crises are defined as “a serious threat to the basic structures or the fundamental values and norms of a social system which – under time pressure and highly uncertain circumstances – necessitates making critical decisions” (Rosenthal, Charles & ‘t Hart, 1989, p. 10). Crises therefore, can be seen as occasions where urgent decision making under uncertainty is required with a threat of high impact consequences and need to be managed by senior-management.

Yang et al (2013) argue the importance of awareness of different considerations and requirements for a variation of crises as each requires a customized set of actions. In other words, there is need for a training methodology specifically focused on the cybersecurity crisis domain. Unfortunately, the rarity of the incidents within one company limits the opportunity for training and learning on the job. How can practitioners then ever be prepared for such rare events? One way is to prepare for complex and rare situations like cyber crisis through the use of simulation games.

Simulation games can address the need for such a training methodology. Crisis simulations are designed to take rare and uncertain situations into account. Gestwicki and Stumbaugh (2015) make the notion that the goal of educational systems is transfer – that what a student learns in one context can be applied in
another. Borodziec & van Haperen (2002) argue that simulation exercises provide the only experimental means to train people in a close-to realistic environment for unknown crises. Therefore, crisis management simulation training is an often used method to prepare for crisis situations (Bergstrom et al, 2012). These are typically performed in a simulated environment, which received much efforts from the academic community in developing these environments and assessing the effects (Bergstrom et al, 2012). Specifically, simulation games can be used to invite participants to an imaginary world and experience unknown situations without the negative consequences. A good simulation game specifically designed for senior-managers to combat cyber crises, therefore, offers the opportunity for participants to become aware of the challenges and dynamics of crisis decision making, considerations specifically for the cyber domain during cyber crisis and learn to act upon those being immersed in a (safe) simulated environment.

Unfortunately, simulation game design for the purpose of preparing senior-managers for cyber crises is still poorly understood. The problem is not necessarily situated in the number of games available. Several reviews geared towards cybersecurity simulation games are able to find numerous examples (Pastor, Díaz & Castro, 2010; Le Compte, Watson & Elizondo, 2015; Hendrix, Al-Sherbaz & Victoria, 2016). However, three main gaps are found in reviewing the cybersecurity simulation game literature: 1) practical cybersecurity game design is poorly explained, conceptualized or justified, 2) existing cybersecurity simulation games focus on preventive training and awareness, not on crisis response and 3) the target group for cybersecurity simulation games are mostly teenagers, children or security operational personnel. Chapter 2 will address these three gaps in greater detail.

When taking the above perspective into consideration, a tension exists in the cybersecurity simulation game research field. On the one hand, there are two indicators that a cyber crisis simulation game has justification: 1) each crisis asks for different considerations and requires a customized set of actions, and 2) that simulation games are an often used method to prepare for crises. However, when looking at the cybersecurity simulation game literature no evidence of any cybersecurity simulation game exists that focuses on preparing senior-managers for crisis response, let alone research that explicate how to design such games. The presumption here is that cyber crises have characteristics that challenge the translation into a crisis management simulation game. In order to address the lack of a cyber crisis simulation game which prepares senior-managers for future cyber crises, this thesis focuses on exploring these characteristics involved with cyber crises by going through a simulation game design cycle.

### 1.2 Research questions, Research objective and Contributions

Based on the above section, the main research question is formulated as:

**How to support senior-managers in preparing for cyber crisis decision making by means of crisis simulation games?**

This research question serves a greater objective. Crisis situations, as described in the previous section, require critical decision making under high uncertainty and time pressure. In other words, these decisions can impact an organization internally and externally when remained unhandled. However, due to the rarity of crisis events, there is a lack of training on the job. A designed simulation game should offer a training methodology which takes crisis characteristics into consideration, include cyber domain considerations and offer a safe environment to practice decision-making in. This simulation game then offers participants an opportunity to transfer knowledge into real-world scenarios.
The objective of this thesis research is defined as follows:

*To design a simulation game focused on preparing senior-managers for cyber crisis, which offers participants a safe environment to practice decision-making and creates awareness. Specifically, the game focuses on two main aspects: 1) the simulation game creates awareness for the concepts and consequences of cyber crisis decision making and 2) offers a realistic simulated environment for participants to practice decision-making under crisis characteristics like time-pressure and uncertainty.*

This research objective has several implications for further steps of this research. There are three mainly important. First, the research is a design-study and therefore requires a research design approach, where both scientific rigor and practical relevance are involved. Second, the choice for a realistic simulation game requires detailed insights in the cyber crisis domain, both on a conceptual level and on practical decision-making aspects. Third, the perceived usefulness of the simulation game needs to be evaluated by the target group, this involves playing the actual game. In other words, a playable version of the simulation game is required.

Given these three implications the research objective can be broken down into the following three sub-objectives:

1. **Conceptualization of cyber crisis**: The conceptualization of cyber crisis functions as basis for the cyber crisis simulation game and provides relevance in the application domain. To create a realistic game a comprehensive understanding is created. One notion is important to make. When evaluation of the simulation game provides conflicting insights with the conceptualization of cyber crisis, the evaluation insights will be leading for adjustments on the game. In other words, insights from playing the simulation game are leading for the design.

2. **Conceptual design of the cyber crisis simulation game**: the design steps and choices need to be carefully documented, in other words explained, conceptualized and justified.

3. **Perceived usefulness of the simulation game**: Evaluation of the game requires playing the actual game. The usefulness of the game is only practically useful, when it is perceived this way by participants, and is therefore a self-evaluation.

Given these implications and sub-objectives the following sub-questions are addressed in this research and help to answer the main research question:

1. **Which theoretical aspects are important when dealing with crises? How can these be linked to the design of a simulation game that supports senior-managers in preparing for crisis decision making?**

2. **What are necessary elements and functions of a simulation game to support senior-managers for cyber crises?**

3. **What cyber crisis simulation game can be designed meeting requirements from both literature and application domain?**

4. **How useful is the designed simulation game to prepare senior-managers for cyber crises?**

The approach that is taken to answer these questions is discussed in more detail in the next paragraph.
1.3 Research Methodology

1.3.1 Research Paradigm

The main research objective in this thesis is to design a simulation game to prepare senior-managers for cyber crisis. This objective can be broken down into several components. First, it involves the design of an evaluated artifact. Second, it requires the participants to perceive the designed game as useful for its goal. These components propose design research, which implicates that the designed artifact is not only scientifically rigorous but also relevant in the application domain. Winter (2008) argues that not every artifact construction is design research. In his view, as it is design ‘research’, artifact construction and artifact evaluation are reflected on a generic level. However, situational artifacts are needed to balance the tradeoff between solution generity and problem scope (Winter, 2008). In other words, a solution should be generalizable to remain applicable in a broader scope. However, to be able to solve a specific problem, the environment and situation need to be taken into consideration. This design research philosophy has specific implications for this research project. The differentiation is made between the construction and the evaluation on the one hand, and the problem-specific adaptation on the other hand. In other words, the design of the cyber crisis simulation game and the conceptualization of the cyber crisis domain should be evaluated by experts, where the translation to the actual simulation game is evaluated by the participants.

1.3.1 A three Cycle View of Design Science Research (Hevner, 2007)

One particular design-research approach that fits the research philosophy of Winter (2008) is the Three Cycle View of Design Science Research by Hevner (2007). Hevner states design research as the embodiment of three cycles of closely related activities. The first is the Relevance cycle, in which the activities results in input requirements from the contextual environment into the research and feedbacks the artifact into the environment field. The second cycle, the Rigor cycle, provides theories and methods combined with experience and expertise from foundations into the research and adds newly generated knowledge into the knowledge base. The third and central loop, the Design cycle, supports creating and evaluating of the design artifacts and processes. Advantages of this method is that it structures the design process in a loosely coupled manner, as it provides freedom for the designer in using the cycles.

Concluding from a methodology analysis between two design-research approaches (see Appendix A), Hevner’s approach is most suitable for this research. Differentiators are specifically, evaluation of the effectiveness of the game requires a (nearly) completed artifact and evaluation needs to be separated between experts and participants. Also, Hevner’s (2007) view on the construction of the artifact focuses more on the research goal, instead of the urge to optimize organizational fit. One clear limitation of the approach for this research is the original idea of the application domain which stems from Information Systems research. A particular adjustment necessary to fit this research project’s need is the realistic translation of the domain, in this case cyber crisis, into a simulation game which requires a specific simulation game design approach. Using Hevner’s (2007) method standalone will not result in providing methods for addressing the knowledge gaps, as proposed in this thesis. Therefore, a simulation game design approach is added to the methodologies.

1.3.2 Game Design in Seven Steps (Stoppelenburg, de Caluwe and Geurts, 2009)

One approach that complements Hevner’s design cycle approach, and is focuses specifically on simulation game design, are the seven design steps from Stoppelenburg, de Caluwe and Geurts (2012). Their approach of designing simulation games is based on the concept that human knowledge is similar to models, as will be discussed in later chapters. Simulation games, in their view, have to take mental
models from participants into consideration, but also assist to align (conflicting) mental models from stakeholders or at least share them amongst stakeholders. For them a simulation is the process of designing a model of an existing system and to conduct experiments with this model. They define a model as a simplified image that eases analysis and description of the complex system. More details on simulation games are discussed in Chapter 3.

Stoppelenburg et al.’s design approach consists of seven separate steps, which will be followed in the design of the simulation game. The seven steps are (Stoppelenburg, de Caluwé and Geurts, 2009):

1. Define a Statement of Requirements
2. Analyze processes and Mechanisms
3. Create an Integral Schema
4. Define a Simulation Statement of Requirements
5. Construct the Prototype
6. Test the Prototype
7. Refine and Prepare the Game for Use

As discussed above, Hevner’s (2007) approach provides a general design research structure. However, it lacks concrete steps of a simulation game design. Therefore, the seven steps above are implemented in the general structure, depicted in Figure 1. This figure contains elements from following chapters to provide an overview of the contents of the research. A very critical notion is that Stoppelenburg et al.’s method has no consideration for scientific rigor. In other words, Stoppelenberg’s seven steps are purely a methodology to address the simulation game design as well as address the relevance cycle, and not necessarily contribute to the knowledge base by itself. Important for this research is that the models, processes, mechanisms and requirements for such a game are not available in the existing body of literature and therefore there is still a strong and crucial need to use Hevner’s Rigor cycle to translate the efforts of this research into useful insights.

Figure 1: Combining Hevner’s (2007) cycles and the Seven Steps of Simulation Game Design from Stoppelenberg et al (2009)
1.4 Research Strategy

The final step of the research design is to determine the research strategy and the structured set of activities to perform to answer the main research question. As discussed in the above section, this design research focuses on designing, building and evaluating a cyber crisis simulation game. First, it explores the knowledge base, and addresses further focus of the proposed simulation game. Specifically, it addresses important theoretical concepts that increase the effectiveness of such a game. Secondly, this research describes the environment of cyber crisis including its processes, mechanisms and concepts. Thirdly, it explains the design decisions made for the simulation game, also by taking theoretical and application domain requirements into consideration. Finally, it evaluates the usefulness of the designed and constructed game as well as it reflects on the elements that make the simulation game specifically effective for its goal. The following paragraphs describe in more detail how each aspect of the research will be conducted.

1.4.1 Rigor Cycle: Scientific Grounding

The Rigor cycle uses past knowledge to the research project to ensure its innovation. This guarantees that researchers thoroughly examine existing literature to ensure that the designed artifacts are in fact innovative and not based on the application of well-known processes. The literature within the simulation learning, decision making and (crisis) simulation game design research can provide which methods are historically used successfully and what the advantages and disadvantages are of the methods. Most importantly is that the literature research provides decision variables from which the design of the cyber crisis simulation game is based upon. The proposed method is therefore also desk research on both research fields.

1.4.2 Relevance Cycle: Understanding the Environment

Following Stoppelenberg et al.’s (2012) approach, the first steps within the Relevance Cycle is to define a Statement of Requirements. This will entail all kinds of details, like what the type of learning experience is aimed for etc. The next step, analyzing Processes and Mechanisms, focuses strongly on understanding the environment and its main concepts. Important is that Hevner’s approach is to include scientific foundations into the designed artifact and its environment. Therefore, literature review will be conducted on the cyber and general crisis domains. Additionally, expert interviews are conducted to explicate important mental models in cyber crisis situations. From these theoretical and mental models, an Integral Schema is defined first as a communication tool for evaluation and second to represent the simulated model. In the final step to ensure practical relevance, the simulation game requirements are defined which guide the simulation game design.

1.4.3 Design Cycle: building and Evaluation phases

All of the above methods and theories will contribute to design variables, design requirements and design decisions. Important is to evaluate how effective the cyber crisis simulation game eventually is. Because the game is designed for crisis decision making, groups of participants will be involved. For the game building, the seven steps from Stoppelenburg et al (2012) are applied. In the evaluation, the perceived usefulness is discussed. For the evaluation, the view from Klabbers (2009) on simulation game usefulness is taken. According to Klabbers (2009), there are two types of design branches in simulation games: called Design-in-the-small which focuses on simulation games as artifacts to represent processes and mechanisms of reality and Design-in-the-large, which use simulation games to change unwanted behaviors into preferential ones. The interplay is of crucial importance (Kris and Hense, 2006).
The above mentioned research cycles inform the design of a simulation game for cyber crisis. However, a crucial final step is to link the findings from the design of the proposed game back to the knowledge base. By doing this, the research is not only able to build on previous knowledge, but also contributes any new findings to its knowledge base. Therefore, in the evaluation is not purely focused on if the participants perceived the designed game as useful, but also on the specific game elements as well as meeting the research objective. Feeding back knowledge into the literature makes this research not only a design exercise but ensures that it remains design research.

1.5 Structure of the Thesis

The remainder of this thesis is devoted to the design process, from theoretical basis up to the evaluation of the simulation game and the design process. The following chapters will guide the reader through all elements that the simulation game design beholds and explains how each step in the process has influence on the design. Figure 2 provides an overview of the elements that combined form the input for this research. This figure shows how the simulation game is built up and realized, in such a way that all important influences are represented.

As depicted in figure 2, the process starts with the need for a cyber crisis simulation game (Chapter 2). Here the scope of the research is elaborated, which guides the next steps. From here, the process during the research is not as linearly as depicted in figure 2. The process has been more iterative and jumping between application domain and knowledge base. Both Hevner (2007) and Stoppelenburg (2012) mention to start from the application domain, therefore, interviews have been conducted first at the same time that important crisis concepts were uncovered. However, to structure this iterative process, the chapters are organized in a way that the theoretical framework follows in Chapter 3, as it provides the outset of the simulation game design, regardless of requirements and important application domain concepts. In other words, it provides a blueprint simulation game which fit the outlined research goal, without having too much influences from other chapters. Following are the application domain Chapters 4, 5 and 6 which provide important input for creating a cyber crisis simulation game. In Chapter 4, important models from cybersecurity are explained. Chapter 5 elaborates on the practitioner’s view on cyber crisis, based on expert interviews. Chapter 6 combines Chapters 4 and 5 and provides the requirements for the simulation game. From there the simulation game design initiates, elaborated in chapter 7, going into the specific elements and test game runs. Chapter 8 evaluates the simulation game
for its perceived usefulness as well as the insights created during the design process. Chapter 9 answers the main research question and reflects on the most important choices made during the design. Taking all the above into consideration, figure 3 depicts the chapter structure of this thesis.
Figure 3: Thesis outline, inspired by Hevner (2007)
PART I: Knowledge Base

2. The need for training: cyber crisis simulation games

As discussed briefly in Chapter 1, the presumption is formed that cyber crises have certain characteristics that challenge the translation into a crisis management simulation game. To recall, this presumption is based on the premises that 1) each crises asks for different considerations and requires a customized set of actions, 2) that simulation games are an often used method to prepare for crises and 3) that there is no evidence found of cybersecurity simulation games that focus on crisis management. Therefore, it can be argued that there is a need for a cyber crisis simulation game. This chapter explores this need for a cyber crisis simulation game more extensively. Subsequently, this chapter provides guidance for future chapters, in what the research activities will focus on, and more importantly what it will not. In other words, this chapter explicates the scope of the simulation game design and addresses why this scope is chosen.

This chapter discusses the phases of crisis management and further focuses the simulation game on the preparation phase of crisis management in paragraph 2.1. In line with this focus, this chapter dives in the crisis management planning domain and discusses some of its limitations (paragraph 2.2). In paragraph 2.3 the role of senior-managers during crises is discussed. Followed by the elaboration of the existing gaps in the cyber simulation game literature in paragraph 2.4. Finally, paragraph 2.5 concludes the theoretical aspects found important in designing this game.

2.1 Dealing with crisis: crisis management and its phases

The field of dealing with crisis is called crisis management. Dayton (2004) sees crisis management as a catch-all phrase, where it is the broad range of management practices addressing non-routine events. Crisis management according to Coombs (2007) is related to the activity to reduce damages for an organization and defines it as: “Crisis management is a process designed to prevent or lessen the damage a crisis can inflict on an organization and its stakeholders.” Even though researchers use different definitions of crisis management, they divide the process of crisis management in similar phases, emphasizing that crisis management is not one single activity. Dayton (2004) translates it to the crises management phases of: preparation, coping with crisis and back to normalcy.

Dayton (2004) mentions the following main questions during the three phases (p. 168):

- Preparation: How can an organization prepare for the unknown?
- Coping with Crisis: How can crisis managers make the right decisions under circumstances of uncertainty, time pressure and extreme threat?
- Back to normalcy: How can crisis managers bring a shocked system back to normalcy?

The main focus in this thesis lies in preparing senior-managers for cyber crisis decision making. When looking at the phases identified by Dayton (2004), including its questions, one can argue that the focus of this thesis falls mainly in the preparation phase and touches lightly the coping with crisis phase. First because it involves training decision makers for complex and unknown situations, and secondly because it involves practicing decision making under simulated crisis characteristics. However, the emphasis lies on preparing decision-makers instead of making any claims over right decisions even though a realistic environment is created which simulates the wished characteristics.

Both Dayton (2004) and Coombs (2007) provide a literature review on the best-practices of crisis management, and mention preparation as one of the most important aspects of crisis management. Also in the crisis response and post-crisis phases, best-practices contain steps of preparation and pre-defined
planning. Examples include having templates available as press releases and pre-defined employee messages with blank spots to be filled in at a later stage (Dayton, 2004). The following section will focus on crisis management planning and its shortcomings in preparing crisis managers.

2.2 Preparation: Crisis Management Planning and its limitations

Crisis management planning sets in place predetermined plans and/or resources to restore the system back to normalcy after an unexpected event, interruption or incident. Different fields of study focus on this type of planning, which are similar to the crisis management planning definition. For example, emergency planning (Chrichton, Ramsey, & Kelly, 2009), incident management (Nja & Rake, 2008) or business continuity planning (Alesi, 2008; Lindstrom, Samuelson, & Hagerfors, 2010).

These planning and preparation steps make it possible to handle a crisis situation efficiently, because much of the thinking and execution happens upfront. They help enable rapid coordination of actions (Rankin et al., 2013). However, one important notion that is stressed by both Dayton (2004) and Coombs (2007) is that the planning should be a reference tool for crisis managers, not a step-by-step blueprint. The main reason for this is that it is hard to foresee all possible events when planning. In other words, to deal with uncertainty.

Even though there is strong indication on the importance of crisis management plans (Ritchie, 2004; Penrose, 2000), Coombs (2014) contradicts the common view that crisis management is simply the presence of having a crisis management plan or only involves responding when crisis occurs. He argues that the traditional view on crisis management is too limited and has a reactive approach. Having just a crisis plan is not sufficient. Boin and McConnell (2007) share this view and argue that planning for emergencies and crises is necessary but not sufficient. In their view, the contribution of crisis plans lies in (and is limited to) the gain of efficiency; pre-defining roles and responsibilities.

It is believed that the insufficiency of the crisis management plan comes from the contradiction of terms. Boin and McConnell (2007) state: “How can we plan for a phenomenon that, in its very nature violates the very regular patterns upon which planners rely in order to prevent it?” It is this rational expectation, that we can predict crises, which becomes the weakness of crisis management as crises are more complex in nature, transboundary and interconnected (Parakevas, 2006). Transboundary crises cross geographical, functional and time boundaries. These characteristics increase the complexity of crisis and make it a bigger challenge for crisis managers to handle, let alone prepare for them (Snowden and Boone, 2007).

The result is that crisis plans are often just ‘fantasy documents’ (Boin & McConnell, 2007). In other words, the perception of preparedness that comes with a crisis management plan is not reflective to the challenges and complexities of an actual crisis event. Even though Boin and McConnell (2007) mention it ‘unwise’ to completely disregard planning as a preparation tool for crisis, companies should be careful in putting blind trust in the capacity of plans to prepare crisis managers for the complex, extraordinary and critical threats they encounter in times of crisis. Penrose (2000) cited former General Dwight D. Eisenhower, who said “in war, before the battle is joined, plans are everything, but once the shooting begins, plans are worthless.”

The contradiction of terms between the traditional approach applied by many crisis management planning approaches of a predictable world and chaotic nature of crises result in predominantly static ‘fantasy documents’ which lack flexibility to deal with crisis situations characterized by ambiguity, lack of information and constant change. Boin and Lagadec (2000) recognized the transformation of crises and named them ‘future crises’, which are similarly characterized as transboundary crises. Boin and Lagadec (2000) take the position that future crises require a preparatory effort that combines resilient oriented strategies and anticipation-based strategies, like crisis management planning. Resilience is determined as
an organization’s ability to return to a state of normalcy after a disruption (Bhamra, Dani & Burnard, 2011). Resilience seems to come from similar grounds as Boin and Lagadec’s (2000) view, where it offers a preparation tool to reduce risk in uncertain environments. A crucial aspect of resilience is the realization that organizations are part of and are dependent on their context to reduce risks of threats (Bhamra, Dani & Burnard, 2011). In concept, a resilient organization implements detection and enhanced monitoring, which is followed by organizational response, subsequently followed with either positive or negative adjustment which results in eventual organizational learning in response to an event which poses a threat (Burnard & Bhamra, 2011). Even though resilience is a dynamic way to cope with unexpected events, it seems a high level practice in which depends on the organization’s ability to implement and further develop the specific components. Although undoubtedly important for an organization to be resilient in face of disruption, it is not the focus of this research. This thesis focuses on preparing the individual senior-manager for cyber crisis at the moment the disruption would actually take place, and not on putting in the required organizational preparation elements in place.

### 2.3 Preparing senior-managers for crises

A less discussed aspect so far is the role of senior-managers during crises. Boin and Lagadec (2000) articulate the dangers of insufficient prepared senior-managers in a useful manner, specifically in the light of earlier discussed future crises: “Insufficiently prepared organizations and managers will be unable to respond to the difficulties created by this changing theatre of operations. Crisis managers need to be trained in order to avoid the elementary pathologies that accompany crises and breakdowns.” (p. 187).

Important is that according to Boin and Lagadec (2000), this preparation for senior-managers should not necessarily focus on the tactical level as specialized bodies within the organization can address these activities. Their opinion is to focus trainings for senior-managers more on situations that cannot be anticipated, requiring non-programmable responses. Tactical problems are not the main challenge for senior-managers. During crises senior-managers are faced with threats that jeopardize the very survival of their organization and should take lead to prevail potential catastrophe in a very uncertain environment.

During crises, many overwhelming events need attention from crisis managers. Everything screams for attention at the same time. The need for adaptability and flexibility in crisis management becomes evident during crisis situations (Rankin et al, 2013). The dynamic and fast-moving nature of crisis necessitates decision makers to adjust to the situation at hand. Different researches note that preparing both through documentation as adding flexibility increases effectiveness (Mandinka et al, 2006; Lindstrom & Pettersson, 2007). Given this need for flexibility, preparing for crisis blindy trusting on crisis management planning documents only is unwise and should be strengthened with training methods which prepares senior-managers on an individual level to deviate effectively from planning when deemed necessary. According to Boin and Lagadec (2000), the aim of creating awareness at the highest levels can be raised through workshops and simulations, specifically to new types of situations to the decision makers and their responsibilities and formulate the aim as follows: “The aim is to forge new attitudes: tolerate open and sharing questioning about uncertain situations; reflect on the decision making process in absence of clear expertise; understand the need to communicate internally and externally whilst in a situation of uncertainty, even complete ignorance, for extended periods of time; steering complex systems by accommodating the coexistence of conflicting logics.” (p. 189).

As discussed in the Introduction, simulation games can invite senior-managers by offering experimental means to train participants in a close-to realistic environment for unknown crises (Borodicz & van Haperen, 2002). Linked to the view of Boin and Lagadec, these crisis simulations are designed to create rare and uncertain situations in which participants transfer the knowledge from, which indicates that this knowledge can be used in another context (Gestwicki and Stumbaugh, 2015). Specifically, simulation games can be used to invite participants to an imaginary world and experience unknown situations without the negative consequences.
Given the above perspective, one can argue that there is a need for a simulation game specifically focused on preparing senior-managers for cyber crisis would offer the opportunity for participants to become aware of the dynamics and challenges of crisis decision making while being immersed in a (safe) simulated environment, which enables the transfer of this experience into other domains. However, clearly missing so far is the cyber perspective. Therefore, the next paragraph focuses on reviewing the cybersecurity simulation game literature to discuss what the existing body of knowledge can inform the design of such a game.

2.4 Cybersecurity simulation games

As Bergstrom et al. (2012) mention, crisis simulation games have received much efforts from the academic community in developing simulated environments and assessing their effects. In the Introduction was mentioned that no evidence of a simulation game that focuses on preparing senior-managers for cyber crisis has not been found as well as that three gaps existed in the cybersecurity simulation game literature. The remainder of this paragraph addresses these claims in more detail.

The literature has been searched by starting with querying literature databases for a combination of cyber terms (like cyber security, cyber etc.), crisis and simulation games. However, no such specific game was found. Therefore, the search slimmed down to the combination of cyber terms and simulation games from the last decade. This resulted in six papers that focused on cybersecurity simulation games, these are a combination of papers that either discuss specific cybersecurity simulation games or review the literature themselves. Because six sources are rather limited to generate observations from, the found observations are cross validated with three literature reviews that aim to offer a state-of-the-art for cybersecurity simulation game field.

Four observations are derived from a brief literature review conducted on cybersecurity simulation game literature. An important note here is that the examples discussed under the observations can be a combination of multiple observations, but they highlight the observation that not has been mentioned to that point.

**Simulation games use cybersecurity merely as a scenario**

A couple of simulation game papers exist which focus around a cybersecurity scenario. However, these type of simulations do not address the characteristics of cybersecurity, but simply use its story to conduct research outside the domain of cybersecurity. Person and Bishop (2014) use a simulation game, called CyberSIM, for participants working in large organizations to help them learn how to communicate and collaborate more effectively with their peers in other offices or agencies. CyberSIM is designed to explore key components of collaborative behavior and to help students to develop more effective communication skills by prioritizing functions in a simulated environment. A second example is Rosoff et al. (2014), which use the cyber case to conduct scenario-simulation behavioral experiments to explore how individual users respond to common cyber-based financial fraud and identify theft attacks by systematically manipulate variables related to characteristics of the attack and attackers. This type of research is focused on behavioral aspects, but do not address training on cyber concepts nor focus on decision-making aspects.

.. are mostly geared towards training and awareness for children, teenagers or students..

Secondly, a large group of cyber security simulations focus strongly on education and awareness for children, teenagers or students. CyberAware is a mobile game app created for small children, to raise awareness for security concepts (Giannakas et al., 2015). Their research focuses on delivering cyber security knowledge in a form of a digital game, used to increase joy and efficiency in the learning process of children. The game supports and guides students toward the correct answer by offering tips and advice
when the player’s answer is incorrect. Another similar project, SecurityEmpire, is developed to teach high-school children cybersecurity concepts (Salazar et al., 2013). Their objective is to raise awareness for teenagers between 15 and 18 years old, on the control over personal information on social networks. The augmented-reality game focuses on the threats that high-school students face in social networks and their interactions with other online services to create a familiar environment to explain information security concepts. Strong emphasis is put on robust passwords, multilevel security and healthy skepticism.

.. are focused on the tactical or operational level..

One Cyber simulation game which focuses on decision-making aspects and their consequences is Cyberia (Bishop & Frincke, 2005). This game focuses on increasing the awareness of the impact of poor security choices and the concrete steps that can improve security within it for cybersecurity students. Specifically, the objective for the player is to provide the necessary security measures to protect valuable information assets while keeping the organization’s users happy and productive. This is done by a resource-management simulation where decisions are made by players regarding procedural, technical, and physical security. Many of the security choices involve risk management. This game does focus on players’ decision-making, however on a tactical level and not on senior-management level.

..and lack the explanation, contextualization or justification of their designs.

Gestwicki and Stumbaugh (2015) even analyzed 21 games, focused on teenagers, which designed to teach cybersecurity concepts. Their analysis results in a three-tier taxonomy of games: Games that convey cybersecurity concepts through narrative and/or theme only. These games do not require any decision-making that reflect an understanding of cybersecurity concepts. Three types were mentioned: (Type 1); Games that integrate multiple-choice questions that correspond to cybersecurity concepts. Answering these questions correctly requires an understanding of the concepts (Type 2); Games that require ambiguous decision-making that making good decisions implies an understanding of cybersecurity concepts (Type 3). However, their concern with existing literature is that there is no empirical assessment of any of the 21 analyzed games, and very few of them explaining, contextualizing, or justifying their designs.

The above observations are based on a small amount of sources, and lack the rigorous approach of an extensive literature review. However, the above observations do indicate where the cybersecurity simulation game research field could have gaps. To increase validity of these observations, three additional literature reviews which aim to offer a state-of-the-art analysis of cybersecurity simulation games are consulted. The following three literature reviews are used to assess the above mentioned observations:


This paper reviews the state-of-the-art in simulation systems designed for information security and information assurance education, training and awareness. This review uses a taxonomy that differentiates five types of simulation systems. The authors found that 8 out of 13 tools analyzed in their article are classified in the PacketWars category, which utilize network attack and defense at a *tactical level.* The other categories that were represented by the simulation systems were Sniffers, canned attack/defend scenarios and management flight simulators. What is important is that these three categories all focus on the operational / tactical level. Notable is that none of the tools analyzed were of the fifth category, the only one that would require high-level decision making, role-playing game. Additionally, they found that the target audience for these tools were mostly students.


Le Compte et al. (2015) conduct a literature review on several serious games for cybersecurity to eventually make observations for a framework for future simulation games. The most relevant
observation from their reviewed games is that the games are mostly designed for educational purposes for use in school or university, which affirm the observation earlier made on the target group.

C. Hendrix, Al-Sherbaz & Bloom (2016). Game Based Cyber Security Training: are Serious Games suitable for cyber security training?

This paper investigates whether games can be effective cyber security tools by conducting a structured literature review on 28 papers discussing cyber security games. Two observations made by Hendrix et al. (2016) are similar to the ones made in this paragraph. First, in their review on simulation game studies, they notice that games target the individual end user and the authors even address the lack of games that address management decision making.

Additionally, Hendrix et al. (2016) criticize a large portion of the reviewed simulation game papers for their lack of scientific rigor. The foremost reason was the lack of evaluation of the training or the approach in designing the simulation game in any way. Another reason was that authors were superficial in their explanation on the methods, the results or both. In the end, only 11 simulation games had evaluations which could be scientifically scrutinized, with clearly described methods and outcomes.

Table 1: Observations validated with three literature reviews

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Simulation games use cybersecurity merely as a scenario</td>
<td>• Not mentioned. These systems were filtered in the selection process.</td>
<td>• Not mentioned.</td>
<td>• Not mentioned. The literature review has focus on answering the question: are serious games suitable for cyber security training?</td>
</tr>
<tr>
<td>Cybersecurity simulation games are mostly geared towards training and awareness for children and teenagers or students</td>
<td>• Target audience the reviewed simulations systems addressed was mainly for students.</td>
<td>• Most reviewed serious games are designed for educational purposes for use in school or university.</td>
<td>• All the selected simulation games are focused on training and awareness for students, teenagers or children. Therefore, this is not an observation.</td>
</tr>
<tr>
<td>Cybersecurity simulation games are focused on the tactical or operational level</td>
<td>• All found games are focused on the tactical and operational level.</td>
<td>• Partly mentioned. But no particular observation mentioned by the authors.</td>
<td>• Not mentioned. Their literature review focused on the learning contribution that the simulation games make.</td>
</tr>
<tr>
<td>Cybersecurity simulation games lack the explanation, contextualization or justification of their designs</td>
<td>• Not mentioned. The main focus was to analyze the focus of the systems.</td>
<td>• Not mentioned. Their goal was to design a framework for future serious games, particularly focused on the goals and functions and were not particularly interested in design.</td>
<td>• The authors criticize a large portion of the reviewed simulation game papers for their lack of scientific rigor. Foremost reason was lack of evaluation and second the superficial explanation on the methods, the results or both.</td>
</tr>
</tbody>
</table>

In summary, of the four observations made above, three are explicitly mentioned in other literature reviews conducted over cybersecurity simulation researches. Table 1 summarizes the analysis of the found observations across the three literature reviews. Therefore, a review on the cybersecurity simulation game field shows that there are some aspects of concern. First, games are focused on behavioral aspects, but do not focus on decision-making aspects. Second, the literature is mostly focused on education and awareness on cybersecurity concepts for children, teenagers or students. These types of games are mostly focused on prevention. Finally, cybersecurity simulation games lack empirical assessment and literature in which game design choices are explained, conceptualized or justified. The bottom line is that it can be concluded no simulation game seems to exist with the focus on crisis management on the senior-management level, let alone one that explains, contextualizes or justifies the game design approach and or game elements.
2.5 Conclusion: the need for a Cyber Crisis simulation game

In this chapter several important aspects have been identified that guide subsequent simulation game design efforts. Together, the specific need can be summarized as: simulation game specifically focused on preparing senior-managers for cyber crisis would offer the opportunity the participants to become aware of the dynamics and challenges of crisis decision making while being immersed in a (safe) simulated environment, which enables the transfer to this experience into other domains. Given Hevner’s three cycles, there are two main sources that inform the design of this simulation game. First, it is the knowledge base, which consists of the scientific theories and methods. Second, it is the application domain which has to be simulated, in this case it is cyber crises.

To be able to design the proposed simulation game, the following theoretical concepts need to be addressed from theory, and will be further discussed in Chapter 3:

Simulation Games and Learning. The basis of the design is the simulation game. As earlier discussed simulation games offer experimental means which can train participants in close-to realistic environment for unknown crisis (Borodzicz & van Haperen, 2002). Consequently, this requires knowing which elements are used in simulation games.

Additionally, a very important aspect of simulation games is the transfer of knowledge (Gestwicki and Strumbaugh, 2015). Therefore, the learning function from simulation games will be addressed in the next chapter. Important is that the aim of the learning should be to forge new attitudes: tolerate open and sharing questioning about uncertain situations; reflect on the decision making process in absence of clear expertise; understand the need to communicate internally and externally whilst in a situation of uncertainty, even complete ignorance, for extended periods of time; steering complex systems by accommodating the coexistence of conflicting logics (Boin and Lagadec, 2000). Hence, the focus is not on making the right decision but on making participants aware of their decision making.

Decision making under uncertainty. The simulation game elements make it possible to simulate the aimed situation. As discussed above, preparing senior-managers should not focus on the tactical level, but on situations that cannot be anticipated, requiring non-programmable responses (Boin and Lagadec, 2000). Combined with uncertainty being a very important characteristic of crisis situations (Parakevas, 2006; Snowden and Boone, 2007), focus will be on decision making under uncertainty. But this should also include the mechanisms that are the basis for this particular decision making.

As mentioned earlier, simulation games offer opportunities to create a close-to realistic environment. In this case, it is cyber crisis decision making. Specifically, this simulated environment should increase awareness of the dynamics and challenges of cyber crisis decision making. However, the three gaps mentioned in this chapter were: 1) Cybersecurity simulation game design is poorly explained, conceptualized or justified, 2) Existing cybersecurity simulation games focus on preventive training and awareness, not on crisis response and 3) The target group for cybersecurity simulation games are mostly teenagers and children or security operational personnel. These gaps provide challenges from a design point of view, as cybersecurity simulation game literature is limitedly able to serve as an input for the design of the proposed simulation game. Consequently, inputs for what makes this simulation game specifically geared towards cyber crisis need to come from different sources than literature. Explicitly, the inputs are the elements from reality that need to be simulated within the simulation game parallel with concepts from theory. The following inputs will be gathered from the application domain, and will be described further in chapters 4 to 6: Cyber crisis management processes and mechanisms, cyber crisis chaos and emotions during crisis.
What follows is that the theoretical framework, discussed in chapter 3, will focus on the design of a simulation game which incorporates the theoretical aspects of *Simulation Games and Learning* and *Decision making under uncertainty* and its basic mechanisms. The aspects mentioned for the application domain will be discussed extensively in chapters 4 to 6, but will not be limited to the concepts discussed in this chapter.
3. Theoretical Framework: Simulation Games, Situational Awareness and Decision-making under uncertainty

In chapter 2 the need for a cyber crisis simulation game was elaborated and a couple of key elements identified which are to be included in the game. The following elements, as discussed earlier, are included in the simulation game design: Simulation games, learning and decision-making under uncertainty. All have their own theoretical basis, which need exploration to be able to use in the simulation game design. Together, these elements and their theoretical basis form the foundation for the conceptual design, regardless of influences from the application domain. In other words, the combination of these elements and theories offers a blueprint for a conceptual design, in which the application domain provides input to in later stages, eventually resulting in a complete cyber crisis simulation game design.

This chapter builds this blueprint from the outside in. First, as the most important vehicle in which the other two concepts are carried, is Simulation Games (3.1). Secondly, it is generally accepted that situational awareness precedes decision-making, and therefore deserves mentioning (3.2). Finally, as last building block of the theoretical framework is Decision-making under uncertainty (3.3). The final paragraph of this chapter (3.4) will provide an overview of the discussed theoretical concepts which will influence the conceptual design. In other words, it provides the promised blueprint for the conceptual design of the simulation game.

3.1 Simulation Games

The first element to start with is the arena in which all action shall take place, the simulation game. As described in chapter 2, simulation games can offer a flexible and safe environment in which rare and uncertain situations can be simulated. Another advantage is that simulations can offer a close-to-real experience to participants, without the actual negative consequences (Borodicz & van Haperen, 2002). Great, but what then is a simulation game? The first section will focus shortly on the definition and its general elements. The question that follows from a designer’s point of view is which elements of simulation games should be considered? To address the goal of awareness for cyber crisis concepts, dynamics and mechanisms, a section is dedicated to learning by simulation games. In other words, it discusses the ways in which participants learn during simulation games. These concepts offer a set of important design principles for later stages. Combined these are the design principles and elements that form the backbone of the simulation game design, later to be complimented by models from situation awareness and decision-making under uncertainty.

3.1.1 Simulation Games and Characterizing Elements

Some important concepts that are often used interchangeably are gaming, simulation and simulation games. But what are the main differences between these concepts? Klabbers offers insights on the different concepts in his book on gaming The Magic Circle (2009). In his view “a game is any contest or effort (play) among adversaries or teammates (players) operating under constraints (rules and resources) for an objective (winning, victory, prestige, status, or pay-off). The exercise, or activity, should involve overt competition, or cooperation, between the individuals or teams, who are competing against each other, or together (while jointly conquering circumstances) fighting the odds” (p. 33).

To explicate the differences, he mentions simulations as a process which reproduces a set of conditions or the attempt of problem-solving or deal with consequences by representing the problem or a scenario mathematically, using a computer model. Then in his view, a simulator is a device that is created to reproduce real-life conditions to train people. However, the description that Klabbers (2009) uses to
describe simulations are very underdeveloped and of a different level of detail than his definition of
games. These definitions might exclude certain examples from each other, but definitely do not
contradict each other. In other words, these two can be combined into a term called simulation games.

Stoppelenberg, de Caluwé and Geurts (2012) use exactly this term in their extensive book on simulation
games. In their view a simulation is “the process of the design of a model of an existing system and the
conduction of experiments using this model.” (p. 22, translated from Dutch).

Stoppelenburg et al (2012) and Klabbers (2009) agree that both games and simulations use models to
represent the processes and objects and how they relate to their environment. Klabbers (2009) mention
models as either a physical representation or a theoretical description to give insights on how it feels and
looks or how the internal processes work or might work. For Stoppable et al (2012) models are a
simplified depiction of a complex system which eases the description and analysis of this complex system.
It is this method from Stoppelenburg et al (2014) of model building which is guiding for this thesis. In
other words, a combination of different models is taken together to form a larger model, which
eventually is the proposed simulation game. Figure 4 shows Stoppelenburg’s view on creating a
simulation games from models.

![Diagram: Simulation Game as Model Construction](p. 43)

From this, Stoppelenberg et al (2012) argue that a simulation model is a model in its purpose replicate the
dynamics of a system and to analyze the system at interest. To simulate, then, is to depict reality in a
particular artefact which enables the exploration of dynamic characteristics of this reality by
experimenting with the artefact.

Additionally, they add their definition of a game. They do not create a concept of a game on itself, but
put that in light of simulations. In their view, simulation games find their functionality from the behavior
of the participants. Similarly, to the concept from Klabbers (2009), players fulfil roles, try to accomplish
goals, have to perform actions, achieve results (positive and negative) as a consequence of their activities
in relation to other players or elements. Simply put, a simulation game combines both concepts: there is a
(simulated) model of a (real or conceptual) system and there are actors, having different roles, which try
to achieve specific goals within a set of rules.
Summarizing, simulation games have the following characterizing elements:

- Actors, with different roles and perspectives;
- Which follow a set of rules;
- Perform actions in a simulated model which is derived from a reference system;
- Participants, by their actions, become part of the model.

### 3.1.2 Learning from Simulation Games

Now that we know what simulation games are, let's dive into why they are effective. One of the main characteristics of simulation games is learning. This is an important concept, as without any learning, it would be a game merely for entertainment purposes. The following four sections discuss four aspects of learning in simulation games and their inner workings. The first discusses the learning preferences simulation games foster for. The second dives into experiential learning, which lies on the foundation of simulation game learning. The third section discusses that learning is internalized through debriefing. The section on learning ends with describing the role of the facilitator during simulation games. All of these sections contribute to aspects of the simulation game design. These aspects can be found back in the structure of the game, the debriefing, and facilitator documents. More details on these components are in chapter 7, but are formed as a basis in the sections discussed here.

### Learning Preferences

One important aspect to take into consideration is learning preference(s) of the individual. In simulation sessions, participants often have different backgrounds and come from different departments within an organization (or across organizations). But most importantly, these individuals have different personalities and learning preferences. From a design perspective, adjusting a simulation to the particular participants is time-consuming. On the other side, when a game is not addressing the learning preferences, there is the danger of becoming ineffective. Roisters and Simons (2006) have created a language of learning: a language which enables identifying learning preferences and therefore to be able to better take these preferences into consideration. The focus of this language is on the context in which an individual prefers to learn. One important notion from Ruijters and Simons (2006) is that when the context does not nurture these learning preferences, barriers will occur.

Ruijters and Simmons (2006) provide five learning preferences:

1. Adopting best practices: learning by jumping on the band wagon, to observe what works and what does not work, learning on the job, also under pressure and not specifically in a safe environment. This learning preference is chaotic, unpredictable, and always moving. Observe, listening to others, trial-and-error, evaluate what is useful and what is not are favorite activities.

2. Participate: Learning in dialogue, together with others, by conducting an assignment, to undertake initiative and to collectively provide meaning. By talking about it you can provide collective meaning. To discuss is helpful to sharpen and bring light to ideas.

3. Acquire knowledge: learning from experts, goal oriented knowledge creation. Following lectures, reading articles and books. To educate others as well.

4. Practice: learning by deliberate practice in a safe environment including critical reflection. Typical examples are role-playing and simulation. Time is required to feedback on thinking and acting and to reflect. Making mistakes is very valuable.


Simmons (2008) states that within simulation games, the learning preferences of participate, practice and exploration are stimulated and developed. Additionally, when simulation games are played in a group in a single room, the learning preference of adopting best practices is also added. In other words, the only learning preference that simulation games do not foster for is to acquire knowledge. What the four learning
preferences present in simulation games have in common is these are learning based on action. In other words, these learning preferences are based on building personal experiences. The next section discusses experiential learning.

**Experiential Learning**

One of the most cited theories on learning is the experiential learning model from David Kolb (professor of Organizational behavior). Kolb defines learning as “the process whereby knowledge is created by the transformation of experience”. Experiential learning, then, is the process of making meaning from direct experience, or learning through reflection on doing. In Kolb’s (2014) theory, learning happens through four different phases in a cycle: having a concrete experience, followed by observation of and reflection on that experience, which leads to formation of abstract concepts (analysis) and generalizations (conclusions), which are then used to test hypothesis in future situations, resulting in new experiences (Thatcher, 1990). From this, choices and decisions are formed about the next steps, where the cycle repeats itself. By repeating the cycle over and over, the new learned behavior can be internalized. Stoppelenburg et al. (2012) use the Kolb cycles to design their simulation game runs. In other words, specific experiences are recalled during the simulation game. In the debriefing observations and reflections from playing the game are discussed. Intentions for next rounds are formulated and subsequently tried in the next round. For Stoppelenburg et al. (2012) a game run exists of four or five of such cycles. Therefore, to build further on Kolb’s (2014) learning cycles and Stoppelenburg et al.’s (2012) game runs, these will also be implemented in the designed simulation game. The game runs are explained in more detail in chapter 7.

Kolb’s (2014) theory on learning cycles stem from the field of organizational psychology. A researcher focusing on learning by using simulation games is Thatcher (1990). Who also builds on Kolb’s (2014) theories specifically for simulation games. Thatcher (1990) summarizes Kolb’s four phases as: concrete experience (CE), reflective observation (RO), abstract conceptualization (AC), and active experimentation (AE). Thatcher (1990) sees this model as fundamental for simulation games, since simulation games are a form of “controlled” experience from which learning can come from if the whole experience is used effectively. Thatcher stresses the words whole experience in which it meant the number of Kolb cycles, but most importantly, the debriefing. Thatcher (1990) states this as follows: “In developing the use of games and simulations in various learning contexts, I became more and more convinced that the debriefing – the process of reflecting on and exploring what had occurred from the point of view of each participant – was the place at which the fundamental learning which resulted from the experience took place” (p. 263). Figure 5 shows how Thatcher (1990) implements the Kolb’s cycles in his model. This model is included in the structure design of the simulation game, which will be elaborated on in chapter 7.
Figure 5: Learning from a Simulation. Adapted from (Thatcher, 1990, p. 269)
Debriefing

Simulations in essence are a form of experiential learning, as participants are actually engaged in an experience. As Stoppelenburg et al (2012) mentioned, this experience is dynamic. These dynamic experiences are formed by the participants themselves as the simulation game develops. According to Thatcher (1990), three types of learning are present in simulations:

1. Learning the facts: expressed in the game contexts and dynamics (not only facts, concepts and generalizations but also skills)
2. Learning the process simulated by the game
3. Learning the relative costs and benefits, risks and potential rewards of alternative strategies of decision-making.

An additional element specifically for learning, mentioned by Thatcher during simulations (1990), compromises of the emotional side of being inside a game and seeing the effects from the decisions taken by the team on the environment and the players.

In their book Reflection: Turning experience into learning, Boud, Keogh and Walker (2013) discuss reflection and define the process as “a generic term for those intellectual and affective activities in which individuals engage to explore their experiences in order to learn to understandings and appreciations.” Three important stages exist within the process of reflection (Thatcher, 1990):

- Returning to the experience: In which the experience is recollected, the events are replayed or explained to others. What Boud et al mean by this is the initial perception of the events from the individual participant’s point of view.
- Attending to feelings: here both positive and negative feelings are addressed. According to Thatcher (1990) a vital part of reflection.
- Re-evaluating the experience: this involves analyzing of experience, especially when knowing the first two phases of reflection. This step is deliberate and crucial for the internalization of the learned knowledge, attitude or skills.

Thatcher (1990) argues that it is the reflection or reflective observation (RO) is the crucial link between experience and the process of change and adaption in the mind which becomes part of the learner’s inner conceptual models. Thatcher formulates the reflection a lot better than I can: “It is the equivalent of that process used by young children when they talk through and discuss the solution of a problem or the performance of a task either to other children or adults, or to themselves. This process of articulating one’s thinking is a vital part of the process of converting experience into learning or of using one’s conceptual apparatus in a concrete experience by raising to the surface the thoughts and embryonic ideas of the individuals in the learning situation.” (p. 266).

One idea from Thatcher (1990) which is implemented during the game is having a designed response questionnaire available. This is a self-evaluation which each participants completes and uses during the debriefing session. By doing this, the individual participant is forced to consider important points to simulation, before their experience is under snowed during general discussion.

The above mentioned phases and steps are incorporated into the game in the debriefing phase. These will form the structure for the debriefing and offer guidance for the facilitator to address topics when reflecting on the game and participants. The implementation in the design will be discussed further in chapter 7.

The Role of the Facilitator

Inherently linked to debriefing is the facilitator. A very important role in simulations games lie in the hands of this facilitator. When the players are debriefed and introduced to the most important facts, the facilitator has no control over the speed which these materials offered to them are used, nor the order in
which the participants use them. An important role for the facilitator then is to be supportive to the flow or dynamic of the simulation game, to facilitate debriefing, and thus promote discussion and reflection, in other words to enable the use of materials as effectively as possible. An important notion that Thatcher (1990) makes is that the facilitator has to learn to not interfere.

Stoppelenburg et al (2012) take the same perspective in the role of the facilitator as Thatcher. They promote the importance of the simulation game running from itself, but stress that sometimes the facilitator is needed to guide the participants to new aspects of the game. But most importantly, facilitators have to intervene when problems occur, that lie beyond the control of the participants, which could halt any learning experiences. Therefore, it is important to understand some group processes. There are four aspects which are identified in effectively working in a group:

1. Contents or Task: This involves the task, the activities that participants have to perform. The ‘what’ of the cooperation, the goal that is sought for and the messages that are exchanged. Contents can be observed in information, opinions, arguments, facts and goals
2. Procedure or method: Procedures are the institutions or structure. These are the intentions and agreements that the group made about the way a task is approached.
3. Process (or interaction): This involves the actual steps. In the process, the agreements and rules are implicit. Often, there are non-visible interests, needs, uncertainties and motives. This aspect focuses on how participants interact with each other.
4. Emotions: These are the emotions that individuals express in playing their role.

As the facilitator has such an important role in 1) guiding the game and 2) harness parts of the learning, they are required to be informed as good as possible. This will be governed in a document which is called: “the facilitator document”, which explains the above mentioned theories and principles to facilitators. More detail of this document design is given in chapter 7.

3.1.3 Creating a realistic and safe environment with narratives

As earlier discussed, one of the objectives is to create a safe and realistic simulated environment to practice decision-making in. Two main elements of simulation games are addressed in this section, to support the simulation game design. In other words, these form an important design principle which will be adhered to during the formulation of the specific game elements in chapter 7.

Working with narratives

In the entire design process, there are many efforts done to provide a realistic environment which foster practice and learning for participants. These elements and mechanisms are processed in the simulated model of reality or concept and stem from the application domain. However, there is one principle that is inherently part of simulation games, which is addressed here: narratives. During a simulation game, emotions can heat up, especially when there is more at stake than seem at first. Different group phenomena can cause dysfunctional patterns and dissolution of groups (Bion, 1961). Bio (1961) found three basic assumptions that are created on an unconscious level that hinder a groups productivity.

Common to these assumptions are the fear for the environment and insecurity of the place of the individual in this environment. Shortly the three basic assumptions are (Bion, 1961):

1. Dependency: The assumption that the group leader has to protect them.
2. Fight-flight: The group is a dangerous place. A lot of ‘we’ against ‘they’ language.
3. Pairing: People assume that when forming a pair with another individual, the other will help them to go through difficulties. This causes emotional subgroups and disruption.

Fears are part of working in any social environment. It is the task of facilitators to recognize the dysfunctional patterns and discuss these, to create a safe environment for participants. Additionally, simulation games can create these safe environments by using narratives (Stoppelenberg et al., 2012).
Simulation games are a narrative space (Breuer, 2008). Within this narrative space the two worlds of the narrator and the participants will meet and an exchange of ideas, experiences and feelings happen.

Narratives are grounded in everyday life and in some way shape our lives, also in organizations (Czarinas, 2004). Stoppelenberg et al (2012) also address this topic and mention narratives for simulation games specifically. According to them, narratives offer insights in the perceptions of individuals and offer procedures for specific situations. They add that listening to narratives and exchanging those can lead to mutual understanding and organizational improvement. The idea here is that people actually change by adding experience to their own already existing experiences.

Abma (2006) mentions favorable characteristics from working with narratives: equality between participants, an open climate, and the absence of taboos. According to Abma (2006) narratives work because they always address the things that truly matter to people. Emotions are wrapped inside narratives and therefore have a sense of feelings. Additionally, they are also influenced by the moral or political viewpoint of the narrator. This involvement of concern, emotions and wants and needs keep people involved.

Following this powerful principle of narratives, the design will focus on creating a narrative for the participants (scenario and events) but also will evolve around the creation of a narrative from playing the game. The offered narrative will invite them to the safe environment where the second offers participants the opportunity to evaluate their actions after the game. In other words, during the debriefing participants can return to ‘their story’.

3.1.4 Conclusion: the backbone of the simulation game

In the above three sections several theoretical concepts are discussed which shape the design of the cyber crisis simulation game. Combined, these concepts form the General outline of the simulation game which is shown in Figure 6. It starts with the arena, the simulation game, which acts as a vehicle for the rest of the components. Characterizing for a simulation game is that it is an environment simulating a real or conceptual model in which actors assume particular roles, are bounded by a set of rules and strive for specific goals. Most importantly participants become part of the simulated model by participating.

The underlying thought here is that simulation games are the basis of the design, as they offer experimental means that can train participants in close-to-realistic environment for the situation that is wished, by using simulated models from both reality and concept. However, simulation games find their functionality from the behavior of the participants, as players fulfil roles, try to accomplish goals, have to perform actions, achieve results as a consequence of their activities in relation to other players or elements. Therefore, a simulation game combines both concepts: there is a simulated model of a (real or conceptual) system and there are actors, having different roles, which try to achieve specific goals within a set of rules.

A second very important function from simulation games is learning, as discussed in Chapter 2. There it was mentioned that the knowledge and experience learned in one domain can be transferred to another. Research shows that within simulation games, the learning preferences participate, practice and exploration are stimulated and developed. Additionally, when simulation games are played in a group in a single room, the learning preference of adopting best practices is also added. What the four learning preferences present in simulation games have in common is these are learning based on action. In other words, these learning preferences are based on building personal experiences. This experiential learning (Kolb, 2014), lies on the foundation of simulation game learning according to Thatcher (1990). Thatcher summarizes Kolb’s four phases as concrete experience, reflective observation, abstract conceptualization and active experimentation. These cycles are implemented in the general outline of the simulation game.
Most importantly, the learning happens from going through the *whole experience*, which includes a number of cycles, but most importantly the debriefing.

It is during the debriefing that a special role exists for the facilitator. In Chapter 2, it was mentioned that part of the aim for the learning efforts for senior-managers was to forge new attitudes: tolerate open and sharing questioning about uncertain situations and reflect on the decision making process in absence of clear expertise (Boin and Lagadec, 2000), among others. As the facilitator has such an important role in 1) guiding the game and 2) harness parts of the learning, they are required to be informed as good as possible. This will be governed in a document which is called: “the facilitator document”, which explains the above mentioned theories and principles to facilitators, including: types of learning, stages of reflection, their role, group processes and when to take action.

Additionally, implemented is a designed response questionnaire. This is a self-evaluation which each participant completes and uses during the debriefing session. By doing this, the individual participant is forced to consider important points to simulation, before their experience is under snowed during general discussion. This document also helps the facilitators guiding the debriefing session.

The last element to discuss is the use of narratives. Abma (2006) mentions favorable characteristics from working with narratives: equality between participants, an open climate, and the absence of taboos. According to Abma (2006) narratives work because they always address the things that truly matter to people. Emotions are wrapped inside narratives and therefore have a sense of feelings. Additionally, they are also influenced by the moral or political viewpoint of the narrator. This involvement of concern, emotions and wants and needs keep people involved.

Following this powerful principle of narratives, the design will focus on creating a narrative for the participants (scenario and events) but also will evolve around the creation of a narrative from playing the game. The offered narrative will invite them to the safe environment where the second offers participants the opportunity to evaluate their actions after the game. In other words, during the debriefing participants can return to ‘their story’.

The last element which is depicted in Figure 6 is the individual factors from Ensley (1995), which will be discussed in the next paragraph. However, a part of Endley’s model of situation awareness fits well in this figure. Simulation games can offer a form of training to practice and improve abilities and offer a form of experience. Additionally, during the play of the game, participants are exposed to other participants including their abilities and experience and are able to reflect on their own. Therefore, factors like information handling mechanisms, long term memory and automatism are addressed implicitly. In other words, the participants bring these factors into play, but are not necessarily addressed during play, but afterwards during reflections and debriefing.
3.2 Simulated Models from Theory

The above discussed theories and concepts inform us about the generalities of this simulation game. However, it’s just the outset of the theoretical framework. There are more concepts to explore, particularly for a cyber crisis game focused on decision-making under uncertainty. As discussed above, the simulation game includes a simulated model. This model will consist of multiple models, informed by both theory and practice. In the following section, the first model will be addressed: situation awareness, as this concept precedes decision-making. Second is decision-making under uncertainty. Together, these models form the simulated models from theory.
3.2.1 Situation Awareness

Discussed in the previous paragraph, the simulation game involves a simulated model from reality and concept. From a theoretical point of view, one model that particularly offers a bridge between simulation games and decision making is situation awareness from Endsley (1995). In the following paragraph this concept is explored in more detail and explains how it influences the simulation game design. First, the theory is explained briefly, including why this model is particularly helpful in designing the simulation game, which includes the angle that the model takes on decision making. Secondly, three main models that involve situation awareness are discussed to be implemented in later stages: Situation awareness, Team situation awareness and Sources of Information. Together these add to the simulated model from theory that is created for the simulation game. These will be enriched with models from the application domain in later stages.

Background and Relevance

Situation awareness (SA) is a model stemming from military academia, often used for the design of (military) display systems (Endsley, 1995). Endsley (1995) defines situation awareness informally as “knowing what’s going on” and, more formally, as “the perception of the elements in the environment within a volume of time and space, the comprehension of their meaning and the projection of their status in the near future” (p. 36). In a (somewhat) recent review, Wickens (2008), concluded that the definition of situation awareness is still expressed in very similar terms to the formal one used by Endsley in 1995 and therefore has remained relevant.

Endsley (1995) stresses that true SA, involves more than just being aware of the numerous pieces of data. It requires a more advanced levels of situation understanding and a projection of future system states in the light of the operator’s goals. Additionally, she adds some clarifying statements to her definition of SA. The first is that SA, is a state of knowledge and not the processes which lead to this state, as described in the informal definition “knowing what’s going on”. The process is then referred to as situation assessment or achieving, acquiring, or maintaining SA. A second statement regarding her definition is that SA does not encompass all of a person’s knowledge. It only refers to the portion related to the state of the dynamic environment. Therefore, any supporting documents like procedures, plans, checklists etc. – even though important, as described in chapter 2 – are not part of SA.

Even though the use of Endsley’s model in this thesis lies outside of designing display systems, it suites the to be simulated cyber crisis well. Endsley addresses the importance of SA in decision-making in dynamic environments and utilizes a model of decision-making that takes SA into account. As will become clear in chapters 4 and 5, cyber crisis is a highly dynamic and complex environment. In other words, the model of situation awareness describes the domain of cyber crisis decision-making fairly well. The next section focuses on Endsley’s model and its components, and specifically discusses how they will be represented in the simulation game design.

In addition to forming the basis for decision-making as an important input, SA impacts also the process of decision-making itself. Manktelow and Jones (1987) reviewed literature concerning deductive problem solving and showed through numerous studies, that context of the problem largely determines the ability of individuals to adopt an effective problem-solving strategy. In other words, it is the situations specifics, that determine which mental model is created and also the following problem-solving strategy. And in a way this fits the dynamic environment view that SA has. Paragraph 3.3 follows-up on this view on decision-making in more detail.
Endsley’s (1995) model of Situation Awareness

Endsley sees the need to incorporate SA concepts into human factor design efforts, due to the critical role SA has in decision-making, especially in complex and dynamic environments. Therefore, she chose to create a model which shows the relation between SA, decision-making and performance. Endsley’s (1995) model is descriptive of situation awareness and combines the aspects that influence the SA building. In other words, it synthesizes the different sources of information for situation awareness. Figure 7 depicts Endley’s Model of situation awareness in dynamic decision making. It shows the place which situation awareness takes in the decision-making process. Additionally, according to this model, a person’s perception of the relevant elements in his or her surroundings are, from any source of information, form his or her situation awareness. The sources of information model will be discussed in section 3.2.4. However, what becomes clear from the model is that a decision-maker takes information from both task/system and from individual factors.

In other words, according to the model, a combination of factors as the state of the environment, Task/System factors, Goals and Objectives, Expectations and Individual Factors influence SA. Endsley differentiates three different levels of SA (the higher the better the SA). Each of the three hierarchical phases is described here briefly (Endsley, 1995):

**Level 1 SA: Perception of the Elements in the Environment.** The first step in achieving SA. Involves perceiving the status, attributes, and dynamics of relevant elements in the environment.

**Level 2 SA: Comprehension of the Current Situation.** This level of SA is based on a synthesis of the level 1 elements. Therefore, it goes beyond being aware of the present elements, and adds an understanding of the significance of these elements in the light of the operator goals. Endsley (1995) mentions that experience come in play to tie the elements together, forming a holistic picture of the environment and comprehending the significance of objects and events.

**Level 3 SA: Projection of Future Status.** This final level builds on the knowledge and status and dynamics of the elements and the comprehension of both of the situation. In other words, this level builds on level 1 and level 2 SA. Being able to project the future status – at least in the very near term – provides knowledge (and time) necessary to decide on the most favorable course of action to meet objectives.

SA, therefore, is more than the mere perception of information about the environment. It also involves comprehending the meaning of that information in a holistic form, taking goals into consideration, and providing projected future states of the environment that are valuable for decision-making. This makes SA a construct that takes a range of underlying human processes in consideration. The model of SA can apply across a wide range of application areas. Figure 7 depicts Endley’s model.
When taking Figure 7 as a discussion image, it not only shows where SA is situated in the decision-making process, but also demarcates SA clearly in this process. There are couple of important considerations according to Wickens (2008), relating to SA.

**SA is not the same as taking action or performance.** In other words, observing, understanding and making projections of the situation is different from actually taking action to this situation. Decision-making and Performance are also influenced from other factors. One can argue that good SA is desirable, but is not a guarantee for good performance. Wickens (2008) mentions the example of an operator with excellent SA of a system but lacks the knowledge of procedures to fix the problem or may not have the execution skills to apply this knowledge.

**SA is only applicable in dynamic situations where variables are changing.** SA therefore is not the same as long-term memory knowledge. In a highly dynamic situation where variables change, a good SA is required.
Influence on Design

So far, the model of Endsley, and its components have been discussed. But how does it inform the conceptual simulation game design? As described in paragraph 3.1 a simulation game exists of multiple simulated model from reality and concept. Endsley’s (1995) model suites well, as it is specifically created for dynamic situations and includes decision-making. This section describes the elements from the discussed model that will be incorporated in the simulated model.

Individual Factors. Endsley (1995) speaks of individual factors that influence the ability to acquire SA, given the same data input. This is hypothesized to be a function of an individual’s information-processing mechanisms, influenced by abilities, experience, and training. Simulation games can offer exactly a form of training to practice and improve abilities and offer a form of experience. Additionally, during the play of the game, participants are exposed to other participants including their abilities and experience and are able to reflect on their own. Therefore, factors like information handling mechanisms, long term memory and automatism are addressed implicitly. In other words, the participants bring these factors into play, but are not necessarily addressed during play, but afterwards during reflections.

Additionally, the individual can have certain preconceptions and objectives that can act and filter the environment in forming SA. According to Randel et al (1996) more skilled individuals are able to go through the SA levels a lot quicker than less skilled equivalents. However, the same built up towards SA is still maintained. To keep the learning value existent in the simulation game, also for experienced players, a complete new world is created. In this simulated world factors are leveled out as much as possible by implementing fictitious organizations, roles and objectives. In other words, ones with little knowledge can learn from the provided information and ones with lots of knowledge have to adjust to the knowledge provided. These are described in more detail in chapter 7.

Situation Awareness – Decision Making – Performance Loop. In the Situation Awareness model, the loop starts with state of the system then goes into SA followed by decision-making, where the performance of the actions changes the state of the system again through feedback. This exact loop will be implemented in the simulation game design. Whereas information comes from multiple sources, participants will have to determine what is going on and how to act upon it and facilitators provide responses as feedback. An important notion is that the feedback provided from the facilitators is not a reflection on if they did well or not, it is merely a response to their actions. Participants will evaluate the returned responses in terms of performance levels.

Task / System Factors. Like individual factors, these task/system factors influence SA, decision-making and performance. The SA model then takes together the Task and System Factors. However, in light of this thesis, it eases the discussion to take them apart. The reason is that factors from tasks and factors from systems are different in the context of a simulation game. In terms of Task Factors, Endsley (1995) mentions stress and workload and complexity as factors which influence the loop discussed in last section. Within the game, events and tasks (and especially the combination of these) are designed to challenge the participants. In other words, these elements are created in such a way which is intended to increase stress and complexity. However, it is important that the separate elements are not evaluated for their complexity and stress levels, but the game as a whole. The designed tasks and events are discussed in chapter 7.

Secondly, there are the System Factors, these are more relevant from a systems design point of view. In other words, these factors need to be taken into account when designing display and other types of interfaces for operators. For the design of the Cyber Crisis simulation game, also system factors are also simulated by making use of an information system, which is the main communication tool during the game. This information system is used between participants and facilitators to convey messages and
information, in contradiction to the more static playing cards. Important to note is that this information system is considered as one of the game elements, and is merely intended to assist in increasing reality and reduce complexity for facilitators by streamlining communication and gathering information to reflect upon in later stages. This tool therefore helps facilitators in implementing the SA – Decision making – Performance Loop as described in the previous section. Given this, the mentioned information system game element does not follow any of the system factors that Endsley (1995) mentions in her model for the purpose of design, but simulates the existence of such a system.

**Team Situation Awareness**

As described in chapter 2, and will be elaborated upon more in chapter 4 and 5, Crisis decision-making happens in teams. Where Endsley (1995) originally wrote her articles focusing on individual operators, for example of aircrafts, different scholars have taken on the concept of *team situation awareness* (team SA). Team SA has emerged as important in understanding team dynamics, and answers the question: what does each worker know about the understanding and workload of the other, and how is this supported? The most critical notion is how the concept of team SA goes beyond the collective average or sum of SA for the individuals that make up the team (Gorman, Cooke & Winner, 2006; Cooke, Gorman, Winner & Durso, 2007; Cooke, Salas, Kiekel & Bell, 2004). This team SA can be represented as shown in Figure 8. Overlap between each team member's SA will exist. And this combination or a subset of information constitutes much of the team coordination. This coordination can happen in different ways like verbal, written etc. But more importantly, it is the shared Situation Awareness of the state of the environment which determines the quality of the team coordination.

![Figure 8: Team situation awareness (adopted from (Endsley, 1989))](image)

**Influence on Design**

Similar to the model of SA in dynamic systems, earlier given, will the model of team situation awareness informs the conceptual design. This model will be represented in the simulated model, by designing the role descriptions and objectives that participants assume, the events and tasks in such a way that team
members are left unaware of some of the information which is given to one player, but not the other. These are also included as a counterpart to the information system discussed above which is “public communications”. In other words, participants will have different descriptions, goals, get personal phone calls and have their own responsibilities during the game. This increases the need for coordination and requires participants to share information as much as possible.

**Sources of Information**

The third and final model related to situation awareness which is represented in the game is *sources of information*. As was mentioned in the section focused on the model of situation awareness, an individual or group synthesizes information from different sources to derive situation awareness from. Cues can be received through visual, aural, tactical, olfactory or taste receptors. Some cues are so subtle that they are registered on a subconscious level only (Endsley & Robertson, 2000). According to Ednsley and Robbertson (2000), SA then comes from three different sources:

1. Direct observation from the real world;
2. Through any Display System;
3. Through verbal and non-verbal communication with team members & others.

A depiction is shown in Figure 9.

---

**Figure 9: Sources of SA information (adopted from (Endsley and Robbertson, 2000))**
Influence on Design

Endsley and Robbertson (2000) state that not in all environments it is possible to directly observe from the real world. In the case of a Cyber Crisis simulation game, this could also prove challenging. The main focus will lie on decision-making, and having direct observations of the reaction is complex. For example, when the public opinion is not happy with the decisions taken by the team, it is not possible to show any emotions of the general public except through information systems. Saying this at this point remains vague, however chapters 4 and 5 will explicate the consequences of decision-making more, which will create more insight in the point made here.

What remains is that information from SA perspective comes from two sources: through display systems which represents the real-world and through communication with team members and others. Chapter 7 will describe these elements in more detail. However, the game design includes:

- Phone calls representing ‘other stakeholders’;
- Information system for communication to their own organization and to the outside;
- Information system which represents outside stakeholders, e.g. newspaper;
- Team members with their own roles and objectives.

3.2.2 Decision-making under uncertainty

In the previous paragraph, the notion was made that it is the situations specifics that determine which mental model is created and also the problem-solving strategy that follows. This view fits the environment of dynamic decision-making which Endsley (1995) has portrayed. Putting this in other words, it depends on the situation at hand which problem-solving strategy is taken. As a consequence, the simulation game will not address any problem-solving strategy in particular, but leaves this open for participants to formulate given the available information. However, there are still concepts to address regarding decision-making. In the last paragraph, decision-making was merely a part of a larger model which is specifically formulated to put situation awareness in perspective. It does not address important background of dynamic decision-making in much detail, which is the focus in this paragraph.

Specifically, this paragraph explores the underlying theoretical concepts of the notion made on decision-making. This involves Naturalistic Decision Making and one of its models Recognition Primed Decisions (RPDs). Included in the section is a discussion on how much RPDs shape the course of the simulation game and how much decision alternatives are implemented by design. Furthermore, this paragraph focuses on uncertainty in decision-making, which enables its simulation in following stages.

Naturalistic Decision-making

Decision-making in dynamic environments as described by Endsley (1995) has its own theories and models. Additional to the prescriptive and normative approaches to describe decision making is an approach that characterizes by understanding how people actually make decisions in the real world (Liptshitz et al., 2001). This view on decision-making is called Naturalistic Decision Making (NDM) (Klein, 2008). It is a descriptive approach that focuses on decision-making under demanding situations (Marold et al., 2012). In other words, it fits dynamic environments like cyber crisis situations. Important characteristics of NDM are time pressure, uncertainty, vague goals, high stakes, group and organizational constraints, changing conditions, and varying amounts of experience. Randel et al. (1996) characterize naturalistic decision making as dynamic and has continually changing conditions. Since conditions are dynamic, goals and objectives are likely to change with new information, this possibly also includes priorities.

Essential in this theory on decision-making is studying the information people are looking for and arguments used instead of using abstract models and empirical prescriptions. This approach is also very fitted with simulations as it is characterized by field studies, which is what basically happens with prototype testing. This method of describing the decision-making offers possibilities for feedback to the
participants. Zsambok, 1997:4) states a short-hand definition of NDM as ‘… the way people use their experience to make decisions in field settings.’ Similarly, it is believed that in naturalistic environments with time constraints, changing conditions and stress, recognition-primed decisions (RPDs) take place (Klein, 1989).

**Recognition Primed Decisions**

Naturalistic Decision making yielded different decision making models. One particular of interest for this thesis is the recognition-primed decision making (RPD) by Klein (1997). The RPD model describes decision making in terms of the cognitive processes employed by decision makers during crisis situations, including time pressure, complexity, hazard, dynamic and limited time and information. Decisions within the RPD model are made based on experiences and knowledge from the decision-makers, which as the name pertains is about recognizing a situation as typical and recall the appropriate decision to deal with it effectively. What becomes clear is that RPD is then not particularly focused on generating different types of options (like in brainstorming) but that there is a strong focus on classification of the situation (Randel, 1996). Within this line of reasoning, opportunities for improvement arise by increasing the experience of decision-makers to recognize and deal with situations. Therefore, it is argued that training can provide this building of experience (Crinchton et al., 2000). But it is also argued by Klein (1998) that intuitive decision-making, based on pattern matching and recognition of familiar and typical cases, can be trained by increasing the decision maker’s experience and knowledge base.

This leaves room to develop training programs that incorporate exercises and realistic scenarios so that decision makers have the opportunity to expand their repertoire of patterns (Stokes, Kamper and Kite, 1997). Therefore, creating these training opportunities in simulations, improves by learning to deal with different types of situations, by adding it to the individual repertoire of the decision-makers. This links back to Endley’s (1995) model on situation awareness, which mention individual factors as experience, ability and training as influence for decision-making.

**Influence on design**

RPDs, inform us that decisions are made based on experiences and knowledge from decision-makers, and is about recognizing a situation as typical and recall the appropriate decision to deal with it effectively. It focuses more on classification of the situation (read SA). These abilities and experiences can be trained. As described in section 3.2.2, the simulation game implements a level of knowledge in the form of a fictitious world (also fitting the narrative principle), to lower possible knowledge and experience gaps between participants. Included in the knowledge within the game is the formulation of decisions that participants can take. However, here lies room for discussion in terms of how much of the possible decisions do you want to prescribe? Too little, and the simulation game might become complex for participants and unmanageable for facilitators. Too much, and the simulation game might be too unrealistic or too restrictive. On the other side, one also has to take into consideration that participants have different background, therefore a balance between serving these backgrounds, especially on the ones they lack, without over explaining and taking the flow out of the simulation game.

Therefore, taking these aspects into consideration the following principle is maintained in designing decisions in the simulation game:

- To meet needs for participants that lack understanding in the decision making in crisis situations and to reduce complexity for both participants and facilitators, there is an action list available which contain actions that are available for them to take. These will be derived from the application domain and address the cyber crisis in the way experts and scholars see it. This includes real scenarios. The application domain is discussed in chapters 4 and 5.

- As RPDs fit the dynamics of a cyber crisis, these will be stimulated by adding a category of “other” playable actions which foster for any situation where the decision-makers decide to take a decision they know from experience but is not “hard-coded” in the simulation game. In this
way, the flow of the game is not disrupted even though the simulation game design did not consider the decision taken.

As a consequence, the game becomes flexible in its communication between participants and the responses that facilitators have to provide. Here the information system discussed in 3.2.2 will play an important role. This system will provide the flexibility that this decision freedom brings. Another important implication is that this game requires an extra facilitator. Next to the facilitator that observes actions and debriefs the players, there will be a facilitator that simulates the 'outside world' by responses and provided information. But what then does this facilitator provide? In the next section, the influences of uncertainty in the decision-making is discussed.

Uncertainty in Decision-making

Uncertainty is one of the most often used terms when describing Crisis situations, as was discussed in chapter 2. Additionally, what will be elaborated more in chapter 5, the cyber crisis domain crosses geographical, functional and time boundaries. These types of crises are called transboundary crises (Boin, 2009). These characteristics even add more uncertainties for decision-makers. First there is the uncertainty of, for example, where the threat is coming from, how long it will persist, and the effectiveness of the taken measures. Second, the ripple effect caused by a single event can cause unmanageable damages across customers, patterns and internal functions. There is no need to go into more detail than this at this stage. As the specifics of the application domain are part of chapter 5, they will be discussed in greater detail there. The point here is, there is a great involvement of uncertainty in cyber crisis.

Therefore, when designing a simulation game specifically for cyber crisis decision-making, uncertainty needs to be implemented. It is important to go into the details of the what, who, where of the cyber crisis application domain, an important way to increase the reality level of the simulation game. However, before it is possible to derive uncertainties from the application domain and to be able to simulate uncertainty, it is important to know the foundations of uncertainty, specifically in decision-making.

What, then, is uncertainty? Liptshitz and Strauss (1997) offer extensive research focused on uncertainty in decision making. Their definition of uncertainty falls in line with the Naturalistic Decision-making perspective, as “a sense of doubt that blocks or delays action”. These doubts can be specified in three broad dimensions: issues, sources and inclusiveness and subjectiveness.

Within the domain of the issues Libshitz and Strauss (1997) identify three categories:
- The nature of the situation;
- The alternative of the decision;
- The potential outcomes.

The second dimension mentioned are the specific sources, in other words where the uncertainty comes from. Here a strong link between information and uncertainty is drawn by Libshitz and Strauss (1997). Uncertainty in terms of information is associated as the perceived gap between available information and the information that a decision-maker would like to have. Libshitz and Strauss identify three different sources:
- Incomplete information;
- Inadequate understanding;
- Overwhelming information or undifferentiated alternatives.

A third dimension mentioned is that doubt is both inclusive and subjective. With inclusiveness Libshitz and Strauss mean that there no particular form of doubt exists, it just does. Subjectivism refers to the
fact that each individual experience different forms of doubts. But even though that doubts are both inclusive and subjective, they result into common effects on decision-making. Examples given are hesitance, indecisiveness or procrastination.

**Influence on Design**

Uncertainty is defined as “a sense of doubt that blocks or delays action”. This means that any simulation of uncertainty has to create a similar emotion. Given the inclusiveness and subjectivisms, that there is no particular form of doubt and that each individual experiences it differently, this might be challenging. However, the two other dimensions offer the characteristics that form the base in simulating this sense of uncertainty. The issues and sources discussed above are implemented in the simulation game design as follows:

- **The nature of the Situation.** Participants are unaware of the entire story and are expected to uncover the unknowns.
- **The alternative of the Decision.** There are different alternatives given which the team can choose from, additional to an “other” category.
- **The Potential Outcome.** There is no particular script that tells where the story should go. The game is all about the decision-makers creating a narrative themselves. An important notion that has been implemented is: There is no wrong or right. In the end, they decide if things went well or not, but this is not the main goal.
- **Incomplete information.** Players will be provided information from different sources, but this will never be complete and straightforward. Messages are designed to be vague, but informative enough to keep the flow of the game going. More detail on these in chapter 7.
- **Inadequate understanding.** Together the participants have to find out what happened. The briefing is kept vague to force participants to formulate their own actions, instead of being dictated by the simulation game. Important is that inadequate understanding should only be the case for their actions, and not for game elements.
- **Overwhelming information or undifferentiated alternatives.** Events designed (see chapter 7) are sometimes given simultaneously, therefore require preparation and action from game participants at the same time. Also, as described in paragraph 3.2.3 there are different sources of information, which possibly offer their information at the same time.

**Group decision-making under uncertainty**

When decision-making moves from the individual level to the group level, social interactions and contexts can influence uncertainty and decision-making. Social influence is the process in which individual judgments, behavior and attitudes change in presence of other people (Marold, 2012). Even though the focus of this thesis is more on decision-making under uncertainty, specifically in the light of a cyber crisis, it is of value for the facilitators to know these events to happen.

One aspect in when the individual decision-makers need to assess or make predictions about the expertise of other group members. This particularly is the case when information which is required is not completely accessible and understandable. These kind of situations in uncertainty in group decision making are described by Hanson (1996). In these uncertain situations, decision-makers rely on experts that advise them, which additionally builds up on the uncertainty. In other words, it is unclear for the decision-makers if the information provided from others, especially the experts, is reliable. According to Hanson (1996) there are three different aspects to this uncertainty:

1. When experts are recognized but decision-makers disagree;
2. When experts are not recognized;
3. Whether experts are reliable at all or not.
A second class in which social influence have effect in decision-making comes from the social psychology, and are called decision-making biases. Jones and Rolfs (2000) mention several examples of group-decision biases:

- The false consensus effect: overestimating the level of agreement from others;
- Groupthink: minimizing conflict without critically testing, analyzing and evaluating ideas;
- Group polarization: more extreme decisions when in a group than when independent.

A third class is strategies with dealing with uncertainty. Libshitz ad Strauss (1997) identify three main classes of tactics that are used to cope with uncertainty:

- Tactics of reduction: including retrieve additional information or increase predictability;
- Tactics of acknowledgement, involving taking uncertainty into account when selecting decisions;
- Tactics of suppression, which is basically denying of uncertainty.

### Influence on Design

This section touches lightly on group decision-making uncertainty, and have as goal to inform facilitators in observing the game. As decision-making practice is one of the goals in this thesis, it is important to include mechanisms that are discussed here. Therefore, the concepts touched in this section are added in the observations section in the facilitators document.

### 3.2.3 Conclusion: Simulated Models from Theory

The paragraph 3.1 describes the general simulation game / learning aspects of the proposed game. But what is actually simulated? Paragraph 3.2.1 and 3.2.2 have described the simulated models in more detail. This is depicted in dashed box in Figure 10, *simulated models from reality and concept*. As discussed in Chapter 2, preparing senior-managers should not focus on the tactical level, but on situations that cannot be anticipated, requiring-programmable responses. Combined with that uncertainty is a very important characteristic of crisis situations, the needed simulated models from theory are *decision-making under uncertainty*. The missing cyber crisis characteristics, or models from reality, need to be added from the application domain in the next part.

### Model of Situation Awareness in Dynamic Decision-making

Situation awareness is the perception of the elements in the environment within a volume of time and space, the comprehension of their meaning and the projection of their status in the near future. Even though the origin of SA comes from the design of military display systems, it suites the to be simulated cyber crisis well as it involves SA in a model with decision-making and is specifically meant for dynamic systems. Implementing the models has the following influences on the conceptual design.

#### Individual Factors

Abilities, experience and training are addressed by playing the game. Additionally, participants can learn from other players. Therefore, these factors are more implicitly included in the game design. Secondly, to keep learning existent for every participant, a complete new world is created. In this world fictitious organizations, roles and objectives are introduced to level out differences in experience as much as possible between participants.

#### Situation Awareness – Decision Making – performance Loop

Information comes from multiple sources, participants will have to determine what is going on and how to act upon it and facilitators provide responses as feedback. Participants evaluate themselves if they performed well.

#### Task Factors

Events and tasks are designed to challenge the participants. An important note is that separate elements are not evaluated for their complexity and stress levels, but the game as a whole.
System factors. These are simulated by the use of an information system, which is the main communication tool during the game. This system is used between participants and facilitators to convey messages and information, in contradiction to the more static playing cards.

Team Situation Awareness
Role descriptions, objectives, events and tasks. Team members are left unaware of some of the information which is given to one player, but not the other. This increases the need for coordination and requires participants to share information as much as possible.

Sources of Information
Sources of information. In the conceptual design information comes from two sources: display systems which represents the real-world and through communications with team members and others. And include:

- Phone calls representing ‘other stakeholders’;
- Information system for communication to their own organization and to the outside;
- Information system which represents outside stakeholders, e.g. newspaper;
- Team members with their own roles and objectives.

In paragraph 3.2.1 three models of situation awareness were explicated. Paragraph 3.2.2 focused on decision-making under uncertainty. Specifically, it focused on Recognized Primed decisions, uncertainty in decision-making and group decision-making under uncertainty. The following influences on design are discussed:

Recognition Primed decisions.

- An action list is available that contains actions that are available to take. The contents of these possible decisions are derived from the application domain address the cyber crisis in the way experts and scholars see it, including real scenarios. This list offers participants that lack understanding in decision making possibilities, to keep the game going. Additionally, it reduces complexity for both participants and facilitators.
- As RPDs fit the dynamics of a cyber crisis, these will be simulated by adding a category of “other” playable actions which foster for any situation where the decision-makers decide to take a decision they know from experience but is not “hard-coded” in the simulation game. In this way, the flow of the game is not disrupted even though the simulation game did not consider the decision taken.

As a consequence, the game becomes flexible in its communication between participants and the responses that facilitators have to provide. Here the information system discussed in 3.2.2 will play an important role. This system will provide the flexibility that this decision freedom brings. Another important implication is that this game requires an extra facilitator. Next to the facilitator that observes actions and debriefs the players, there will be a facilitator that simulates the ‘outside world’ by responses and provides information.

Uncertainty in Decision-making.

Uncertainty is defined as a “sense of doubt that blocks or delays action”. The issues and sources of uncertainty discussed above are implemented in the simulation game design as follows:

- The nature of the Situation. Participants are unaware of the entire story and are expected to uncover the unknowns.
- The alternative of the Decision. There are different alternatives given which the team can choose from, additional to an “other” category.
• **The Potential Outcome.** There is no particular script that tells where the story should go. The game is all about the decision-makers creating a narrative themselves. An important notion that has been implemented is: There is no wrong or right. In the end, they decide if things went well or not, but this is not the main goal.

• **Incomplete information.** Players will be provided information from different sources, but this will never be complete and straightforward. Messages are designed to be vague, but informative enough to keep the flow of the game going. More detail on these in chapter 7.

• **Inadequate understanding.** Together the participants have to find out what happened. The briefing is kept vague to force participants to formulate their own actions, instead of being dictated by the simulation game. Important is that inadequate understanding should only be the case for their actions, and not for game elements.

• **Overwhelming information or undifferentiated alternatives.** Events designed (see chapter 7) are sometimes give simultaneously, therefore require preparation and action from game participants at the same time. Also, as described in paragraph 3.2.3 there are different sources of information, which possibly offer their information at the same time.

---

**Simulated Models from Theory**

---

### 3.3 Conclusion: theoretical concepts and their influence on design

This chapter covered the important theoretical concepts that were identified in chapter 2 as important for dealing with crises. These were simulation games, learning and decision making under uncertainty. This chapter took a dive into these concepts but also supporting underlying mechanisms, like the models for
situation awareness and especially addressed how these theoretical concepts can be linked to the design of the proposed simulation game.

The most important aspect is highlighted in this chapter: how each of these concepts influence the conceptual design, without touching on the theory once more. It answers the second part of the first sub-question: How can these be linked to the design of a simulation game that supports senior-managers in preparing for crisis decision making?

The combination of the discussed elements and theories offer a blueprint for the conceptual design as given, in which the application domain provides input to in the next chapters, eventually completing the conceptual simulation game design. The paragraphs in this chapter have discussed the basis of the simulation game from the outside in, starting with simulation games, and filling in the to be simulated model with theoretical concepts from situation awareness and decision-making under uncertainty. Two figures are constructed based on these theoretical concepts, which are discussed in paragraphs 3.1 and 3.2, including the influences for design that were given. These figures combine the different elements and show how they work together.

Together, the combination of the elements forms the blueprint of the conceptual design. To make an analogy, we know how big the rooms in the house are, that we want chairs, tables and a cozy kitchen. Additionally, with the simulated models, we know which general functions will be included in the house, like eating, relaxing etc. However, it clearly misses identity. By adding the details, the colors, specific furniture etc., the game will truly be the house of our dreams. Speaking in simulation game terms again, clearly missing are the simulated models from reality. In combination with the theoretical aspects discussed below as design concepts, these will provide the specifics to make this a cyber crisis simulation game. For this the application domain is explored in the next three chapters, starting with the view from practitioners.

Given this extensive chapter on theoretical concepts, it is helpful to provide a list of theoretical concepts and their influence on the simulation game design. There are concepts mentioned in the table which have no place in the two figures in paragraphs 3.1 and 3.2, as well as there are concepts that are in the figures but not mentioned in table 2. The models used in the figures serve as a blueprint for the conceptual design and are predominantly set, unless proven unfeasible during tests or in conflict with design choices. However, the concepts in table 2 are used again when discussing design choices. This list is used as a reference in the following chapters but foremost returns in Chapter 7, when the conceptual design is explained in greater detail. From the theoretical concepts discussed in this chapter the following list is constructed:

Table 2: Reference for the theoretical concepts

<table>
<thead>
<tr>
<th>No.</th>
<th>Theoretical Concepts</th>
<th>Source</th>
</tr>
</thead>
<tbody>
<tr>
<td>SG1</td>
<td>Simulation games offer a flexible and safe environment in which rare and uncertain situations can be simulated.</td>
<td>Borodzicz &amp; van Haperen (2002)</td>
</tr>
<tr>
<td>SG2</td>
<td>Simulation games use models to represent the processes and objects and how they relate to their environment.</td>
<td>Stoppelenburg et al. (2012), Klabbers (2009)</td>
</tr>
<tr>
<td>SG3</td>
<td>SG is a model that replicates the dynamics of a system and to analyze the system at interest.</td>
<td>Stoppelenburg et al. (2012)</td>
</tr>
<tr>
<td>SG4</td>
<td>Simulation game: there is a (simulated) model of a (real or conceptual) system and there are actors, having different roles, which try to achieve specific goals within a set of rules.</td>
<td>Klabbers (2009)</td>
</tr>
</tbody>
</table>
### Learning from Simulation Games

| Learn1 | Within simulation games, the learning preference of participate, practice and exploration are simulated and developed. Additionally, when simulation games are played in a group in a single room, the learning preference of adopting best practices is also added. | Simmons (2008) |
| Learn2 | Learning happens through four different phases in a cycle: having a concrete experience, followed by observation of and reflection on that experience, which leads to formation of abstract concepts (analysis) and generalizations (conclusions), which are then used to test hypothesis in further situations, resulting in new experiences. By repeating this cycle, the new learned behavior can be internalized. | Kolb (2014), Thatcher (1990) |
| Learn3 | The number of Kolb cycles, together with the very important debriefing form the whole experience. | Thatcher (1990) |
| Learn4 | Three types of learning are present in simulations: learning the facts, learning the process and learning the relative costs and benefits. | Thatcher (1990) |
| Learn5 | Emotions are important aspect for learning in simulations | Thatcher (1990) |
| Learn6 | Three important stages exist within the process of reflection: returning to the experience, attending to feelings and re-evaluating the experience. | Boud, Keogh and Walker (2013) |
| Learn7 | Having a designed response self-evaluation questionnaire available, forces participants to consider important points to simulation, before their experience is under snowed during general discussion. | Thatcher (1990) |

### The role of the facilitator

| FAC1 | The facilitator has to learn not to interfere. | Thatcher (1990) |
| FAC2 | Sometimes the facilitator is needed to guide participants to new aspects of the game. But most importantly, facilitators have to intervene when problems occur, that lie beyond the control of the participants, which could halt learning. | Stoppelenburg et al. (2012) |
| FAC3 | It is the task of facilitators to recognize dysfunctional patterns and discuss these, to create a safe environment for participants. | Stoppelenburg et al. (2012) |

### Creating a realistic and safe environment with narratives

| NAR1 | Simulation games are a narrative space. Within this narrative space the two worlds of the narrator and the participants will meet and an exchange of ideas, experiences and feelings happen. | Bruer (2008) |
| NAR2 | Favorable characteristics from working with narratives: equality between participants, an open climate, and the absence of taboos. | Abma (2006) |
| NAR3 | The evolvement of concern, emotions, wants and needs keep people involved. | Abma (2006) |

### Situation Awareness

| SA1 | Situation awareness: “The perception of the elements in the environment within a volume of time and space, the comprehension of their meaning and the projection of their status in the future.” | Endsley (1995) |
| SA2 | It is the situations specifics, that determine which mental model is created and also the following problem-solving strategy. | Endsley (1995) |
| SA3 | SA is more than the mere perception of information about the environment. It also involves comprehending the meaning of that information in a holistic form, taking goals into consideration, and providing projected future status of the environment that are valuable for decision-making. | Endsley (1995) |
| SA4 | Two important considerations, relating to SA.  
1. SA is not the same as taking action or performance.  
2. SA is only applicable in dynamic situations where variables are | Wickens (2008) |
### Changing

**SA5**  
The individual can have certain preconceptions and objectives that can act and filter the environment in forming SA. More skilled individuals are able to go through the SA levels a lot quicker than less skilled equivalents.  
---  

**SA6**  
In the SA model, the loop starts with *state of the system* then goes into *SA* followed by *decision-making*, where the *performance of the actions* changes the state of the system again through *feedback*.  
---  
Endsley (1995)

**SA7**  
In terms of Task Factors, *stress and workload* and *complexity* are mentioned as factors which influence the loop discussed in SA6.  
---  
Endsley (1995)

### Team Situation Awareness

**TSA1**  
Team SA goes beyond the collective average or sum of SA for the individuals that make up the team. Overlap between each team member's SA will exist. And this combination or a subset of information constitutes much of the team coordination. This coordination can happen in different ways like verbal, written etc. But most important it is the shared Situation Awareness of the state of the environment which determines the quality of the team coordination.  
---  

### Sources of Information

**Inf1**  
Cues can be received through visual, aural, tactical, olfactory or taste receptors. SA comes from three different sources:  
1. Direct observation from the real world  
2. Through any Display system  
3. Through verbal and non-verbal communication with team members and others  
---  
Endsley and Robbertson (2000)

### Decision-making under Uncertainty

**DM1**  
Important characteristics of Naturalistic Decision-making are *time pressure, uncertainty, vague goals, high stakes, group and organizational constraints, changing conditions, and varying amounts of experience*.  
---  
Marold et al. (2012)

**DM2**  
Naturalistic decision making is dynamic and has continually changing conditions. Since conditions are dynamic, goals and objectives are likely to change with new information, this possibly also includes priorities.  
---  
Randel et al. (1996)

**DM3**  
Essential for NDM is studying the information people are looking for and arguments used instead of using abstract models and empirical prescriptions.  
---  
Randel et al. (1996)

**DM4**  
Decisions within the Recognition Primed Decisions model are made based on experiences and knowledge from the decision-makers, which as the name pertains is about recognizing a situation as typical and recall the appropriate decision to deal with it effectively.  
---  
Klein (2008)

**DM5**  
RPD is not particularly focused on generating different types of options but that there is a strong focus on classification of the situation.  
---  
Randel (1996)

**DM6**  
Intuitive decision-making, based on pattern matching and recognition of familiar and typical cases, can be trained by increasing the decision-maker’s experience and knowledge base.  
---  
Klein (1998)

### Uncertainty in decision-making

**UN1**  
Uncertainty: “a sense of doubt that blocks or delays action”. These doubts can be specified in three broad dimensions: *issues, sources and inclusiveness and subjectiveness*.  
---  
Libshitz and Strauss (1997)

### Group decision-making under Uncertainty
When decision-making moves from the individual level to the group level, social interactions and contexts can influence uncertainty and decision-making. Social influence is the process in which individual judgments, behavior and attitudes change in presence of other people. These include: assess or make predictions about the expertise of other group members, decision-making biases and dealing with uncertainty.

PART II: Application Domain

Let's go back to the goals again, the simulation game has the purpose to give senior-managers a training tool to make them aware of cyber crisis concepts and important mechanisms and enables them to practice decision-making under uncertainty. Part I left off with the blueprint for the conceptual design. In other words, we know which mechanisms, models and theories are applied in the background to reach the goals that are set out including their influence on the conceptual design. This however, does not come close to a completed game yet. So far, generalizable elements from theory are used to build up the game, but could still be any type of game when slightly adjusted. In this part the sub-question *what are necessary elements and functions of a simulation game to support senior-managers for cyber crises* is answered. In other words, these chapters aim to gain an understanding on what the most important aspects of cyber crises are and how these are different from other types of crises.

Coming back to the research paradigm from Winter (2008) on design research, the design of the simulation game still lies in the generalizable and does not solve anything in practice at all. This brings us to Part II, to implement the specifics of the problem area the participants are dealing with to the general simulation game and complete the conceptual design. It is the moment that we move from the right side of the Hevner cycles (knowledge base) to the left side's application domain. In other words, the game design should build on the experiences and knowledge from the practitioners to be able to 1) create a simulated world in which the game evolves around, 2) inform the design on important mechanisms and processes and 3) inform the design on the requirements to make the simulation game successful in the application domain. These functions are followed from a number of theoretical concepts mentioned in Chapter 3, which will be mentioned in more detail in the following chapters.

As depicted in Figure 1, it is this moment when the first steps of the game design methodology, from Stoppelenburg et al. (2012), are introduced. The three chapters in Part II will focus on describing these design steps in detail and inform the conceptual design in their own way are:

**Concepts and Models from the Cyber and Crisis domain.** This first chapter of Part II explores the cyber and crisis concepts to inform the conceptual design on creating a simulated world. In other words, these concepts are represented by the scenario’s, events and tasks in the final game design. Ultimately, the translated concepts and models discussed here bring the participants into a realistic representation of cyber and crisis during the simulation game.

**The Practitioners View on Cyber Crisis.** The second chapter analyzes and gives insight in the important processes and mechanisms involved in Cyber Crisis Decision-making derived from interviews with cybersecurity and crisis experts.

**Requirements for a Cyber Crisis Simulation Game.** This chapter focuses on defining requirements for the simulation game from a practical point of view. These include functional requirements, organizational requirements and simulation game requirements. These requirements scope the focus of the other two chapters and provides guidelines during the construction of the prototype.

Finally, Part II ends with a conclusion that ties the three chapters together, by providing a statement of Simulation Game Requirements. From this, the actual construction of the prototype will be based upon. The requirements given in the conclusion of part II will be used to compare the final design against, and offers tool of reflection.
4. Concepts and models from the Cyber and Crisis domain

From both the theoretical chapters as well as the application domain chapters discussed so far, we have created a high level image of what the game should look like conceptually. These are essential elements in making a simulation game, however, what these are missing is detail about the environment. When taking the perspective of a participant, the details can bring that last bit of realism into the room in which they are situated. To actually make an impact, participants have to believe they are in a crisis situation and not playing a game. Therefore, this chapter explores the cyber and crisis concepts to inform the conceptual design on creating a realistic simulated world. In other words, these concepts are represented by the scenario’s, events and tasks in the final game design. Ultimately, the translated concepts and models discussed in this chapter bring the participants into the wished realistic representation of cyber and crisis during the simulation game. The focus therefore lies on finding and using models and concepts that make a cyber crisis different from other situations. But, to get to this stage, first it is important to understand what crises are and especially which phases exist in crisis management. With this a general understanding of crises is created, which is built upon in the remaining paragraphs of this chapter. This will be discussed in paragraph 4.1. Secondly, paragraph 4.2 discusses the elements that characterize cybersecurity and especially demarcates the option space for particular simulation game elements. In paragraph 4.3 the two perspectives from paragraphs 4.1 and 4.2 are taken and are used to analyze a situation of cyber crisis. Together, a set of design principles, models and elements are derived which assist the design of the simulation game from an application domain perspective.

4.1 The Crisis Model

As discussed in Chapter 3, simulation games offer an environment in which rare and uncertain situations can be simulated (SG1). Therefore, it is important to know what a crisis exactly is to be able to simulate these situations. Additional to the simulation game blueprint created in Chapter 3 and its models from theory, this paragraphs offers a model from the application domain (SG4). In other words, in this paragraph a crisis model is created that is used to simulate a crisis situation in the simulation game. Furthermore, this model also serves as a foundation for a cyber crisis and is used in the following paragraphs of this chapter as well.

4.1.1 Crisis Models

In conceptualizing Cyber crisis, one important notion is to understand what defines a crisis. However, when looking at different definitions of crisis, there seems to be none generally accepted. This has been the conclusion of many scholars over the years (Buchanan, 2013). Jaques (2009) mentioned that the word crisis has bothered for over 30 years, and finds the term poorly defined. Shaluf et al. (2003) additionally notes that there is no universally accepted definition of crisis, and finds it unlikely to emerge in the future. Roux-Dufort (2007) identifies the vagueness of definitions as one of crisis research challenges.

It can be said then that a single definition of crisis does not exist. What might be helpful in the light of designing a simulation game, is a model of crisis (SG2, SG4). This model is then a simulated model from reality. However, when looking at crisis literature, little effort has been spent on modeling crisis situations.

When analyzing the numerous definitions of crisis, two main views seem to be pre-dominantly followed. The first is crisis as an event and the second is crisis as a process. However, these two views are not necessarily mutually exclusive. The following sections discusses definitions used by both views to create some insights on their reasoning, enabling to identify cyber crisis.

4.1.2 Crisis as an Event: unexpected with threat of severe consequences
Many researchers see crisis as the event that causes the unwanted consequences (Mitroff et al., 1996; Coombs, 2007; Pachall, 1992; Lerbinge, 1997). Even though they use a slightly different definition of crisis, they suggest that the event itself is the crisis. This event has been called many different things by scholars: major failure (Howard, 1993), serious accident (Howard, 1993), major occurrence (Howard, 1993; Fearn-Banks, 1996), situation (Shaluf et al, 2003; Regester & Larkin, 1997) and even something (Howard, 1993).

These terms are quite vague. When going into detail on these moments in time is that scholars give subjective characteristics to the definition of crisis. However, scholars agree strongly on two aspects. First, that crises are for that particular moment: sudden (Howard, 1993; Coombs, 2007; Pachall, 1992), unforeseen (Howard, 1993; Coombs, 2007; Pachall, 1992), surprise (James et al., 2011), Unexpected (James & Prideaux, 2003) or rare (Fowler et al., 2007). In other words, involved people did not see the event coming at that moment in time.

The second characteristic on which researchers agree is that crisis forms a threat for organizations (Howard, 1993; Fowler et al., 2007; James et al., 2011; Coombs, 2007; Mitroff, 2005; Shaluf et al., 2003). This threat can be to people, property and/or environment (Howard, 1993), the organization entirely (Mitroff et al., 1996) or more vaguely to the basic structures or the fundamental values and norms of a social system (Dayton, 2004). However, none of the researchers define what they define as threat. An older publication on threat perception defines threat as: “an anticipation of impending danger” (Cohen, 1978, p.95). This notion is quite important, as it implicitly states that decision-makers have to foresee the potential dangers of the event. Another notion of this definition is that there is a probability of consequences, but these do not necessarily need to unfold.

Consequences mentioned by literature are either vague and high-level or on the other side more specific. On the high-level spectrum, there are terms like extensive damage (Howard, 1993) or high consequences (Fowler et al., 2007; Mitroff, 2005; James et al., 2011; Dayton, 2004). Others focus more on the internal workings of the organizational by mentioning disruptions of operations (Howard, 1993; Coombs, 2007) and disruptions of the functioning (Laws & Prideaux, 2005). A more external view mentions consequences like reputational damage (Cooms, 2007; Lerbinge, 1997; Fear-Banks, 1996) and image (Howard, 1993). Both the internal view and the external view have effect to or are linked with consequences like financial (Coombs, 2007; Lerbinge, 1997), profitability (Fowler et al., 2007; Lerbinge, 1997) and even the viability (Fowler, et al., 2007; Mitroff, 2005) of a company.

What becomes clear from the above characteristics found, is that some parts of definitions of crisis pertain everything. Almost all of the above found characteristics are open for interpretation. And will not provide any help in excluding or differentiating crisis types. However, what is important is that the view of crisis as an event by itself is perhaps not entirely correct. Especially when taking cybersecurity into consideration, which will be discussed in paragraph 4.2. When looking at the consequences discussed above, these also involve longer-term consequences, arguably which are excluded in the view of a crisis as an event. In that case, consequences or at least managing consequences are part of the crisis situation which should be addressed as this is most important, not merely the event.

### 4.1.3 Crisis as a Process: Complex due to uncertainty

The above characteristics also show a very inward view of crisis. A crisis is an unforeseen event for a particular organization, there is a threat from a particular perspective and the consequences are seen from the organizational point of view. Even the most external consequence, reputation, is seen from the organizations point of view. Often, the consequences span much further than the vocal organization. Crisis managers also need to incorporate the public view on the company, as consequences also threaten different stakeholders (Pearson & Clair, 1998). Regester and Larkin (1997) even mention it as a situation
of public knowledge which sometimes results in an outrage. Another emotion from outside is disbelief (Dayton, 2004).

However, taking everything in consideration and dealing with crisis situations is not a mundane task, as so much depends on leaders to make the “right decision”. Here the view of crisis as an event is not sufficient to address the problem of crisis management. The research field that focuses on effectively dealing with crisis consider crisis more as a process instead of an event. However, this view does not reject the view of crisis as an event but, broadens the scope of crisis and incorporates the event. Pauchant & Mitroff (1992) describe crisis as a continuum, beginning with an incident, continuing with an accident, followed by conflict, and ending with a crisis. A similar crisis perspective that fits the organizational view more is that of Roux-Dufort (2007), who states that crisis is “a process of incubation that starts long before the triggering event” (p. 106). In other words, the event simply triggers the crisis. This view seems to fit the cyber domain more. For example, a hack on itself (event) is not a crisis. But due to consequences like media attention and customer victims it could be perceived as a crisis.

A significant part of viewing crisis as a process is complexity. Mitroff et al. (2004) see crisis management as a field that has to deal with inherently ill-structured problems. In other words, there is uncertainty about the current state and the desired state. These situations require Naturalistic decision-making, as discussed in Chapter 3 (DM1). Even though uncertainty exist they are still required to make decisions that affect the future, in other words have Situation Awareness (SA1). Additionally, Mitroff et al. (2004) mention that there is a strongly coupled system of problems that interact with each other. Their view on a crisis is then “a highly interactive set of problems, each of which is ill-structured” (Mitroff et al., 2004, p. 179). An important addition to this view is that crises are processes which are extended in time and space, (Shrivistava, 1995) and therefore are no events. However, as many of the internal systems interact with each other the decision-making process during crisis is covered under a veil of fog, in which outcomes are hardly oversee due to its complexity.

Cyber fits the definition of the transboundary crisis. This more modern typology of crises arises from the changing nature of crises and disasters from the last decades (DM1). Boin (2009) suggests that crises of the future will be more transboundary in nature. In his words, these events will last much longer, infect other sectors and functions and change continuously. The main difference is that they cause damage in different ways, posing stronger challenges to the legitimacy of public and private organizations. The transboundary crises are set apart from traditional crises due to the tightly woven web of critical infrastructures that characterize modern society today.

The first characteristic of the transboundary crisis is the crossing of geographical borders. cyber events are clearly not limited to one geographical location (Boin, 2009). A perpetrator can initiate attacks from anywhere in the world, where the same person can start a second attack mere minutes later on a target in a different continent. This makes attribution and pursuit of involved actors a challenge. But, more importantly, threats can stem from anywhere.

Secondly, a transboundary crisis crosses functional boundaries. In case of the Cyber domain, attacks can take place at the point-of-sales in retail stores. However, this affects not only the retail stores but also the financial institutions issuing payment and credit cards. Not to forget the card holders, which could be confronted with fraud and identity theft in all kinds of forms and locations worldwide.

Finally, a transboundary crisis transcends traditional time boundaries. As Boin (2009) states, where a traditional crisis has a clear beginning and end, the transboundary crisis is hard to pinpoint in time. Also this characteristic is shared by the cyber domain. A crisis could be perceived by decision-makers when actual intellectual property is stolen, however this could have started years in advance when a patient perpetrator gained access to the system.
The above characteristics make the transboundary, and therefore also the cyber, crisis hard to manage. First there is the uncertainty of, for example, where the threat is coming from, how long it will persist, and the effectiveness of the taken measures. Second, the ripple effect caused by a single event can cause unmanageable damages across customers, partners and internal functions.

### 4.1.4 Combining the two views: Crisis Model

In this paragraph, a perception of crisis, is described. This model is meant for the game to be simulated during play. Because of the subjective characteristics given by scholars, it can be concluded that crisis is clearly a perception. In other words, crisis is only seen as a crisis when this is perceived this way by the involved. This makes a stronger case for crisis on a continuous scale, where an event is somewhere along this scale, however this does not necessarily mean there is a crisis. For example, when a hack happens in an organization, this does not necessarily is a crisis. Hacks happen on a daily basis, but not all are crises.

Additionally, the view on crisis as a process offers a helpful analytical tool to look at crisis. However, crisis as an event offers valuable characteristics. Therefore, in the light of this research both views cannot be seen separately. Combining the two approaches of crisis results in the general model of crisis depicted in Figure 11. This figure shows that a crisis starts with an incubation time, followed by a triggering event, followed by decision making under a veil of fog and finally the crisis has internal or external consequences.

![Figure 11: Crisis Model, combining both views on Crisis](image)

### 4.2 Characterizing Cybersecurity for a simulation game

In the above paragraph the crisis model is discussed. It combines both views of crisis as an event and as a process. In the light of this research, both offer valuable characteristics that can prove helpful. An example from the cyber domain is that a crisis can erupt from a single event, let’s say a hack. However, this hack could originate from a situation of vulnerability several months before the actual discovery. Next to that, in case of a hack a state of crisis does not necessarily stop after the situation has been brought to normalcy. What this shows is that both views; crisis as an event as well as a process are needed when describing cyber crisis.
What remains untouched so far is the discussion on what cyber crisis is. In line with SG3, stating that simulation games replicate the dynamics of the system and to analyze the system at interest, it is important to replicate cyber crisis. Participants need to be placed within a world of cyber crisis, to be able to practice the decision-making during such crisis. Additionally, a link exists with situation awareness, where it is stated that it is the situations specifics, that determine which mental model is created and also the following problem-solving strategy (SA2). As a consequence, the simulated environment, the events, the scenarios and the tasks need to be created in such a manner that forms the suited mental models. These mental models will be discussed in more detail in Chapter 5. This paragraph focuses on the detailed elements that characterize cyber crisis. In other words, this paragraph focuses on the elements from cybersecurity that need to be focused on when creating a game specifically for cyber crisis. To speak in simulation game terms, these elements from the application domain can be incorporated into the scenarios, events and tasks and have as goal to bring participants into that wanted cyber crisis situation. Important to notice here is that no literature has been found that discusses cyber crisis as a concept. Therefore, the information discussed here discusses important and characterizing concepts from the cybersecurity domain, after which the cyber crisis elements will be discussed in the next chapter.

4.2.1 What is Cyber Security?

Cyberspace

Following (SG2), in which simulation games represent objects and especially how they relate to their environment, it is important to understand what cyber is. As the purpose of this thesis focuses on creating a simulation game, it is best to keep the definition of the cyberspace simple. At the core, cyberspace “is the realm of computer networks (and the users behind them) in which information is stored, shared, and communicated online” (Friedman & Singer, 2014, p. 13). In different words, it is an environment in which the digitized information is created, stored, and shared. Additionally, according to Friedman and Singer (2014) it also comprises of the computers that store and infrastructure that enables transport of this information. These includes mobile networks, the internet of networked computers, intranets, physical fiber-optic cables, and even space-based communications (Friedman & Singer, 2014). Another part of their definition is the users behind the computer networks. Friedman and Singer (2014) stress the importance of their influence on the networks, either in use, as victim, as vulnerability or as attacker. The implications of the connected flow of digital information is that it is not strictly bound to any geographical locations. Even though the machines and people are tied to a place on earth, the information can flow from one place to another in just a fraction of a millisecond. Taking the above perspective in consideration, the scenarios, events and tasks should be geared towards situations which take place inside this cyberspace.

The meaning of Security

Security is a commonly used word. The Oxford Dictionaries (n.d.) defines security as: “The state of being free from danger or threat”. This definition leaves open for interpretation, as danger could be an accident as well but also as result of criminal activity. However, they use three sub-definitions: 1) “The safety of a state or organization against criminal activity such as terrorism, theft, or espionage”, 2) “Procedures followed or measures taken to ensure the security of a state or organization”, 3) “The state of feeling safe, stable, and free from fear or anxiety”. When taking into account these sub-definitions to construct a definition of security, one could summarize it that security is the safe-guarding against adversaries, by implementing security procedures which influence the feeling of safety, stability and anxiety. Once this safe-guarding is challenged, one then desires to return to a state of safety. In the crisis model described above this has been called the return to normalcy. This links back to SG4, which states that participants have to achieve specific goals, where returning to a feeling of safety can be one of those goals. However, there are similar forms of security.
Cyber Security vs. Information Security vs IT Security

Creating a simulation game specifically focusing on cybersecurity requires a demarcation of the terms. This demarcation can be helpful as it focuses the option space for the game elements. In other words, understanding what cybersecurity is compared to these definitions assist in making design choices for game elements.

Similar terms often used in literature are cybersecurity and information security (von Solms and van Niekerk, 2013). Few seem to make a clear distinction between the concepts or the relationship between these two definitions. Von Solms and van Niekerk (2013) explore the definitions of information security and found that cybersecurity concepts spread wider than those of information security.

Von Solms and van Niekerk (2013) begin their exploration by looking into information security. For them the aim of information security is to ensure business continuity and minimizing business damage by limiting the impact of security incidents (Von Solms & Von Solms, 2004). In their view these can be defined in by the following characteristics:

- Information security has the features of Confidentiality, Integrity and Availability. In other words, the CIA triad. However, even though that the CIA triad is still very important, they argue that additional characteristics should be added to fit the changing environment of the computer industry. The ones added to the characteristics of information are: accuracy, authenticity, utility and possession;
- Information can have many forms. This can be either printed paper, conversations, film clips etc.;
- Finally, they believe that information security is not a product or a technology, but a process.

They stress that it is very important to also make a difference between information security and information technology security. Information technology security characterizes itself by: the projection of the actual technology-based systems on which information is stored and/or transmitted. Specifically, this includes “all aspects relating to defining, achieving and maintaining the confidentiality, integrity, availability, non-repudiation, accountability, authenticity, and reliability of information resources” (ISO/IEC 133351, 2004, p.3).

They therefore conclude that because IT security secures the underlying information resources; it is a sub-component of information security. The difference are the additional characteristics as stated by the ISO standards. It is therefore that the overlap is not complete between information and IT security.

In their model of comparing the different definitions, they compare threats, vulnerabilities and assets. The strong difference lies in the assets that need to be protected. In IT security, these are the IT systems and infrastructures. Where in Information Security the IT systems have vulnerabilities, but the most important assets to protect is Information. However, most importantly, information security stretches further than protecting the underlying IT systems. It extends outside the technology and includes any type of information not stored or communicated using IT (Vol Solms & van Niekerk, 2013).

Here is where the difference between IT security, information security and cybersecurity comes in. The assets that need to be protected in cybersecurity can range from the person behind the computer to connected fridges, to interests of a society like the banking networks or critical infrastructure. In other words, these assets include everyone and everything that can be reached through cyberspace.

In turn, in cyber security, according to Von Solms and van Niekerk (2013), the IT systems and Information are the underlying cause of vulnerability. Their main point here is that it is still possible that
the assets that are dealt with in cybersecurity are information and IT systems. However, the most important characteristic of cybersecurity is that all assets that should be protected needs to be protected because of the vulnerabilities that exist as a result of the use of IT systems that form the basis of cyberspace. As a consequence, cybersecurity far extends the boundaries of the information per se as defined for information security. According to Von Solms and van Niekerk (2013) these assets include personal and physical aspects, tangible and intangible, of a human being, societal values or even national industry. Their definition of cybersecurity then is: “the protection of cyberspace itself, the electronic information, the ICTs that support cyberspace, and the users of cyberspace in their personal, societal and national capacity, including any of their interests, either tangible or intangible that are vulnerable to attacks originating in cyberspace.” (Von Solms & van Niekerk, 2013, p. 101).

![Figure 12: The relationship between IT-, Information- and Cyber security (Von Solms & van Niekerk 2013, p.101)](image)

Von Solms and van Niekerk (2013) demarcation between cybersecurity, IT security and information security is very helpful in creating the scenarios, events and tasks. However, when looking at their definition of cybersecurity, it raises some questions that not seem to be addressed: 1) what are we trying to protect? and 2) what are we trying to protect against? These questions can provide a lot more detail, which assist in creating the realistic environment which is aimed for in the simulation game (SG1, SG2, SG3, SG4). Additionally, these details provide crucial details that participants within the simulation game use to classify the situation (DM5), and subsequently adjust their problem-solving strategy to this situation (SA2).

**What are we trying to protect? The CIA triad**

What are organizations trying to protect? As Von Solms and van Niekerk (2013) stated that we should protect anything accessible through cyberspace which has interest for either individuals, organizations or even nation states. Note that in this thesis, the focus lies on the organizational cyber security, and subsequently leaves out the perspectives of the nation states, and the individual home-users. We do take into consideration the individual end-users of corporate networks. Focus makes it a bit easier to discuss what we are trying to protect.
Our computer systems handle, store and send almost everything through corporate networks. Many of this information has some kind of value. Protecting this information is thus of utmost importance. This not only includes internal secrets, and sensitive personal information, but also transactional data reveal important details about the relationships of firms or individuals (Friedman & Singer, 2014).

A very well-known model for Cyber security is the CIA triad (Friedman & Singer, 2014; Bishop, 2003; von Solms and van Niekerk, 2013), as mentioned above.

This abbreviation stands for: Confidentiality, Integrity and Availability and appear to be the highest goals for cybersecurity. Confidentiality is about keeping data private. Confidentiality is often supported by technical measures like encryption and access control, but also by legal protection. Integrity means that data has not been changed without authorization. This requires not just trust, but there must be a confidence that the systems behave as expected. Friedman and Singer (2014) call integrity the subtlest but most important part of the CIA triad. And availability means being able to use the system as anticipated. However, Friedman and Singer (2014) stress that one characteristic should be included within the cyber security domain: resilience. This characteristic is also very important in the light of a crisis situation. Resilience is what allows a system to endure security threats instead of failing or crashing down. It focuses on keeping the systems running with the understanding that attacks and incidents happen unavoidably. As a consequence, in the event of a cyber security incident, priorities in approaching this situation would be: to prioritize resources and operations, protect key assets, and systems from attacks, and ultimately restore normal operations.

Confidentiality, integrity, availability and resilience provide the simulation game possible themes which it can focus on. As described in Chapter 3, the participants within the RPD model try to the recognize the system as typical (DM3). When designing a scenario, a possibility is take all of these into account, in which the narrative unfolds in one particular direction. This stimulates RPDs as well as the dynamics, including changing goals and objectives (DM2). Participants are then forced to continuously look for information (SA2) and classify the situation appropriately (DM5) and act based on their situation awareness (SA1).

Confidentiality, integrity and availability could be affected by software errors and blue screens of death. However, it is only a cybersecurity issue when someone tries to exploit the systems’ unavailability. This introduces the next section: what are we trying to protect against?

**What are we trying to protect against? The Presence of an Adversary**

Within the cyberspace domain, Friedman and Singer (2014) note that deviation of the system’s intended use can be an error or accident. However, they believe that this deviation is only a security problem when caused by an adversary (or attacker). Orbs et al (2012) agree to this. Their “Diamond Model of malicious activity” includes a malicious actor and their capabilities to exploit the infrastructure and or victim. Kott (2014) proposes a model of cybersecurity research with three main components: (1) an attacker with their tools and capabilities, (2) a defender with their tools and techniques, operational assets and network and systems and (3) Policy, which is a set of defender’s assertions or requirements about what event should and should not happen. In that sense the cyber security incidents depend on the attributes, structures and dynamics of the network of computing devices under attack, and the tools and techniques of defenders and attackers (Kott, 2014).

For the purpose of the proposed simulation game, it is therefore important to understand the types of attackers and their capabilities. This specifically links back to the theory on situation awareness discussed in Chapter 3. As described in the previous section, participants have to make decisions based on the level of situation awareness they have (SA1). One important aspect then is classifying the adversary they are
facing during the crisis (DM5). This involves assessing the threats on their main goals (SA3), and eventually determines which problem-solving strategy is taken (SA2, DM4).

The concept of an adversary within cyberspace has been around since the start of the World Wide Web. The study on cyber adversaries was initiated in the early 1980’s, when personal computer became the mainstream and the word ‘hacker’ entered the lexicon as a person skilled at programming and manipulating operating systems. Even though the word ‘hacker’ initially did not have a negative connotation, several years later it was used to describe malicious activity on the web (Meyers, Powers & Faissol, 2009). In Rogers comprehensive work of cyber adversaries and their motivations (Rogers, 2006), he found that hackers displayed a high level of moral disengagement (convincing oneself that ethical standards do not apply in certain contexts, as well as differential association (a criminology theory which proposes that individuals learn values, attitudes, techniques and motives for criminal behavior through interaction with others). However, Rogers’ (2006) study specifically focuses on cyber criminals. In Meyers et al. (2009) work of summarizing and discussing the different taxonomies for cyber adversaries, a wide range of adversary types are discussed based on methods, motivations, maliciousness, and skill levels. Mostly by building on Rogers’ (2006) work and on several other taxonomies, Meyers et al. (2009) propose the following classes, ordered on levels of skills and sophistication:

- Script kiddies, newbies, novices
- Hacktivists, political activists
- Cyber punks, crashers, thugs
- Insider, user malcontents
- Coders, writers
- White hat hackers, old guard, sneakers
- Black hat Hackers, professionals, elite
- Cyber Terrorists

These will be explained in more detail below. What becomes clear from the characteristics is that there is a wide range of adversary types. First of all, they differ strongly in skill and sophistication (capabilities), there is a wide range of motivations for their actions, due to the difference in skill level they apply different (sets) of tools and some are more hazardous than others. This has strong implications on the perception of being secure. The question that arises when talking about security level is then: secure against what?

### 4.2.2 Threats

Cybersecurity and the Crisis model share an important characteristic: threat. Friend men and Singer (2014) stress the importance of the difference between vulnerabilities and threats. They believe that when there is a vulnerability, like an open door, this not necessarily means that there is a threat. In other words, a threat is the potential of an unwanted event happening. This is only the case one someone actually wants to go through that open door. On the other hand, this one vulnerability can lead to many different threats. Friedman and Singer (2014) note that the important factors of understanding a threat are the actor and the consequence. Therefore, in their view, a threat is the combination of the vulnerabilities and the actor’s objectives. This is a similar definition as used in the Bodeau et al.’s (2010) definition of cyber threat: “A specific adversary of class of adversaries which seek to exploit the organization’s or a mission’s dependence on cyberspace, to achieve specific goals.” (p. 2).

Important is that these adversaries cannot be taken together on a very popular term “hacker”, but are quite different from each other. As seen from the above two definitions of a threat, the foremost important aspect to differentiate the actors are their objectives and goals. Another important differentiation to make is the location from which the attack is originated. Earlier explained is that attacks
can stem from anywhere in the world, and can attack anything that is reachable through cyberspace (McCusker, 2007). However, a crucial adversary not to forget is the insider threat.

These insiders are trusted users of the system which already have certain access rights (Bishop, 2008). Additionally, these access rights can give them the freedom to look for any existing vulnerability existent in the system which is merely designed to keep the bad guys out (Friedman and Singer, 2014). It also makes a difference if you are the actual target of the attack, or that attackers just want to attack. All boils down to the same thing: the attacker's objective.

Friedman and Singer (2014) state that there are only three things you can do to a computer: steal its data, misuse credentials, and hijack resources. Howard and Longstaff's model (1993) of computer and network attacks additionally includes: increased access and corruption of information. However, even though not specifically stated in Friedman and Singer (2014), there is no mentioning that these activities are the attacker's goals. As can be seen when discussing the details on attacker types, goals and capabilities one can only conclude that the attacker's goals are more high-level. However, given the strong dependency that organizations have on their information systems, these five actions systems can bring a lot of damage.

Altogether, many different things can happen on an organizations network, but the important notion is that this has to be done by someone. As depicted in figure 13, the concept of a threat summarizes the actions that an adversary takes while attacking an organization. It starts with goals or objectives. From there, vulnerabilities are sought and when found exploited with the actor's capabilities, to conduct malicious actions to reach their ultimate goal. Therefore, this requires understanding of the concepts of vulnerabilities, attacker (including their goals and capabilities), and attack types.

![Threat model](image)

Figure 13: Threat model

The next three paragraphs discuss the elements of the threat model in greater detail. This increases the understanding of the combinations that are possible in creating a realistic scenario (SG1, SG2, SG3) as well it provides necessary details to differentiate classification of the situation from the participant's point of view (DM2, DM4, DM5).

**Vulnerabilities**

According to the Information Security Organization (ISO/IEC 27001:2013, 2013), a vulnerability is “a weakness in an asset or group of assets. An asset’s weakness could allow it to be exploited and harmed by one or more threats.” In other words, these are weaknesses in either systems, configurations, designs, people etc. which can be exploited by attackers to serve their goals to their objectives. Landwehr et al’s (1994) taxonomy of computer security consisted of three major components of a vulnerability: (1) The nature of the vulnerability, (2) the time where the vulnerability originated and (3) where the vulnerability was introduced. Importantly for the Cyber crisis model is the type of the vulnerability.

A short grasp in the literature of vulnerabilities already shows the wide range of existing vulnerabilities. In the scope of this thesis, not much attention is paid on the details, however it is important to mention a view important vulnerabilities. This list is not meant to be complete and exhaustive but to give an idea of
the vast amount of vulnerabilities that exist and might be incorporated in the game scenarios and events. Four of the most important vulnerabilities are:

**Human Vulnerability.** The easiest way into a system is arguably to just ask the victim. This category falls within the category of social engineering and does not require any tampering with computer systems. More often used techniques are phishing and spear phishing, within these types of social engineering the attackers try to lure the user of the system into clicking a malicious link or to fill in their password the second version is specifically targeted to a small group of users. However, the vulnerability can also be present without the interaction between attacker and victim. When employees just ignore basic security precautions, attackers can enter systems by exploiting standard passwords like user: admin password: admin, as these were never changed since the system was implemented (Friedman & Singer, 2013).

**Application Vulnerability.** Attacks on web application often make misuse of user input validation (Fu and Li, 2010). This user input is send back to the server to be processed and executed. When there is a lack of sanitation checks on possible input, it is possible that code is being executed by the server. This check for sanitation is especially important because input is send through the internet by using the browser. These and other vulnerabilities can have far reaching effects for the confidentiality, integrity and availability of the web application (Holm et al., 2013) and its data.

**Software Vulnerability.** This type of vulnerabilities is often exploited by more advanced attackers (Friedman and Singer, 2014). These are often attributed to mistakes in design or implementation (Al-Feraghan, 2010). As Al-Fedaghi mentions, that typically the approach to providing protecting against vulnerability is for each vulnerability to apply patches to close “holes” in the software, and therefore countering the exploitation. But this approach is doomed to fall behind in the battle against attackers. As Ross Anderson (2011) states in his paper Why information security is hard a product like the Windows Operating System has around 1 Million bugs. Given the time to find and patch these vulnerabilities, an attacker just has to find a vulnerability that has not been patched yet. Or, if the patch is found publicly, one can exploit systems in which the user ignored patching.

**System Level Vulnerability.** The last one found is the system level vulnerabilities. One common vulnerability is the buffer overflow. These type of attacks are found to be so commonly existent because these vulnerabilities are common and easy to exploit (Cowan et al., 2000). As the name of the attack depicts, the attack involves overflowing the capacity of the system, specifically its memory. Computers use working memory to store data and instructions. When there is too much data written on the memory it will spill over into the allocated “buffer” and overwrites the space where the computer stores the next instruction to be executed (Friedman & Singer, 2014). This is exactly what the attackers wants, as the buffer overflow allows attackers to inject and possible execute the attack code. In other words, the program will either break or it will exactly do what the attacker wanted (this includes gaining rights over certain programs).

The above listing of vulnerabilities remains high-level; clearly though, either humans or computer systems can be targeted by attackers. Also it shows that given the fact that many modern organizations have complex networks with all kinds of systems, software (either Commercially of the Shelf or customized), applications and thousands of employees it is a challenge to protect against attacks.

**Attackers**

As discussed earlier, there exists a range of different types of adversaries to consider. One cannot just put aggregate and throw under the common denominator of ‘hacker’. Meyers et al’s (2009) taxonomy of cyber adversaries is based heavily on the extensive work of Rogers (2006) on the taxonomy of adversaries and some other works focused on the taxonomy of adversaries. The descriptions given by Meyers et al (2009) focus on the following characteristics:
• **Skill level:** The level of sophistication an adversary has and familiarities with exploiting vulnerabilities.
• **Maliciousness:** The level of damage that an adversary can have on the victim.
• **Motivation:** The reason why adversaries conduct malicious activities.
• **Method:** The distinguishing tools and manners in which the adversary acts.

Given these characteristics one can identify the view from which they defined the adversaries. A couple of characteristics can be identified. First, there the taxonomy is focused on individual adversaries. These adversaries can be part of a larger group; however, these groups are not necessarily identified. Secondly, the characteristics are not mutually exclusive. This means that within a characteristic, an adversary can be divided into multiple categories. Therefore, theoretically, it is possible that an adversary can be recognized to have multiple characteristics in one type, but also share characteristics of other types. Thirdly, not all types are malicious types but are added for completeness. In this thesis, these might be less interesting than others. Still, the proposed taxonomy of Meyers et al. (2009) give a good overview on the adversary landscape. The following types were recognized by Meyers et al. (2009), ordered by their skill level:

**Script kiddies, newbies, novices.** These adversaries are the least sophisticated and even hold very limited programming skills. They are novice hackers and often use scripts that are pre-written (also known as ‘toolkits’) by more advanced attackers in their exploits. These script kiddies are young and are motivated by boredom and thrill-seeking. Due to their limited skills they have a low level of maliciousness. However, due to the advancement of toolkits the ability for them to conduct larger attacks is growing. An example is the Distributed Denial-of-Service attacks conducted by five young Dutch boys between the age of 15 and 21 to deny 1,8 customers of Internet Service Provider Ziggo to the Internet for two days (Security.nl, 2015).

**Hacktivists, political activists.** These adversaries are no criminals in the sense that their motivation is not for personal gain, but rather a political cause. Attacks often used by hacktivists are denial of service and website defacements on rival organizations. The damage that they cause is quite focused on the victim organization, however it can have broader consequences. Even though the opinion of hacktivists is to do good, the media and organizations often speak of hacktivists as terrorists (Vegh, 2002).

**Cyber punks, crashers, thugs.** These adversaries have similar motivation but have greater skills than the script kiddies, but also include personal gain. These adversaries pick their targets for prestige and are featured in media (Rogers, 2006). These adversaries can write their own scripts and conduct malicious acts as spam, defacing websites and identity theft. One interesting notion is that these type of adversaries occasionally become internet security consultants (Meyers et al., 2009). They either switch ethical standards or they do not see a decent living in this field of being an adversary.

**Insiders.** According to Meyers (2009) the least publicized group of adversaries, yet they believe represent the greatest risk for companies. This is shared by (Friedman and Singer, 2014). As earlier described, insiders are already have elevated access privileges and can know possible vulnerabilities. This in combination with the motivation of revenge, in response to negative events in the company can make a very damaging combination. This can include changing information, disclosing secret information, stealing intellectual property or even worse to introduce vulnerabilities into the system for others to exploit.

** Coders, writers.** These adversaries are involved in creating the toolkits that are used by other adversaries, especially in the script kiddie category. Their motivation is power and prestige and position themselves in the role of mentors and get fame by producing these toolkits. They are (more or less) highly skilled and understand software on the systems level. Their damage level can have far reaching consequences as their created malware can get distributed and have a life of their own. The typology of
coders, writers can be a bit misleading as they could also include programmers within companies. A proposition to change would be: malware architects as they are design and program, maintain and distribute these malware packages.

**White hat hackers, old guard, sneakers.** This is not a group of malicious adversaries, but are added for the sake of completeness by Meyers et al (2009). These type of hackers see themselves as ethical hackers and do not wish to cause any damage. These hackers are motivated by the intellectual challenge of finding vulnerabilities in systems and the creation of new types of programming. Often white hat hackers work at (security) organizations and are hired to assess company’s implemented defenses.

**Black hat hackers, professionals, elite.** As the typology already indicates, these are very skilled individuals. Their technical skills are so sophisticated that they employ them for professional and organized crime. Like any other criminal outside the cyber domain, their motivation rests on money and greed (tangible personal gain). In contrast to other groups, these criminals do not look for any prestige or fame and to remain low-key and evade authorities. They remain successful in this, as still very little is known about them (Rogers, 2006). Within organized cybercrime, their technical skills are acquired by other criminals as ‘guns for hire’.

**Cyber Terrorists.** Meyers et al (2009) define this type of adversaries the most dangerous and skilled of all cyber adversary classes. Cyber terrorists are employed by nation states and are engaged in information technology warfare. It is their job to conduct attacks that have a destabilizing effect, disrupt operations, and destroy assets and data of an enemy nation or government organization. Individuals recruited for this type of work are highly skilled and are motivated by ideology. They are often deployed in well-funded machines with other very dangerous individuals. Secret services like the US NSA and the British MI5 use cryptography puzzles to hire individuals that have the code-cracking capabilities they look for (Melina, 2014). An example used by Meyers et al (2009) is the terrorism occurred in Estonia in 2007, following a controversial removal of Russian World War II monument; in which a massive denial of service attack crippled websites of Parliament, several national newspapers, and the central bank. A similar crippling DDoS attack preceded the conflict between Russia and the Republic of Georgia in 2008 (Markoff, 2008). Such attacks are impossible to prosecute, as you do not know for sure who is behind them. This makes these types of attacks even more dangerous, and guarding against these attacks is a top national priority.

**Attacks**

In determining which types of attacks exist, there is one challenge: that the notion of an “attack” is quite broad. As Mayers et al (2009) state an attack can encompass “attack vectors, operating systems, hardware and software targets, access schemes, attacker objectives, specific implementation and design vulnerabilities, and the attack payload” (p. 11). In one of the most extensive works on computer security incidents was conducted by Howard and Longstaff (1988) in which they analyzed data consisting of over 4,500 security incidents between 1989 and 1995. This resulted in a taxonomy containing of five primary components: attackers, tools, access, results and objectives. This is a general attack taxonomy and not necessarily focusing on the attack types. Its advantage is also its disadvantage as it does provide a broad scheme within which different incidents could be easily be placed. However, no details were given in this taxonomy. A more detailed work on network and security incidents is from Hansman and Hunt (2005), which focus on the attack vectors (the main means by which the virus reaches the target), targets of the attack (hardware / software / people), specific vulnerabilities and exploits (the security flaws) and the payload of the attack (outcome and effects). To stay in line with the approach from Mayer et al (2009) given above, this thesis stays with the attack taxonomy they propose based on the above two researches. Mayers et al (2009) propose the following attack classes deployed by adversaries to exist in exploiting vulnerabilities. Of course, any serious security incident employ more than one of these given attack classes, and are therefore not mutually incompatible alternatives (Mayers et al., 2009).
Viruses. A computer virus is a program that copies itself and infect system files without knowledge of the user. Viruses can be transferred when there is connection between the host system and the target system, either through computer networks, the internet or a form of removable media (e.g. a USB stick). The spread of viruses is dependent on running the executable virus code; therefore, it is often attached to legitimate program executables.

Worms. Worms are also a form of malicious software, and are self-replicating that uses a host network to send copies of itself to other computers on the network. They are different from viruses in the sense that, because of their self-replicating character, do not need to be attached to programs and can spread without user interaction. Next to that, worms infect network infrastructure rather than system files. These worms predominantly exploit vulnerabilities in operating systems, striking unupdated systems after a major security patch. The most common forms of worms install some sort of ‘backdoor’ on the infected systems to allow remote control. These systems together can form ‘botnets’ that are dedicated to for example send spam or originate a Distributed Denial of Service attack.

Trojans. Just like the mythical Trojan Horse, this type of malware conceals its function during attack. In other words, they piece of software seems to perform a desired function, while secretly executing malicious content. Users are fooled into installing the Trojan via different attack vectors, most often online downloads or e-mail links. Also Trojans install a ‘backdoor’ on infected systems to allow remote access, or engage in data destruction. These Trojans however, often do not self-replicate and therefore rely on their host program to spread.

Buffer Overflows. In computer systems, a buffer overflow happens when a program writes more information into the buffer (temporary memory storage) than the space allocated to it in memory. During this type of attack, attackers exploit this property by forcing a buffer overflow to overwrite the local variables and alter program execution, forcing the process to execute malicious code introduced by the user. This buffer overflow technique may be used as a method of enabling other attacks such as worms to be executed on a system.

Denial of Service. A denial of service attack function by making a computer network or resource inaccessible to legitimate users. Every system can handle a certain amount of data on their networks (bandwidth). A denial of service attacks then floods the network by generating requests which are transferred across the network. Targets include the network routers (resulting in slow network performance), DNS services (resulting in an inability to access websites), and email accounts (resulting in a “mail bomb” of spam). A large scale Denial of Service is called a distributed denial of service attack, where multiple systems are combined to flood the bandwidth and resources of the target. One important note is that these attacks do not require any control of the target networks or users of the network. However, very large attacks also require a lot of resources from the attacker, which is often accomplished by building a large botnet.

Network Attacks. In Mayers et al (2009) view, network attacks happen when network protocols are manipulated to exploit other users or systems. Mayers et al (2009) use this category in a broad way, in which IP spoofing, in which the source IP address is falsified; phishing, in which a legitimate website or email is reproduced by a hacker; session hijacking, in which the theft of a session cookie leads to exploitation of a valid computer session; and cross-site scripting attacks, in which malicious code is injected into web applications. These attacks are often used in conjunction with other attacks in the taxonomy, such as denial of service attacks.

Password attacks/user compromise. Password attacks have the objective of gaining control of a particular system or user's account. There are three basic kinds of such attacks: guessing, based on knowledge of the user's personal details; dictionary attacks, which loop through a list of dictionary words and try to find a match; and brute force attacks, which loop through sequence of random characters.
Information Gathering / Resource misuse. The last category of attacks is not inherently malicious, but is often found as a precursor or component of other attacks. These attacks are used to gather information about the target in an attempt to exploit its defenses and learn more about the system. A mapping exploit is used to gain information on the hosts in a network, including what programs are running and what operating system is used. Security scanning is similar, but involves testing the host for known vulnerabilities in the hardware or software it is using. A packet sniffer is designed to intercept and log traffic on a network, which can potentially be decoded later (Hansman, 2003).

4.2.3 Conclusion: Characterizing Cybersecurity

This paragraph elaborates on the cybersecurity domain from a simulation game perspective. Participants need to be placed within a world of cyber crisis, to be able to practice the decision-making during such crisis. By simulating cyber crisis by incorporating characterizing elements in the scenarios, events and tasks participants can create the mental models that fit the situation. To speak in simulation game terms, these elements from the application domain can be incorporated in the scenarios, events and tasks and have as goal to bring the participants into that wished cyber crisis situation.

Given the above discussed elements this paragraph yields the following characteristics from the cybersecurity domain that can be incorporated in the simulation game design in later stages. Still at miss is a clear understanding of cyber crisis. However, as discussed above, no literature of such cases is found. This problem is approached by two activities. The first is to provide additional aspects from expert interviews, which will be discussed in Chapter 5. Secondly, the following paragraph will take both the crisis model (paragraph 4.1) as well as the concepts described in this paragraphs to discuss a cyber crisis that occurred in the past: the Sony hack in 2014.

Table 3: Cybersecurity Concepts

<table>
<thead>
<tr>
<th>No.</th>
<th>Cybersecurity Concepts</th>
<th>Source</th>
</tr>
</thead>
<tbody>
<tr>
<td>CS1</td>
<td>Scenarios, events and tasks should be geared towards situations which take place inside cyberspace. Cyberspace “is the realm of computer networks (and the users behind them) in which information is stored, shared and communicated online.”</td>
<td>Friedman &amp; Signer (2014)</td>
</tr>
<tr>
<td>CS2</td>
<td>Security is the safe-guarding against adversaries, by implementing security procedures which influence the feeling of safety, stability and anxiety. Once this safe-guarding is challenged, one desires to return to a state of safety. Returning to a feeling of safety can be an end-goal.</td>
<td>Summarized from Oxford Dictionaries (n.d.)</td>
</tr>
<tr>
<td>CS3</td>
<td>In cybersecurity all assets that should be protected need to be protected because of the vulnerabilities that exist as a result of the use of IT systems that form the basis of cyberspace. The definition of cybersecurity is: “the protection of cyberspace itself, the electronic information, the ICTs that support cyberspace, and the users of cyberspace in their personal, societal and national capacity, including any of their interests, either tangible or intangible that are vulnerable to attacks originating in cyberspace”.</td>
<td>Von Solms and van Niekerk (2013)</td>
</tr>
<tr>
<td>CS4</td>
<td>Confidentiality, integrity, availability and resilience provide the simulation game possible themes which it can focus on.</td>
<td>Von Solms and van Niekerk (2013), Friedman and Singer (2014), Bishop, 2003</td>
</tr>
<tr>
<td>CS5</td>
<td>Many different things can happen on an organizations network, but the important notion is that this has to be done by someone. There are a wide range of adversary types. First, they differ strongly in skill and sophistication (capabilities), there is a wide range of motivations for their actions, due to the difference in skill level they apply different (sets) of tools and some are more hazardous than others.</td>
<td>Orbst (2012), Kott (2014), Rogers (2006)</td>
</tr>
<tr>
<td>CS6</td>
<td>Cybersecurity and the crisis model share an important characteristic: threat. The concept of threat summarizes the actions that an adversary takes while attacking an organization. It starts with goals or objectives. From there, vulnerabilities are sought and when found exploited with the actor’s capabilities, to conduct malicious actions to reach their ultimate goal.</td>
<td>Friedman and Singer (2014)</td>
</tr>
<tr>
<td>CS7</td>
<td>A vulnerability is “a weakness in an asset or group of assets. These are weaknesses in either systems, configurations, designs, people etc. which can be exploited by attackers to serve their goals. Four main ones are identified: 1) human vulnerability, 2) application vulnerability, 3) software vulnerability and 4) system level vulnerability.</td>
<td>ISO/IEC 27001: 2013 (2013), Friedman and Singer (2013), Holm et al. (2013), Anderson (2011), Cowan et al. (2000)</td>
</tr>
<tr>
<td>CS8</td>
<td>There exist a range of different types of adversaries to consider. They can be classified by skill level, maliciousness, motivation and method. The following types were identified: 1) script kiddies, newbies, novices, 2) hacktivists, political activists, 3) cyber punks, crashers, thugs, 4) insiders, 5) coders, writers, 6) white hat hackers, old guard, sneakers, 7) black hat hackers, professionals, elite and 8) cyber terrorists.</td>
<td>Meyers et al (2009)</td>
</tr>
<tr>
<td>CS9</td>
<td>An attack can encompass “attack vectors, operating systems, hardware and software targets, access schemes, attacker objectives, specific implementation and design vulnerabilities, and the attack payload”. The following attack classes are deployed by adversaries to exploit vulnerabilities: 1) viruses, 2) worms, 3) Trojans, 4) buffer overflows, 5) denial of service, 6) network attacks, 7) password attacks / user compromise and 8) information gathering / resource misuse.</td>
<td>Meyers et al (2009)</td>
</tr>
</tbody>
</table>

### 4.3 Lessons Learned from a Cyber Crisis in light of the Media

In this paragraph the crisis model from paragraph 4.1 as well as the concepts from paragraph 4.2 are used to analyze a situation of cyber crisis. As will be explained in more detail in in Chapter 5, experts have mentioned that the outside world plays a very important role during such a cyber crisis. Especially the media plays an important role, where they can influence the public opinion through their publications. Therefore, a major hack was needed, of a commercial company, which have been under a lot of external scrutiny. For this reason, the Sony Hack in 2014 is chosen to analyze, where Sony Pictures Entertainment, the movie making daughter of media company Sony Inc. was hacked.

Especially, when looking at creating a narrative (**NAR1, NAR2, NAR3**), as mentioned in chapter 3, it is important to know how this outside view is formed by the media. In other words, as a model simulated from reality (**SG4**). There, it was mentioned that the participants in the simulation game was not just part of a narrative, but also builds a narrative about their own decision-making (**Learn6**). To link the analysis of the Sony Hack in 2014 with building a narrative, different timelines from media sources have been looked into to gain insights on how Sony and the actions from their senior-managers were portrayed by
the media, described as a timeline. Additionally, the analysis can offer insights on additional stakeholders or processes and mechanisms (SG2, SG3).

An important notion to address is that this analysis builds up to creating a realistic environment, which is simulated by the simulation game (SG1). Taken the approach for this analysis, conclusions from this analysis mostly regard *what could happen during an attack*. In other words, these are additional input for the scenarios, events and tasks. Even though these conclusions might not hold strong scientific validity due to the taken approach, they do enrich the information from the cybersecurity domain (4.2) as well as information given by experts (Chapter 5). These conclusions are part of the validated *integral schema* given in paragraph 5.5.

4.3.1 The Sony Hack (2014)

On November 24th 2014 employees of Sony Picture Entertainment (SPE), part of Sony corp., found their computers to show the picture of hacking group Guardians of Peace (GOP) and a crippled IT network. It turned out that the anonymous hacking group GOP stole and uploaded around 100 terabyte of data from Sony’s servers. It not just entails a hack, but is an example how a cyber incident can become much larger due to the influence from external parties.

4.3.2 Incubation Time

It is unclear how long GOP had access to Sony’s networks. But a general consensus exists that there was communication somewhere between six months and a year (riskbasedsecurity.com, 2014). Important is the way they have gained access. Sony uses SpiritWorld, a system that enables distribution of media. This system has been compromised earlier in 2014, exposing personal information of about 800 people. A decision made by Sony at the time is to not disclose this event (riskbasedsecurity.com, 2014).

According to the Taia Global report (Taia Global, 2015) access to Sony’s network was invoked by sending phishing emails to Sony employees. This e-mail contained a PDF attachment, with a remote access tool (RAT), giving access to the attackers. By gaining increasing privileges, they were able to run the payload from the used malware (Taia Global, 2015).

4.3.3 Triggering Event

On the 24th of November, 2014 Sony employees found their computers showing the warning signals from GOP. See Figure 14. The data was dumped on several file dump websites, for further distribution by others (deadline.com, 2014). In the following month, stolen data was leaked through sharing websites like: Pastebin, MEGA, RapidGator, Torrent and Github (deadline.com, 2014). Within hours a Reddit post appeared stating that Sony was hacked by the Guardians of Peace. The first published data files totaled a 24.6 GB compressed in size (riskbasedsecurity.com, 2014). This data comprised of company information, non-released films and scripts, personal information including medical records of Sony personnel, password credentials for services and lists of existing PC data, Linux servers and Windows servers (Haggard & Lindsay, 2015; deadline.com, 2014).
4.3.4 Immediate Consequences

This hack resulted in a set of immediate consequences:

Crippled networks
The hack crippled Sony’s computer networks and took down access to services, e-mail, phone lines etc. (deadline.com, 2014; riskbasedsecurity.com, 2014). Their networks remained shut down on all locations until at least day 6 (deadline.com, 2014). One of the uncertainties here is not knowing when the organization will be operational again. Lynton, the chairman and CEO of Sony Pictures stated in an interview: “It took me about 24 to 36 hours to fully understand this was not something we were going to be able to recover from in the next week or two” (Kalb, n.d.). Senior management decided to implement a phone tree, in which updates on the hack were relayed from person to person (Kalb, n.d.). On the 18th of December, technical investigations are still carried out (riskbasedsecurity.com, 2014), especially given that Sony is such a large company to investigate.

Threats from non-confirmed others
Not only did Guardians of Peace give them ultimatums, but Sony received other messages claiming they were GOP (Haggard & Lindsay, 2015). Different demands were communicated by the senders. This
raises the questions: are these threats real? Example is the demand for money, if they wish that the information leaking will stop (Haggard & Lindsay, 2015). This message has been denied by GOP.

**Attribution**

In cybersecurity there is always a challenge of assigning the attack to actors, in other words attribution. Attribution is the most discussed aspect of the Sony hack by news organizations and governments. It was clear that GOP was the group that hacked Sony. However different discussions about their ties with other parties were heated. Especially when GOP demanded that a movie titled “The Interview” would be cancelled all arrows were pointed at North Korea (Berghel, 2015). The film’s plot revolves around the assassination of North Korea’s leader, Kim Jung-Un. But many others did not believe any of the arguments that were offered in favor of the attribution to North Korea (deadline.com, 2014; riskbasedsecurity.com, 2014). The attribution remains pure speculation, and it definitely did not help Sony any further.

**Involvement of Third Parties**

It was exactly attribution which involved the U.S. government. Different press releases from the FBI asserted that North Korea was to be blamed for the hacks. Even President Obama was involved by stating “the US would respond proportionally at the place and time and manner that we choose” during his yearly speech (Haggard & Lindsay, 2015). Interestingly, Sony did not seem to take any position in attributing the attack.

Other parties involved were Security Firms, Media, Former employees, North Korea, Snap Chat, MPAA, Theatre Owners, Business Partners (deadline.com, 2014). This all had influence on the situation in three ways, 1) by making a decision for themselves, but subsequently affecting Sony, 2) their data was leaked due to the breach or 3) they are involved in researching the problem.

**Class-action law suits**

Three separate cases of class-action law suits were filed against Sony by former employees for inadequate safeguarding personal information. The first were in the first weeks, but the second and third were followed in the fourth week (deadline.com, 2014).

**Leaked merger plans**

Leaked emails show that Lionsgate (film studio) executives wanted to meet Sony CEO Kazuo Hirai to discuss possibilities of merger of acquisition (deadline.com, 2014). Similarly, a conversation between SnapChat board members and Sony executives of a possible merger of $3 billion, was exposed (riskbasedsecurity.com, 2014).

**4.3.5 Decision-Making**

Even though there is no actual insight in how the decisions were made internally, it is interesting to see which decisions were made and the reasons for making them. These give insights in the type of decisions are taken by whom and as a reaction on which pieces of information. This section will go through the pieces of communication and decisions made in a chronological order.

**We are investigating an IT matter**

Sony spokesperson Jean Guerin says, “We are investigating an IT matter.” (deadline.com, 2014). Meaning on the 24th of November. It turns out that only Sony Pictures Entertainment is affected, not the rest of Sony corp.

**First company-wide alert to all employees comes day 9**
Sony Chiefs Michael Lynton and Amy Pascal issue a company-wide alert to employees about the attack one week and two days after the breach: “It is now apparent that a large amount of confidential Sony Pictures Entertainment data has been stolen by the cyber attackers, including personnel information and business documents. This is the result of a brazen attack on our company, our employees and our business partners. This theft of Sony materials and the release of employee and other information are malicious criminal acts, and we are working closely with law enforcement… while we are not yet sure of the full scope of information that the attackers have or might release, we unfortunately have to ask you to assume that information about the possession of the company might be in their possession. While we would hope that common decency might prevent disclosure, we of course cannot assume that… we can’t overemphasize our appreciation to all of you for your extraordinary hard work, commitment and resolve.” (deadline.com, 2014).

**Apologies from Scott Rudin and Amy Pascal**

On day 17, both Scott Rudin (star producer) and Amy Pascal (chairman, Motion Pictures Group, Sony Pictures Entertainment) apologized for the racially insensitive remarks made in an e-mail conversation between the two, which has been leaked. Their conversations addressed president Obama. (deadline.com, 2014). She tells a reporter: “I didn’t want to make this about me. Everyone at this company has been violated and nobody deserved this. Then the most hurtful e-mail came out… I’m so disappointed in myself, that I ever would have had such a lapse in my thinking” (deadline.com, 2014).

**Sony hires litigator David Boies**

Sony hires known litigator David Boies to deal with the situation on Day 19 (deadline.com, 2014). Boies sends a letter to news organizations demanding that they delete any stolen information they have been given by the hackers.

Boies sends out communications, demanding to erase every piece of information which was received by the hackers stating: [Sony] “does not consent to your possession, review, copying, dissemination, publication, uploading, downloading or make the use” of the information. Additionally, the media is urged to avoid, and delete or destroy the information from their computers if they are in procession of it (deadline.com, 2014).

**Sony cancels press screenings, TV advertising and TV appearances after threats of physical terrorism**

GOP makes certain threats to attack any theaters where the Interview was scheduled to open, specifically to remember the 11th of September 2001. This instigated a large discussion on the issue of both cyberterrorism and free speech (Haggard & Lindsay, 2015). As a reaction to this threats, Sony Picture Entertainment canceled press screenings in multiple cities around the United States. Additionally, TV advertising and TV appearances from the actors were pulled for the Interview. This is one of the few cases in history that a business changes their course of action due to cyber threat (Haggard & Lindsay, 2015). However, the plan is to stick to release date of the 25th of December. Sony shares with theater owners it is possible to cancel the showing if they are worried about any threats made by hackers.

**Sony Pictures cancels the planned Christmas Day release of The Interview**

On day 23, Sony Pictures additionally scraps the planned Christmas Day release of The Interview in a reaction to the decision of major theatres to cancel showing the Interview. “In light of the decision by the majority of our exhibitors not to show the film The Interview, we have decided not to move forward with the planned December 25 theatrical release,” Sony said in a statement (deadline.com, 2014), “We respect and understand out partner’s decision and, of course, completely share their paramount interest in the safety of employees and theatergoers. Sony pictures has been the victim of an unprecedented criminal
assault against our employees, our customers and our business. Those who attacked us stole our intellectual property, private e-mails, and sensitive and proprietary material, and sought to destroy our spirit and morale – The move comes after the National Association of Theatre Owners tells exhibitors it’s OK to yank the film “so that our guests may enjoy a safe holiday movie season experience the many other exciting films we have to offer.”

**Sony forbids media interviews, and went on radio silence**

After making the move on cancelling the movie, Sony communicated a halt on media interviews, stopped any communication on social media and even removed its own name from marketing materials (Fritz, n.d.). Sony did make a PR move and offered an exclusive to the Wall Street Journal.

**Sony publicly reacts to President Obama**

In reaction to the cancellation of the showing of The Interview, President Obama publicly stated that Sony “made a mistake” in caving to North Korean hackers (riskbasedsecurity.com, 2014). Michael Lynton (CEO of Sony Pictures) goes on CNN to respond to President Obama. He states: “We did not cave. We did not back down, he says, proceeding to lay much of the blames on exhibitors who refused to show the Interview. This response was followed up by an official statement: “The decision not to move forward with the December 25 theatrical release of the Interview was made as a result of the majority of the nation’s theater owners choosing not to screen the film. This was their decision. Let us be clear – the only decision that we have made with respect to release of the film was not to release it on Christmas Day in theaters, after the theater owners declined to show it” (Haggard & Lindsay, 2015).

**CEO Michael Lynton personally pursues screening deals**

While Christmas holidays are underway, Mr. Lynton takes personal responsibility in chasing after deals for the wide showing of the Interviews in theaters and online, which are usually done by executives a couple levels down the ladder. “I have tried to make sure all the decision-making relegated to this incident comes back to me so that, as much as possible, the operating groups are not distracted from the normal business they have to do,” he said (Kalb, n.d.).

**Sony changes course of action: the screening will go on**

When Sony decided initially to cancel the screening, they were under heavy public scrutiny from multiple sides (Fritz, n.d.). As a result of the criticism, the decision was reversed soon to be aired in smaller theaters. “We have never given up on releasing the interview and we’re excited our movie will be in a number of theaters on Christmas Day,” said Michael Lynton, Chairman and CEO of Sony Entertainment. “At the same time, we are continuing our efforts to secure more platforms and more theaters so that this move reaches the largest possible audience,” (deadline.com, 2014). President Obama praises Sony’s decision to release the film by stating: “The president applauds Sony’s decision to authorize screenings of the film”.

**Sony is a victim**

Kazuo Hirai, the CEO and president of Sony, stated that “[Sony employees] were unfortunately the victims of one of the most vicious and malicious cyber-attacks that we’ve known certainly in recent history… And I have to say that freedom of speech, freedom of expression, freedom of association, those are very important lifeblood – lifelines – of Sony and our entertainment business”. (Cyber Alert, n.d.). This was a break of silence in January, when all seemed to be over. (CNN, n.d.)

### 4.3.6 Communication Strategy

It is not clear if Sony really had a strategy or plan to solve the issues. Most of the decisions and communications seem to be reactive on what external events. Even though the communications were
from spokespersons or executives, it seemed to be non-consistent and prioritized on saving face instead of actively solve the problem.

### 4.3.7 Long-term Consequences

#### Financial

**Direct Losses.** Sony estimates its direct losses of the hack around 15 million Euro, which mostly involves investigation costs and sanitation costs. Sony is fully insured for this damage, in other words, this has no financial effect on the company. (Berghel, 2015; Haggard & Lindsay, 2015; deadline.com, 2014; riskbasedsecurity.com, 2014).

**Stock Prices.** Let's look at the stock prices during this event. As can be seen in Figure 15, the stock price went down during the first two weeks after the discovery of the event. However, the stock price has recovered fairly quickly, and in February it even reached points higher than the day before the hack. This shows that dropping stock-prices is actually not a long-term consequence, but a short-term one.

![Figure 15: Sony Corp. Stock prices generated from Yahoo Finance](http://finance.yahoo.com/echarts?s=SNE+Interactive#customRangeStart:1416783600,customRangeEnd:1422745200,range:custom,allowChartStacking:tree)

#### Reputational

For Sony, the financial losses were limited. However, according to multiple sources, it has suffered from reputational damage. (Taia Global, 2015) states that Sony Picture Entertainment reputation damage were caused due to the hack. The leaked data included e-mail conversations between Amy Pascal and Scott Rudin, as earlier mentioned. Both later on apologized to President Obama. On the 5th of February 2015, Amy Pascal announced her resignation, possibly linked to the e-mails (Kang, 2015).
4.3.8 Scenario Considerations: Lessons Learned from the Sony Hack

Analyzing the Sony hack from 2014 a number of considerations can be taken into account when designing the Cyber crisis simulation game. Even though not necessarily generalizable as it is only one case, they can form input of what could possibly happen during Cyber Crisis. The statements described in table 3 are lessons that can be learned from the Sony hack in 2014 and can be taken into consideration in the design of the scenarios, events and tasks.

<table>
<thead>
<tr>
<th>No.</th>
<th>Scenario Considerations</th>
</tr>
</thead>
<tbody>
<tr>
<td>Sce1</td>
<td>Crisis starts when there is the perception of it. The hackers were on the network for a time period between six months and a year. This however, was no crisis on itself. When the networks were actually down, warning signals were shown company wide and the data was leaked on data sharing websites, then there was crisis.</td>
</tr>
<tr>
<td>Sce2</td>
<td>The vulnerability could come from third party service providers. Sony was breached through a third-party software service called SpiritWorld. This could be the case for any company, as many organizations rely on many third-party services.</td>
</tr>
<tr>
<td>Sce3</td>
<td>The Story can be kept alive for weeks. Hackers dripped information, instead of dumping it all at once. This kept this stories going for weeks. This caused uncertainty about the duration of the hack. Additionally, there is uncertainty about which information is compromised. In this case the information included non-released materials, personal information including medical records of personnel, password credentials for services and lists of existing machines and servers.</td>
</tr>
<tr>
<td>Sce4</td>
<td>The only real short-term consequence is operational discontinuity. The only decisions that seems to require immediate and quick handling is bringing back the systems to continue activities. The need to bring it back as soon as possible depends on the dependence on the systems and data.</td>
</tr>
<tr>
<td>Sce5</td>
<td>Threats can come from anyone, claiming anything. There were multiple claims for either money, taking down the movie, or even physical threats. But the GOP never showed who they were. This leaves involved wondering each and every moment uncertain over the credibility of the claims.</td>
</tr>
<tr>
<td>Sce6</td>
<td>Financial consequences can be large, when not insured. It can be expected that a large company like Sony is insured to any possible events. However, when firms get smaller and smaller, it might be different. Costs in the Sony hack involved investigative and sanitary costs. However, one can also calculate loss by taking the loss in ticket pricing or other loss of sales as well.</td>
</tr>
<tr>
<td>Sce7</td>
<td>Reputational damage is created by the media. In terms of reputational damage, it was the heavy media coverage over the leaked e-mail conversations between Amy Pascal and Scott Rudin that got the public involved, specifically over its racist contents. This shows that not only the company should be wary of the reputational damages, but single senior managers as well. One side-note is that it was the second time Sony got hacked. Apparently, for Sony these hacks were not critically affecting their core business.</td>
</tr>
<tr>
<td>Sce8</td>
<td>Attribution is hard, and speculation seems to lead the discussion. Many different news sources entered the attribution game. Was it North Korea? Was it China? Anonymous? Speculations on reasons why or why not a particular actor could be the attacker seemed to be the most interesting discussion.</td>
</tr>
<tr>
<td>Sce9</td>
<td>Investigative and sanitary work can take a while, without answers. In any company with the size of Sony, one can imagine how long it takes to investigate and sanitize all the networks, systems, devices and anything else that is part of their ecosystem. If the attacker is skilled, they erase their tracks or put investigators on side-trails. There is no guarantee that investigations offer answers.</td>
</tr>
</tbody>
</table>
Externals will tell the story for you. True or not. As access was obtained through a phishing e-mail, one can imagine that the hack was not extremely complicated (not saying it was easy). However, the story took flight, also due to media and government. These external parties have influence on events but especially the public opinion. But still, many believed that claims made by governments were not based on truth, but assumptions on red flags. Additionally, involvement from parties like governments as well as ex-employees suing the company also forms the story in some way.

Hiring third parties can result in losing the public's sympathy. As it is a large hack, people might feel sorry for Sony. Especially, because it was not the first time. However, when they hired litigator David Boies, making all kinds of threats, people could lose their sympathy for Sony. Additionally, what is forbidden might be more interesting for people as well.

4.4 Conclusion: Concepts and Models from the Cybersecurity and Crisis domain

This chapter provides the details for the conceptual game design. They bring the last bit of realism into the room in which they are situated. Discussed in this chapter are 1) the crisis model, 2) concepts from cybersecurity and 3) analyzing of the Sony hack, a cyber crisis. These provide insights into which details are necessary to build a scenario around including the events and tasks. This chapter forms the final input, combined with all other inputs earlier discussed form the conceptual game design. This chapter discussed the following main topics:

The crisis model. The crisis model is meant for the game to be simulated during play. It combines the views of crisis as an event as well as crisis as a process. Crisis starts with an incubation time, followed by a triggering event, followed by decision-making under a veil of fog and finally the crisis has internal or external consequences.

Concepts from Cybersecurity. The second paragraph especially aims at building a realistic knowledge base of cybersecurity aspects. Additionally, these also provide facilitators, perhaps less experienced in the Cyber security domain, a basis which they can rely during play. In other words, this paragraph builds the final set of elements which the designer but also the facilitator can choose from when first creating the scenarios before the game commences but secondly also the narrative during play. Nine concepts are identified to take along in the design, ranging from demarcation of cyberspace to options for scenarios. However, when looking at the cybersecurity domain, a few characteristics stand out. The first is that it takes place inside cyberspace, which “is the realm of computer networks (and the users behind them) in which information is stored, shared and communicated online” (Friedman and Singer, 2014). Secondly, there is the need to safe-guard against adversaries. In other words, there are actors involved that have an objective against the target company. A question then is, protect for what? Very important concepts within the cybersecurity are ensuring the confidentiality, integrity, availability and resilience of the systems.

Analyzing the Sony Hack. The third paragraph draws lessons from a cyber crisis in which the media played an important role. They can influence the public opinion through their publications. The Sony hack in 2014 is a major hack, of a commercial company, which has been under a lot of external scrutiny. A total of 11 lessons are derived from this particular cyber crisis. Also these provide the game elements with options which could be implemented to unfold during the play of the simulation game.
5. The Practitioners view on Cyber Crisis

In Chapter 4, important concepts from the crisis and cybersecurity domain have been discussed including the analysis of a cyber crisis. These insights and concepts are very helpful in creating scenarios, events and tasks. However, the crisis model, cybersecurity concepts and lessons learned from the Sony hack do not provide procedures and mechanisms yet to be simulated. Missing here are actors and roles (SG1), replication of the system (SG3) and their relation to the environment (SG2). Additionally, the concepts discussed in Chapter 4 lack the focus on decision-making under uncertainty which was found very important in crisis situations in Chapter 3 (DM1) as well as emotions (Learn5, NAR3). However, as literature is not able to inform the simulation game design in a sufficient manner, another source of information is required. Given that perception plays an important role during crisis situations, as described in the situation awareness sections (SA1, SA3) as well as was discussed that during the Sony hack was perceived a crisis around six months after the first breach (Sce1), expert interviews will be conducted. Three different type of experts are interviewed. First, a crisis management expert depicts the p

In the first paragraph of this chapter (5.1), the method for extracting data from the sources is mentioned. The second paragraph (5.2) focuses on the perception of cyber crisis according to the experts. The third paragraph discusses the decision-making aspects as well as questions that arise during cyber crisis (5.3). In the fourth paragraph, the stakeholders are discussed. Finally, in the fifth paragraph (5.5) the two phases of crisis management in cyber crisis are explained: Discovery and First Response and Managing Media. Together, all paragraphs form the integral schema which are the processes that will be simulated in the simulation game. Additionally, this chapter provides a fast number of inputs that can be used in designing the simulation game from a practical point of view.

5.1 Method

In total, seven interviews were conducted for this research, which are summarized in Appendix B. The participants are all part of the same professional services organization with over 200.000 employees worldwide. These experts have years of experience at client organizations, conversing and delivering services to senior-managers of large global corporations. Six of the interviewees are part of the Cyber Security Practice for the Europe, Middle East, India and Africa region. Some in leadership roles. Additionally, two of the interviewees are of specific interest, as one is particularly an expert on crisis management over 20 years and one was an executive of a company which was hit by a cyber crisis in the past. The assumption in conducting the interviews from experts instead of the actual senior-managers, is because as they see different organizations occasionally, each with their own problems and challenges, have insights of the collection of firms that single firms do not have. The participants are selected based on their specific field of expertise (Cyber Security, Crisis Management or have experience in being in Cyber Crisis) and their professional experience range from five to over 20 years of experience.

The interviews are conducted in a semi-structured way. As the design is focuses on creating a simulation game regarding decision-making under uncertainty during cyber crisis the topics discussed during the interview are: 1) definition of crisis and cyber crisis (Sce1, SG4, SA5), 2) important aspects of a cyber crisis (SG2, Learn4, CS1), 3) decision-making during crisis (SA1, DM2, DM3), 4) stakeholders (SG2-4, Sce10, Sce11), 5) processes and mechanisms of cyber crisis (SG1-4, Learn4) and 6) requirements and
considerations for a successful implementation of the simulation game (Hevner, 2006). The first five topics are discussed in this chapter and the sixth is discussed in Chapter 6.

During the interviews the topic is introduced and is followed by a two-way dialogue, with the objective to construct the perception of this expert on the topic addressed. When no new insights are formed or concepts given, the next topic is introduced. The excerpts of the interview are discussed and checked off by the interviewee when agreed and further additions are discussed over email when elements are missing or incorrect.

The following sources of information are chosen to provide the needed insights:

- **Interview with a Crisis Management Expert.** This person depicts the most important processes aspects and stakeholders when an actual crisis would take place and how these are internalized in an organization’s documents. The interview with this expert was focused on creating an overview of the processes when an organization is involved in Crisis. There is no filtering involved. Important is that this person is not a Cyber Security expert, and therefore, his answers are more geared towards a general Crisis. Therefore, we need the input from Cyber Security experts as well.

- **Six interviews with Cyber Security Experts.** These interviews enrich the processes, stakeholders and aspects by adding their mental models from the Cyber Security domain. The answers from: *Important aspects of a Cyber Crisis, Decision-making during Crisis, Stakeholders and Mechanisms of Cyber Crisis* are included in the model that was created with the Crisis Management Expert. One special interviewee is the cybersecurity expert which has experienced a cyber crisis as an executive. This interviewee has also validated the combined models from reality, the *integrated schema*, which is integrated in the simulation game design.

Even though we cannot take all information given for granted, as the interviewees are not experts in all topics discussed, they do offer a very valuable insight. Namely, their perception of a cyber crisis including concepts and feelings. This is important because this enables the creation of a realistic environment for the participants. In theory forming research these answers might create doubts over validity. However, the goal in this thesis is to use this information and to create both a narrative and an environment which includes concepts, mechanisms, processes but also involves feelings. This of course, does not mean that additional literature sources are not consulted.

### 5.2 Cyber Crisis According to Experts

The described crisis model in paragraph 4.1 are geared towards general crisis. In other words, it could be possible to describe any crisis situation with this model. But how about cyber crisis? Even though paragraph 4.2 discussed the helpful characteristics of cybersecurity, it is still unclear what cyber crisis exactly is. The interviewed experts can build on top of the information provided in Chapter 4, to enrich in to a cyber crisis. The interviewees were asked what their definition of crisis was and what cyber crisis then was. Six different experts, six different definitions. This section discusses their answers, specifically, in the light of elements that make a cyber crisis. These are given in a form in which the elements can be incorporated in the game and are called *expert perception of cyber crisis*.

**All Crisis definitions from experts fit the above Crisis model. But focus more on discontinuity.**

The six interviewed cybersecurity experts work in a similar domain, focusing on the management layer of cybersecurity rather than the technical layer. Their definition of crisis, however, is quite different from each other. To give you some insights they defined crisis as:

- “An unexpected event with high impact for an organization requiring immediate organizational response.”
• “An unexpected event which disrupts (parts of) the organization.”
• “The moment in which a company’s operations are discontinued.”
• “An unusual situation in which urgent decisions need to be taken to limit consequences. Several characteristics are: uncertain source, potential impact on the business, quick action and it takes time to get to know the source.”
• “A situation in which direct, urgent measures are required to solve the problem”.
• “An unexpected moment, which largely impacts the availability of service provision and carries financial and reputational consequences. Including both short and long-term consequences.”

What the above definitions show is that the perception from crisis at experts, is not so different from those defined found in literature. Additionally, it’s not only not different, it is just as scattered. Some of these fall under the crisis as a process category and others fall under the crisis as an event category. What is important for the implementation of the crisis model in the simulation game, is that each of the participants needs to recognize some form of crisis. And the common ground between the definitions is that it all starts with an event, moment or situation. In other words, the trigger event as described in the last sections is a suitable representation. Included in their perception of crisis is also that managing the consequences is part of the crisis situation. Therefore, it is also a process.

An often mentioned word by the cybersecurity experts when mentioning crisis is discontinuity. And this somewhere makes sense, as cybersecurity is IT related (CS3). Many of the current organizational services, in which the degree depends of the industry, are dependent on information systems. When something happens with these information systems, critical services are down, and revenues are halted. Additionally, facilities, like IT, affect the way of working for almost all employees as well. Therefore, this could also halt the internal business activities.

Cyber is merely the domain in which Crisis takes place or originates from. During the literature review conducted on crisis, there was a hunch created that a cyber crisis might be quite similar to regular crisis (at least in definition), but originates from a cyber incident. The reason was that no literature was found on cyber related to crisis. The experts mentioned that this made sense. The largest problem was that organizations that were breached did not want to share details on embarrassing events. Therefore, when researchers go into analyzing cyber events at companies, most of the information has to come from media articles.

The experts agreed on the statement that cyber crisis is just another flavor of organizational crisis. After the immediate cyber threat is tackled, the situation evolves into something that is not different from other crisis types. It is believed that a Cyber incident is just a trigger for crisis. In other words, cyber events in isolation are not by definition crises. They mention media management as the logical next step. But like a lot of things, it all depends on the context. Each company has a different value to protect. This can be a combination of anything, be it reputational, financial or assets.

There is high fear of reputational damage.
A large range of examples of crisis events are given by the experts. A grasp: bad intentions of employees to spread bad publicity, breached information from employee hardware that either puts clients under pressure or put them in a negative position, an event which results in the departure of (partial) departments to a competitor, something happens with a client organization which you assessed to be compliant / sufficiently protected and blame you for it, attacks, kidnapped management, mistakes, critical processes disrupted or availability of data is affected. However, it is not these events that escalate a crisis, but the events that follow. As one expert stated: “Any event which results in negative publicity would be bad.” Here is where the link is with why experts think that disruptions should be feared as an organization. They believe that the worst that could happen in an organization are events that force them out of business or close operations. In other words, anything that noticeably gives motivation for any
outside stakeholder to impact the company’s reputation. Both operational and reputational damage have the potential to financially impact the organization, by either stopping revenue creation or loss of trust. Experts believe that negative events will always have a possibility to happen within large organizations. But it is managing the consequences that can keep incidents from escalating. They see reputational damage as the most important one to protect. The notion made is that the external world has a very large impact on crises situations, where the perception of crisis internally is also determined by what happens outside the organization. This includes media, clients, public opinion etc.

A small incident can become a (major) crisis.
Experts often see the events that trigger some organizational crises as small. As said in the section above, hacks and loss of data happen on a daily base, but not all of these become a crisis. These events are often labeled as incidents by practitioners. However, these incidents, when wrongly managed can become a crisis. It is therefore the way that incidents are handled that can turn it into a crisis or not.

Who deals with the Crisis depends on perceived Severity.
When a crisis occurs, there is often an assessment on what the financial and reputational impact is on the organization. This also means looking at the outside world for coverage about the event. Based on the estimated impact, the team is assembled. In other words, there are different severities of crisis. For example, a fire, which is a crisis for some (especially when it's your building), but not for others (the CEO). Therefore, not every crisis situation requires leaders to clear their agenda and focus on the crisis. The severity level is assessed at the place where the event occurs, and escalates either slowly, when it is not clear what is happening or very fast, when it is clear that the impact is very large.

5.2.1 Conclusion: Cyber Crisis according to Experts
From interviewees it can be concluded that crisis definitions do not differ that much from the crisis model. However, it focuses more on discontinuity of IT systems. Additionally, it was agreed that cyber is merely the domain in which crisis takes place or originates from. What became clear is that a high fear of reputational damage exists and that a small incident can become a (major) crisis. These depend strongly on how the crisis is handled by the organization. When potential damages are high, it is the highest level of the organization which needs to solve the problem. These cyber crisis perceptions and some detailed statements are aggregated and summarized in conclusion of this chapter.

5.3 Decision-making and SA questions during a Cyber Crisis
An important aspect that needs to be addressed is the actual decision-making during cyber crisis. As explained in chapter 3, decision-making in crisis situations happen naturalistic decision-making and recognized primed decisions(DM5). In other words, decision-makers classify the situation as an earlier encountered situation, based on the information gained from the environment, to act in a way which suits this (familiar) situation (DM4). The answers from experts link to this very well, as experts explain that crisis decision-making is a chaotic environment in which situation awareness is determined by gathering the facts (SA1). They have to make decisions in light of uncertainty, continuously asking for details and finding out what happened and questions arise for details, as these form the basis for the decision-making (DM2, SA2).

Therefore, the simulated decision-making should ask participants to deal with these type of situations, evoking emotions which are discussed in paragraph 5.6. As discussed in Chapter 3, it is essential for naturalistic decision-making to study the information people are looking for (DM3). The game should be able to provide sufficient information for the participants to keep the information flow going without disrupting the game. Therefore, it is important to prepare for the questions that participants might ask.
Having insights in the types of questions has several advantages. The first is knowing what their questions are during a crisis situation. By knowing this, it is possible to design the game elements in such a way that answers can be given when asked, to keep the flow of the game going. Secondly, these questions can provide input for the action list, mentioned earlier in Chapter 3, by implementing the questions explicitly in the form of actions. In chapter 7 is explained how these elements are implemented in the simulation game design. However, an important notion mentioned on several occasions in this thesis is that the participants themselves decide if they did a good job or not during the simulated crisis. Therefore, the simulation game design does not include such prescribing models (DM3). Participants are asked to make decisions based on experience and knowledge from earlier decision-making (DM4). This choice does not merely stem from the self-evaluative nature of the game, but it also restrains the simulation game from highlighting only certain models and theories from being used, automatically shunning others. Paragraph 4.2, where the details of the cybersecurity domain were discussed, should provide answers for the questions asked by participants.

From the interviews two main categories were identified: scenario related and action related. These two categories have their own impact on the conceptual game design. Scenario related questions are questions related to the details of the situation. In other words, their goal is to gather information for decision-making. In the game, answers to these questions should be available in the scenario either given directly or provided to them by facilitators. That is why these are called scenario related. The second category of questions given by experts, are the action related questions. These are questions for which the Crisis team has to provide answers for. In other words, these are the decisions which the Crisis team has to take during the game, and have to ask scenario related questions for as well. These type of questions are implemented in the game either as implicit choices, or explicit in the action list. The following two sections provide the specific questions mentioned by experts.

5.3.1 Scenario related questions

Assessing the Situation (General Crisis)
- What are we dealing with?
- What are possible consequences?
- Where does it occur?
- When did it happen?
- How did it happen?
- Who is affected by the crisis?
- Who is involved with the crisis?
- Which part of our organization is affected? Was it a Hack or IT disruption?

Assessing the Situation (Cyber)
- Is the leak closed? Are perpetrators out?
- Is the problem contained?
- Can we detect malicious actions on our networks?
- Should we shut down the network?
- Is the threat removed entirely?

5.3.2 Action related questions

Deciding on Strategy
- Do we take charge in this solution or do we delegate?
- Do we need 3rd parties to address the crisis?
- Which strategy do we take?
Priority Setting

- Do we really want to know the impact? Do we want to find out what the impact is?
- Is the situation severe enough to clear my agenda?
- What do we want to protect most in our organization?

Use of Materials / Information

- Do we consider our planning documents? Standard resources and scenarios.
- What do we do with the information that comes from advisors / employees / outside?

Communication

- Are we communicating anything internally, externally? Type of message, timing etc.
- Do we need to inform 3rd parties? (government, regulators, police, Interpol)
- What do our employees have to do?

Most relevant for answering the questions from participants are the scenario related questions. These are the questions in which participants are in search of information, to base their decision-making on. In other words, to build situation awareness. But in a simulation game where questions are not followed by answers, there is a possibility that the flow of the game is disrupted. However, these answers should reflect reality and make sense in the situation at hand. Therefore, the answers and detail to these questions should be readily available to the facilitators in charge of providing information to the participants, but still have some flexibility to be altered.

The design of the simulation game should aim at building a realistic knowledge base of cyber security aspects, by answering questions where needed informed by both the cybersecurity concepts (paragraph 4.2), the scenario considerations (paragraph 4.3) and cyber crisis according to experts. Additionally, these also provide facilitators, perhaps less experienced in the Cyber security domain, a basis which they can rely during play. In other words, answering the above stated questions with the information given in paragraphs 4.2 and 4.3 builds the final set of elements which the designer but also the facilitator can choose from when first creating the scenarios before the game commences but secondly also the narrative during play.

Not all scenario related questions mentioned above need to be answered in high detail, they just have to be present in the scenario. This room for flexibility will be explained in more detail in Chapter 7, when all game elements are described in more detail. Scenario questions that can be detailed out are: Where does it occur? When did it happen? Which part of the organization is affected? Who is affected by the situation? These can be answered in a fairly straightforward manner, by providing participants with this information when asked. They need to be known upfront in the scenario, hidden for the participants and to be found out by gathering information. The other questions require the given background information in the cybersecurity domain or depend heavily on the situation at hand. To be able to coherently explain the use of these questions, they will return in the simulation game design in Chapter 7.

5.4 Stakeholders derived from interviews

In a cyber crisis different stakeholders are involved. To be able to simulate such a situation and be grounded in reality, it is important to know which parties these are and what their role is. It is also the large amounts of stakeholders that increase complexity, especially with a large corporation, as it involves shareholders, business functions, large number of employees etc. These examples are internal
stakeholders, but the external stakeholders should not be forgotten, as they have a major role as was discussed when analyzing the Sony hack (See7, See10). An understanding on these stakeholders, and their responsibilities and or roles within these situations enable participants to take on different roles apart from the ones they have in real-life, when internalized in role and scenario descriptions. All of the experts separated the stakeholders into the group that is part of the crisis solving-team / organizations and the other which is outside of the crisis-solving team or organization, or internal and external stakeholders. The following two sections split the involved stakeholders into these two groups.

5.4.1 Internal

Crisis Team
During the interview with the Crisis management expert, it was clear that every emergency or crisis has its own responsible team, depending on the scale of the situation. When a crisis has immediate (or threat towards a) significant impact on the financial or reputational, decisions are made on the executive level. According to him, a team consists of five people in which the members and their responsibilities differ in different situations. For a cyber crisis on a national level he would include the following five members:

- CEO. Face of the company and main decision-maker.
- Senior Business Leader. Responsible for clients and keeping business functions running.
- CISO (Chief Information Security Officer). Responsible for solving the issue on the technical level.
- Communications / PR. Advising role. Responsible for information, and following the protocol this includes media management.
- Board-member / another member of the executive committee. The expert mentioned no particular role, but mentioned when dealing with large crisis, it involves another senior executive.

Internal Functions
As these senior-managers do not have all knowledge of the problem or domain, the decision-makers are accompanied by their own chosen subject matter experts. The interviewees mentioned the following internal functions as important source of information during a cyber crisis situation:

- IT/ Security. For advice and status on IT infrastructure and its (Cyber) security.
- SOC (Security Operating Center). For advice on detection and fighting Cyber-attacks.
- Company Branches. For advice on the status of the effects on customers and on partnerships.
- Group Incident Management. For advice on how to handle a situation.
- Legal. For advice on the legal consequences, including regulatory follow-up etc. This also includes privacy regulations.
- Risk / BCM. For advice on how to keep/get the systems running again.
- HR. For advice and status on anything regarding employees.
- Communications. For advice on the message to convey and status on how the outside world sees them.
- Finance. For advice and status of financial situations, including budgets and costs.

3rd-party Advisors / Teams
These stakeholders are kept a bit vague on purpose, as it really depends on what the decision-makers want and need at the moment. For example, they could hire any communications expert to help them. On the other side of the spectrum, they could hire cyber security experts to contain or research the problem. Therefore, as all interviewees mention, everyone would ask different questions all depending on what they deem important.
5.4.2 External

Media
One of the three important phases mentioned by the crisis management expert is managing the media. And even mentions it as a very important aspect. This was mainly done to deal with any reputational issues but also to show that the organization is in control. The experts mention it was the fear of the consequences of the media which executives feared. Consequences included loss of trust by the customers, shareholders and partners. There are many types of media, however, none of the interviews went into this aspect. However, the analysis on the Sony Hack from paragraph 4.3 adds a couple of media types.

Regulators
What lies very close to many of the interviewees experience and knowledge is regulatory compliance. One particularly important regarding regulatory compliance in case of a data breach is the mandatory data breach notification. According to this EU regulation, adopted by each member-nation, organizations which are breached need to report this to the national privacy regulator. Failures to notify in a timely manner will face a fine of maximum Eur. 820.000 or 10% of the company’s annual net turnover per violation, whichever is higher (Authorities Persoonsgegevens, (2015, December 30).

Shareholders / Clients
Shareholders and clients might not have a direct say in any direct company decision, they are perceived as important by the interviewees. During the interviews the shareholders and clients were mostly mentioned as “on a notify basis”. In other words, it’s very important to keep them informed, before they start dumping their shares or stop buying products. According to the experts, this can have a domino effect, where others will follow based on fear. Therefore, the Crisis team needs to prevent this from happening.

Partners
This was a recurring stakeholder mentioned by interviewees. In this case, partners mean providers of any services to the organization. Especially when talking IT for larger organizations, there are many providers of services, either hardware or software. Together, these are called the “IT ecosystem” by the experts. But any vulnerability within this ecosystem can become a vulnerability for all organizations connected through these services.

“The General Public”
The general public is mentioned by practitioners as stakeholders that have no financial or emotional connection with the organization. In other words, they are not customers, partners, shareholders etc. However, the general public can influence and be influenced by any media or other persons.

Attackers
Attackers are the ones attacking the organization. Sometimes they also use the media to share demands with the organization, and the outside world. These attackers can both be internal and external, have different skill levels and different motivations. In Chapter 4 attackers were discussed in more detail.

5.4.3 Conclusion: Stakeholders
This paragraph enumerated the stakeholders mentioned during the interviews with experts. There is a clear distinction made between internal and external stakeholders. Some of the stakeholders are (partly) involved in solving the situation, and others should only be notified. External stakeholders include parties like media, shareholders, clients and non-customers. All of the experts believed that these should be
managed in such a way, that reputational consequences are eliminated. Figure 16 depicts the stakeholders discussed in this paragraph. The stakeholders here will be put into context in the next paragraphs when the most important processes and mechanisms are explained.

**Stakeholders**

![Stakeholders Diagram](image)

*Figure 16: Stakeholder Map during Cyber Crisis*

### 5.5 Processes and Mechanisms during Crisis Management

In this paragraph the main processes mentioned by the crisis management expert are described. Together with the stakeholders, these form the basis for the *integral picture* given in the final paragraph of this chapter. The interviewee has over 20 years of experience in crisis management, business continuity and disaster recovery planning. His experiences range from commercial organizations to the military forces. His current responsibility covers the global risk policies and creating awareness and training for crisis managers.

The interview with this crisis expert has been structured differently than the others to optimally make use of his expertise in global risk and creating simulation games. Therefore, the topics covered more procedural aspects, the crisis documents, as well as requirements of the simulation exercise. The interviewee’s expertise was foremost on handling physical crisis, this is the reason why the other six interviews, with cybersecurity experts can enrich the processes described by the crisis management expert. The processes described by the expert are given in 5.5.1 and is followed by 5.5.2 which addresses the additions from the cybersecurity experts on these processes.
5.5.1 Process during Crisis

The interviewee states that during crisis there are a couple of key aspects. These depend strongly on the nature and scale of the crisis. The first aspect the interviewee mentions is the structure of response plans. On the lowest level, a local office can have an emergency response plan (ERP). This ERP has two parts, the first is the paper emergency response plan. Here leaders understand the actions they need to take during the crisis. This includes priorities. For example, human lives are highest in priority over assets. Secondly, the ERP assists crisis managers to assess the situation.

These documents are taken by the crisis management team. These include different members, as discussed in the stakeholders’ section. Again dependent on the scale of the situation, the team comes together within an hour. During this period, the first response to the crisis is determined. Depending on the nature of the crisis, the following response period is more fluid. The team does not necessarily consist of the same persons or functions.

At a certain moment, when the crisis is solved on the regional level, status updates are sent to the global level, when it happens locally. Often, the global crisis team does not meet, but there is constant conversation between them. This depends on threat assessments which are conducted, on reputational and functional effects.

When a crisis has immediate (or threat towards) a significant impact on the financial or reputational, decisions are made on the executive level. The team then would include the CEO, the CISO, and other members of the executive board. The members of the crisis team then pull in their significant subject matter experts.

The steps that should be taken include:

- Getting control of the incident
- Forensics to find out if the problem is actually solved, and find out what happened exactly. The damage has been done, then we have to find out what the scale and nature of the breach is and what do we need to get in business?
- Following is a media management process. Including communication and marketing, focused to protect an organization’s reputation (showing control of crisis). Managing this media is a very important aspect.

The crisis often starts as a perception of we have to protect the business and reputation. Then it follows into a more logical process: we want to know! But still perception driven. Important for the interviewee is putting in all resources possible to plug the breach.

The plans at this moment are mostly reactive in nature and follow a triggering event (the crisis event). But in reality, protocols are less strict and defined. There are too many people involved, for which having a protocol is not effective. The decision-makers however, are advice by experts on crisis situations. Often these experts act 50% on experience, and 50% protocol driven.

5.5.2 Additions from Cyber Security Experts on Decision-Making Processes

From the interviews conducted with cyber security experts, the following additions can be included:

**Incident Discovery**

The discovery of the incident often happens by a person most often from the operational ranks of the organization. This person needs to figure out if the incident needs to be escalated to higher management. There is a trade-off between efficiency and effectiveness here. The earlier you act, the higher the chance
consequences can be lowered. However, crisis teams do not want to spend a lot of time and money when not necessary.

However, when a situation immediately appears serious, the incident needs to be escalated at once. But this should only happen when there is plenty of information available, otherwise decisions will be made based on nothing but hunches. The information is used by the crisis management team to determine if the organization is actually in crisis or not.

Crisis Team Assembles

When a crisis situation is recognized or at least perceived, a crisis team needs to be assembled. These often involve business leaders, communications/PR personnel, CISO and other senior-management personnel like board-members. Different roles are divided in the group, where mostly there is one coordinative person in the group, where the rest are mostly experts from their function.

First Response

The first response contains the first actions taken by the crisis team after the incident is discovered and an impact assessment is conducted. The first response can be divided into first internal action and first communication:

First Internal Action.
During the first internal actions, activities are conducted that create more understanding or solve the problem. Important is to examine the causes of the crisis. Is there a need for external expertise? These types of operations are streamlined when there is a crisis plan / script available. Often this also includes informing employees on how to address this problem publicly.

Specifically, in the case of cyber, when there is a crisis most important is 1) to close the gap / vulnerability and 2) ensure that the perpetrators do not have access any more. The first step is to contain the problem. According to experts, current networks are well-equipped to detect these types of malicious actions on networks. Otherwise, the organization should shut the network down. If they fail to do this, it creates uncertainty, both internally as externally. According to the experts, this is the worst what can happen.

First Communication.
All interviewees mentioned that informing the ones that need to be informed is crucial, both internal and external stakeholders. There are considerations when informing stakeholders. For example, with what information and at which time. Not informing has possible consequences, like uncertainty and public unrest. Informing too quickly can leave open spots or include unjust stories. Therefore, these messages to any stakeholders need to have the right timing.

Planning Documents

Experts believe that basic principles are the same across different crises, however each specific case is different. Therefore, a general guideline is expected in the planning. Without these guidelines, important aspects of crisis management could be forgotten, as one cannot foresee all the needed actions during such chaotic situations. Included are:

• Measures that need to be taken
• Where people have to go or to call
• General outline of the crisis approach
• Steps and procedures
• Procedures or models
5.6 Emotions during Crisis

In line with the perception of crisis is another aspect which has not been addressed so far, are emotions. However, these are part of many of the elements that help build the simulation game. It is emotions which bring an actual game to life, when participants are in the heat of the moment and might forget that they are actually playing a game (Stoppelenburg et al, 2012). Therefore, it is a crucial aspect to address. Most important is what kind of emotions does the game need to evoke to give a realistic feeling of a cyber crisis? From the interviews, the following set of emotions are mentioned:

Uncertainty.
This was the number one emotion that the experts mentioned. Not always using the specific word uncertainty but also: unknowing, more questions than answers, lack of information, what is the best choice? Stuck in the situation, wanting to know what is going on. They all relate to decision-makers that are not ready to take decisions yet, disregarding the source of the uncertainty.

Intuitive Action.
The emotion of intuitive action fits with the situation awareness and recognition primed decisions, discussed in chapter 3. Because of time pressure and stress, decision-makers cannot make the informed decisions that they would like to. Similarly mentioned are: Unclear thinking, irrational thinking and decision-making and inadequately weighed decisions.

Nervousness.
This emotion is a bit less related to decision-making, but more a feeling which takes place on an individual level. There is high uncertainty of what is going on and what the consequences are for the Crisis managers. Include a bit of pressure from the outside and terms like blind panic, stress, adrenaline and increased blood pressure are mentioned.

Pressure from outside.
According to the interviewed experts, there is a strong pressure from the outside world. The outside world are not only their customers, partners and suppliers, but also includes media, blogs, Twitter etc. This puts the spotlight on them to handle the situation. They feel vulnerable and over rushed. A crucial question is: How are we going to explain this to the outside world?

Probably, there are a lot more emotions involved, especially when looking at the scientific mechanisms behind them. However, this is not the goal of this thesis. These emotions are not made explicitly known to participants, but the simulation game has to evoke them in some way. Therefore, the group of four emotion groups can inform the conceptual design well.

5.7 Integral Schema

From the above paragraphs the following models have been created to be simulated in the simulation game. In other words, these are models that are constructed based on the processes and important aspects during dealing with a cyber crisis. These models will be the main simulated models from reality, next to the models already described earlier from theory and from the application domain literature.
5.7.1 Phase I: Discovery and Initial Response

Figure 17: Phase I: Discovery & First Response
5.8 Conclusion: The Practitioners view on dealing with Cyber Crisis

In this chapter, the practitioners view on cyber crisis is depicted. The processes and main mechanisms are derived from interviews from different angles. Together, they form an overview of the process that participants are guided through by playing the game. In other words, it is the general narrative which is created for them in the form of a scenario but also through events and actions is build up upon by themselves. Each simulation game, with a new set of participants, will fill in these elements in different ways. However, this depiction is still on a high level, where it is mostly a designer’s guideline to integrate in the game. It forms an outline of the story the game wants to tell. In other words, it requires filling in the details of the story and the elements around this. When thinking about the simulation game, participants will be situated in a room with each other, talking about a cyber crisis. For this to be completed, all the elements need to be combined into a coherent simulation game. However, to be able to do this, all considerations taken from Chapters 3, 4 and 5 need to be used and incorporated. The following expert perception considerations are derived from the interviews with the experts.
<table>
<thead>
<tr>
<th>No.</th>
<th>Expert Perception Considerations</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td><strong>Cyber Crisis According to Experts</strong></td>
</tr>
<tr>
<td>Exp1</td>
<td>All Crisis definitions from experts fit the described crisis model. But focus more on discontinuity.</td>
</tr>
<tr>
<td>Exp2</td>
<td>Crisis perception starts with an event, moment or situation (<em>trigger event</em>).</td>
</tr>
<tr>
<td>Exp3</td>
<td>Cyber is merely the domain in which crisis takes place or originate from. Therefore, a cyber incident is just a trigger for crisis.</td>
</tr>
<tr>
<td>Exp4</td>
<td>After the immediate cyber threat is tackled, the situation evolves into something that is not different from other crisis types. Cyber events in isolation are not by definition crises.</td>
</tr>
<tr>
<td>Exp5</td>
<td>Each company has a different value to protect. This can be a combination of anything, be it reputational, financial or assets.</td>
</tr>
<tr>
<td>Exp6</td>
<td>There is a high fear of reputational damage. Often it is not the trigger event which escalate a crisis, but the events that follow. Anything that noticeably gives motivation for any outside stakeholder to impact the company’s reputation can force a company out of business.</td>
</tr>
<tr>
<td>Exp7</td>
<td>They see reputational damage as the most important one to protect. The external world has a very large impact on crises situations, where the perception of crisis internally is also determined by what happens outside the organization, including media, clients and public opinion.</td>
</tr>
<tr>
<td>Exp8</td>
<td>A small incident can become a (major) crisis.</td>
</tr>
<tr>
<td>Exp9</td>
<td>Who deals with the crisis depends on perceived severity. An impact assessment is often made before a crisis team assembled.</td>
</tr>
<tr>
<td></td>
<td><strong>Decision-making and SA questions during a Cyber Crisis</strong></td>
</tr>
<tr>
<td>Exp10</td>
<td>Scenario related questions are questions related to the details of the situation. The goal is to gather information for decision-making.</td>
</tr>
<tr>
<td>Exp11</td>
<td>Action related questions are question for which the crisis team has to provide answers for. These are the decisions which the crisis team has to take during the game, and have to ask scenario related questions for as well.</td>
</tr>
<tr>
<td>Exp12</td>
<td>To keep the flow of the simulation game going questions from participants should be followed by answers. Therefore, answers and detail to these questions should be readily available to the facilitators in charge of providing information to the participants, but still have some flexibility to be altered.</td>
</tr>
<tr>
<td>Exp13</td>
<td>Scenario questions that can be detailed out in the scenario are: <em>where does it occur? When did it happen? Which part of the organization is affected? Who is affected by the situation?</em> The other questions require the given background information in the cybersecurity domain.</td>
</tr>
<tr>
<td></td>
<td><strong>Stakeholders</strong></td>
</tr>
<tr>
<td>Exp14</td>
<td>Every emergency or crisis has its own responsible team, depending on the scale. When a crisis has immediate (or threat towards a) significant impact on the financial or reputational, decisions are made on the executive level.</td>
</tr>
<tr>
<td>Exp15</td>
<td>A team consists of five people in which the members and their responsibilities differ in different situations. For a cyber crisis on a national level the following five members are proposed: CEO, Senior Business Leader, CISO, Communications/ PR and Board-member.</td>
</tr>
<tr>
<td>Exp16</td>
<td>As senior-managers do not have all the knowledge of the problem or domain, the decision-makers are accompanied by their own chosen subject matter experts. Experts mention the following internal functions as important source of information during a cyber crisis situation: IT/Security, SOC, Company branches, Group incident management, Risk / BCM, HR, Communications and Finance.</td>
</tr>
<tr>
<td>Exp17</td>
<td>There are 3rd-party advisors / teams involved. Which parties get involved depend on what the</td>
</tr>
<tr>
<td>Exp18</td>
<td>One of the three important phases mentioned by the crisis management expert is managing the media. And is even mentioned as very important. Experts mention it is the fear of the consequences of the media which executives truly feared.</td>
</tr>
<tr>
<td>-------</td>
<td>--------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Exp19</td>
<td>Important regarding regulatory compliance in case of a data breach is the mandatory data breach notification. Organizations which are breached need to report this to the national privacy regulator. Failures to notify in a timely manner will face a fine of maximum Eur. 820,000 or 10% of the company’s annual net turnover per violation, whichever is higher.</td>
</tr>
<tr>
<td>Exp20</td>
<td>Shareholders and clients are perceived as important stakeholders. They are “on a notify basis”, which means it is important to keep them informed during crisis. Experts say that fear can have a domino effect, where clients and shareholders lose trust.</td>
</tr>
<tr>
<td>Exp21</td>
<td>Within the “IT ecosystems” of companies, there are many providers of services, either hardware or software. Any vulnerability within this ecosystem can become a vulnerability for all organizations connected through these services.</td>
</tr>
<tr>
<td>Exp22</td>
<td>The general public is mentioned by practitioners as stakeholders that have no financial or emotional connection with the organization. However, the general public can influence and be influenced by any media or other persons.</td>
</tr>
<tr>
<td>Exp23</td>
<td>Attackers are the ones attacking the organization. Sometimes they also use the media to share demands with the organization, and the outside world.</td>
</tr>
<tr>
<td><strong>Process during Crisis</strong></td>
<td></td>
</tr>
<tr>
<td>Exp24</td>
<td>On the lowest level, a local office can have an emergency plan (ERP). This ERP has two parts, the first is the paper emergency response plan. Here leaders understand the actions they need to take during the crisis. This includes priorities. Secondly, the ERP assists crisis managers to assess the situation.</td>
</tr>
<tr>
<td>Exp25</td>
<td>When a crisis has immediate (or threat towards) a significant impact on the financial or reputational, decisions are made on the executive level. The team would include the CEO, the CISO, and other members of the executive board. The members of the crisis then pull in their significant subject matter experts.</td>
</tr>
<tr>
<td>Exp26</td>
<td>Three important phases of crisis management are: 1) getting control of the incident, 2) forensics to find out if the problem is actually solved, and find out what happened exactly and 3) media management. This includes communication and marketing, focused to protect an organization’s reputation (showing control of crisis). Managing this media is a very important aspect.</td>
</tr>
<tr>
<td>Exp27</td>
<td>The crisis often starts as a perception of we have to protect the business and reputation. Then It follows into a more logical process: we want to know! But this is still perception driven. Important is putting in all resources to plug the breach.</td>
</tr>
<tr>
<td>Exp28</td>
<td>The preparation plans at this moment are mostly reactive in nature and follow a triggering event (the crisis event). But in reality, protocols are less strict and defined. There are too many people involved, for which having a protocol is not effective. The decision-makers however, are advised by experts on crisis situations. Often these experts act 50% on experience, and 50% are protocol driven.</td>
</tr>
<tr>
<td><strong>Additions from cybersecurity experts on Decision-making Processes</strong></td>
<td></td>
</tr>
<tr>
<td>Exp29</td>
<td>The discovery of the incident often happens by a person most often from the operational ranks of the organization. This person needs to figure out if the incident needs to be escalated to higher management. There is a trade-off between efficiency and effectiveness here.</td>
</tr>
<tr>
<td>Exp30</td>
<td>When a situation immediately appears serious, the incident needs to be escalated at once. But this should only happen when there is plenty of information available, otherwise decisions will be made based on nothing but hunches. The information is used by the crisis management team to determine if the organization is actually in crisis or not.</td>
</tr>
<tr>
<td>Exp31</td>
<td>The first response contains the first actions taken by the crisis team after the incident is discovered and an impact assessment is conducted. The first response can be divided into first internal action and first communication.</td>
</tr>
<tr>
<td>Exp32</td>
<td>During the first internal actions, activities are conducted that create more understanding or solve the problem. Important is to examine the causes of the crisis. Specifically, in the case of cyber, when there is a crisis most important is 1) to close the gap / vulnerability and 2) ensure that the perpetrators do not have access any more.</td>
</tr>
<tr>
<td>Exp33</td>
<td>Current networks are well-equipped to detect malicious actions on networks. Otherwise, the organization should shut the network down. If they fail to do this, it creates uncertainty, both internally and externally.</td>
</tr>
<tr>
<td>Exp34</td>
<td>Informing the ones that need to be informed is crucial, both internal and external. There are considerations when informing stakeholders. For example, with what information and at which time. Not informing has possible consequences, like uncertainty and public unrest. Informing too quickly can leave open spots or include unjust stories.</td>
</tr>
<tr>
<td>Exp35</td>
<td>Basic principles are the same across different crises however each specific case is different. Therefore, a general guideline is expected in the planning. Without these guidelines, important aspects of crisis management could be forgotten, as one cannot foresee all the needed actions during such chaotic situations.</td>
</tr>
</tbody>
</table>

**Emotions during crisis**

| Exp35 | Four sets of emotions are mentioned by experts: 1) uncertainty, 2) intuitive action, 3) nervousness and 4) pressure from outside. |
6. Requirements for a Cyber Crisis Simulation Game

From the last chapter we know what games are and which elements can be used to achieve the goal. As a reminder, the objective as stated in chapter 1 again:

To design a simulation game focused on preparing senior-managers for Cyber Crisis, which offers participants a safe environment to practice decision-making and creates awareness. Specifically, the game focuses on two main aspects: 1) the simulation game creates awareness for the concepts and consequences of Cyber Crisis decision-making and 2) offers a realistic simulated environment for participants to practice decision-making under Crisis characteristics like time-pressure and uncertainty.

The above statement shows what the game needs to do with and for participants. Even though its specific enough for earlier chapters, it is not specific enough to actually create a prototype. In other words, two designers can take this objective and come up with a final design which is worlds apart from each other. So what does the designed simulation game actually have to do? What is needed to play the game? And which parts of the application domain will be in the game (and which will be not)? This chapter focuses on these requirements, derived from the seven interviews conducted with experts. It enables to zoom in on their knowledge, and see where the experts believe that a simulation game, in their field can contribute the most. This of course is focused on cyber crisis decision-making situations. In the last three chapters, many inputs have been gathered that can be implemented in the final game design. The requirements derived in this chapter guide the design effort, and make a choice between different inputs. This chapter starts with the methodology of how the requirements are derived from the interviews (6.1). Followed are the three different requirements: functional (6.2), organizational (6.3) and procedural requirements (6.4).

6.1 Method

Following Stoppelenburg et al.’s (2012) approach, there are three types of requirements: 1) functional requirements, 2) organizational requirements and 3) procedural requirements. During the seven interviews conducted, a large set of goals and considerations have been explicitly mentioned. The interview specifically asked interviewees to state the most important requirements that a game should have and considerations that should be taken into account during design. The experts answered the following question: what are the requirements and considerations for a successful implementation of a simulation game that focuses on cyber crisis? As the interviewees have different experiences and expertise’s, the answers vary. However, the answers given can be categorized in six main functional requirements. These are a combination of the mentioned requirements by interviewees, which are given under each aggregated requirement.

For both the organizational and procedural requirements two decision workshops were organized regarding the simulation game requirements. In these two sessions, two practitioners from the same professional services organization as the experts were asked to discuss the requirements that involve 1) the organizational requirements, which are the requirements that define the logistics of the simulation game and 2) the procedural requirements, which address specific game related requirements. The discussed design variables to decide upon are taken from Stoppelenburg et al.’s (2012) game design approach.

6.2 Functional Requirements

This section provides the functional requirements which the game has to address in order to meet the objectives of the simulation game. Functional requirements have the objective to define what a
A simulation game should do with and to the participants (Stoppelenburg et al., 2012), in other words, what are we striving for with the game? These functional requirements are aggregated from the requirements given explicitly by the experts. The mentioned requirements given by the experts are mentioned under the main requirements. There are six functional requirements identified, all have at least two explicitly mentioned requirements from the seven interviewed experts.

**Functional Requirement 1.** The simulation game offers participants to test and assess the effectiveness of the team and preparation plans defined, during times of cyber crisis. These were aggregated from the following requirements given by experts:

1. The game involves testing the team and preparation plans of the organization
2. The effectiveness of the team and the pre-defined plans can be evaluated
3. The game creates awareness for crisis processes
4. The game provides insights on roles involved

**Functional Requirement 2.** Participants are introduced to the complexities linked to cyber crisis and its decision-making. These were aggregated from the following requirements given by experts:

1. The game involves anticipating to the situation at hand
2. The game involves thinking about a problem before taking decisions
3. The game introduces the participants to situations that can occur during a crisis
4. The game shows that there is no best way to solve a crisis situation, as it depends on the characteristics of the situation. However, it is always important to reflect on the decisions.

**Functional Requirement 3.** Participants take notion of the many consequences evolved from their decisions, and that the public opinion takes a major role. In other words, they are under heavy public scrutiny. These were aggregated from the following requirements given by experts:

1. The game involves that their actions are being watched by the public
2. The game shows how small innocent mistakes can cause great damage for the company
3. The game and the simulated consequences inform participants the scale of the problem
4. The game creates awareness of the risks and consequences of (Cyber) crisis
5. The game involves the rule: the one that manages the media best limits consequences
6. Participants understand the speed in which society spreads news in this interconnected world

**Functional Requirement 4.** The simulation game involves group dynamics and emotions. These were aggregated from the following requirements given by experts:

1. The game facilitates that all group members have input and prevent them from hiding their opinion
2. The simulation game addresses emotions under decision-making

**Functional Requirement 5.** The simulation is grounded in reality and provides practice for future situations. These were aggregated from the following requirements given by experts:

1. The simulation game has to be grounded in reality
2. The game offers practice, this increases self-confidence to act in future situations

**Functional Requirement 6.** Participants learn from each other during debriefing. Specifically, focusing on why and how they made decisions during the situation and their consequences. These were aggregated from the following requirements given by experts:

1. The debriefing creates awareness on how participants act in a certain situation
2. The debriefing provides insights in decision-making style and processes
3. The debriefing provides opportunity to reflect and evaluate the course of actions by the participants.
4. Flexibility is required, participants will come up with something which were unexpected.

### 6.3 Organizational Requirements

The functional requirements given above give an overview on what the simulation game should do and bring. However, there are organizational considerations that have to be taken into consideration. These organizational requirements involve: the duration of the simulation game, the number of participants involved, the number of facilitators required (Stoppelburg et al., 2012). In other words, these organizational requirements are the logistical requirements of the simulation game. These requirements influence the outcome of the game design strongly, and therefore have to be considered before going into the actual (prototype) game design. In Stoppelburg et al.’s (2012) method, the focus is strongly on discussing these aspects with the “client organization”. In this case, it is the same professional services organizations as which the experts are part of. Two decision workshops are held to decide on the organizational requirements, which are from Stoppelburg et al.’s (2012) simulation game design methodology as well as from the discussions during the workshops. The outcomes of the discussions were as follows:

**Organizational Requirement 1.** The simulation game will evolve around a fictive organization, in which the scenario and situation is as real as possible. **Functional Requirement 5** states that the simulation game is grounded in reality. However, this requirement is a bit ambiguous, as it still raises the question: *what* needs to be grounded in reality? In my view, there are two main aspects that can be made realistic 1) the scenario/situation and 2) the context. The first requires that the cyber concepts, crisis concepts and their consequences to be realistic. The second requires the game to be made specific for a specific organization. All interviewees believed that the first definitely needs to be realistic. Two interviewees mentioned that each organization requires the incorporation of company specific aspects. To find a common ground to both aspects in reality the following is chosen: the game will evolve around a fictive organization, in which the scenario and situation is as real as possible. This enables the possibility to keep it generalizable, when participants from different organizations are involved, but can be easily tailored to an organization when a group from one organization participates.

**Organizational Requirement 2.** The simulation game can host participants from different organizations and targets senior-managers. As the outcome from a decision workshop it is decided that the game can host participants from different organizations. In earlier chapters it was discussed that the target group is senior-management, that would (in the future) be involved in crisis decision-making. Both the cybersecurity leader with experience in cyber crisis and the crisis management experts indicated that there are around 5 main decision-makers involved. This number will be taken as the max number of decision-makers during the game.

**Organizational Requirement 3.** The number of participants will have a maximum of 10 players. In the above paragraph it is mentioned that the game will involve 5 decision-makers. However, there should be a possibility to extend the game, when there is demand for it. There are several ways to solve this problem. First is to add roles. Second is to enhance already defined roles. As interviewees mentioned, there is a strong involvement from advisors, either internal or external. Therefore, when there are more than 5 participants, the subsequent participants will take the role of the advisor an existing role. However, as can be seen in the functional requirements, the facilitators will have their hands full in observing and reporting on the different game elements. Therefore, not more than 1 extra advisor per decision-maker is allowed. In other words, the maximum amount of participants is 10.
Organizational Requirement 4. The simulation game will have a duration of 4 hours. The target participant is a senior-manager within an organization. In this sense, one can assume that blocking a such a person’s agenda is challenging and can be costly for the organization. Additionally, arranging a number of facilitators for an extensive time can prove costly as well. On the other hand, there need to be enough game-runs to be able to provide both practice and have an extensive debriefing session for evaluation and reflection. During the decision workshop it is decided that the game will take 4 hours in total.

Organizational Requirement 5. Three facilitators will guide the game. From the hosting party, the number of facilitators also need to be taken into consideration. Sending extra personnel will drive extra costs. But having too little facilitators can prove ineffective, especially when all the notes and observations need to be synthesized and evaluated with the participants. Based on the decision workshop the game will have three facilitators:
- 1 facilitator for logistical support and time management
- 1 facilitator will be observing the game and provide the debriefing
- 1 facilitator is the information director from and to the participants

Organizational Requirement 6. The game and the subsequent materials should be understandable in a briefing of around 15 minutes. To also ease the dependencies from a small group of facilitators, the game and the subsequent materials should be easy enough to understand in an explanation of around 15 minutes, both for the participants and for the facilitators. In other words, the briefing should be as short as possible, and any facilitator should be able to pick up the game within a short time span.

Organizational Requirement 7. The game is location independent. Closely related to the target group is the wish to make the game portable. In other words, the number of physical elements should be limited enough to carry to an external organization. This creates flexibility for the facilitators but also for the participating organization(s).

6.4 Procedural Requirements

Given the functional and organizational requirements above, one can subsequently address the procedural requirements. In other words, these are the requirements that address the simulation game elements, that not necessarily have to do with any contextual factors. These are adopted from Stoppelenburg et al.’s (2012) approach and are also discussed during the decision workshops.

Procedural Requirement 1. The participants of the game decide themselves if they did well in the simulation session. For this type of simulation, one filled with uncertain decision-making and its consequences, it is quite a challenge to evaluate. Especially, knowing that from a facilitating point it is also hard to predict what will happen in the future. Therefore, the participant’s effectiveness has to be evaluated by themselves in the reflection and evaluation rounds.

Procedural Requirement 2. The game will guide the participants through discrete time steps of decision-making moments during cyber crisis. One of the most important considerations is if the simulation game will simulate events real-time or in discrete steps. Both have their advantages. For example, when playing in real-time, the realness is represented, including increasing the time-pressure involved. However, when looking at cyber-attacks, like the attack on Sony in 2014 (described in more detail in Chapter 4), one can argue that there is actually little time-pressure involved in cyber crisis. At Sony, hackers were presumed to be present on the network about 6 months to a year before the disruption of the network. As the focus lies on decision-making, the focus should be more guiding the participants through the decisions involved during the entire crisis, instead of just a couple of hours. Therefore, the decision is to involve discrete time steps.
**Procedural Requirement 3.** Participants will be able and are expected to take on different roles than their own in real-life. When roles are drafted, one consideration would be if the roles are being filled with the actual role of the senior-manager or if all participants should be able to take on any role. As explained earlier, the game is required to have some flexibility to be able to host a game for several persons from different organizations. This automatically points towards the choice of the participants should be able to fill multiple roles. An advantage to this is that participants will see some decisions from a different point of view then they normally would, increasing their knowledge to be applied in their own role.

**Procedural Requirement 4.** Participants will cooperatively make decisions to limit the faced consequences. Within gaming there is the concept of winning and losing. However, within a simulation game, this is much more ambiguous. Also in this simulation game, there is no winning and losing. It is of high importance that the participants emerge themselves in cooperative decision-making to limit the consequences they are faced with. In the end they reflect on their actions, team work and emotions.

**Organizational Requirement 5.** The game balances between patronizing and explaining background information. One important consideration is that the interviewees indicated that senior-management often does not know about cybersecurity, either concepts or types of consequences involved. On the other side, these senior-managers are experienced and (probably) intelligent people. Therefore, it is very important to balance patronizing and giving them background information.
6.5 Conclusion: Statement of Requirements

Table 5 summarizes the above mentioned requirements which will be used for the design in Chapter 7.

Table 5: Requirements for the simulation game

<table>
<thead>
<tr>
<th>Requirement Category</th>
<th>Requirement</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Functional Requirements</strong></td>
<td><strong>Functional Requirement 1.</strong> The simulation game offers participants to test and assess the effectiveness of the team and preparation plans defined, during times of cyber crisis.</td>
</tr>
<tr>
<td></td>
<td><strong>Functional Requirement 2.</strong> Participants are introduced to the complexities linked to cyber crisis and its decision-making.</td>
</tr>
<tr>
<td></td>
<td><strong>Functional Requirement 3.</strong> Participants take notion of the many consequences evolved from their decisions, and that the public opinion takes a major role. In other words, they are under heavy public scrutiny.</td>
</tr>
<tr>
<td></td>
<td><strong>Functional Requirement 4.</strong> The simulation game involves group dynamics and emotions.</td>
</tr>
<tr>
<td></td>
<td><strong>Functional Requirement 5.</strong> The simulation is grounded in reality and provides practice for future situations.</td>
</tr>
<tr>
<td></td>
<td><strong>Functional Requirement 6.</strong> Participants learn from each other during debriefing. Specifically, focusing on why and how they made decisions during the situation and their consequences.</td>
</tr>
<tr>
<td><strong>Organizational Requirements</strong></td>
<td><strong>Organizational Requirement 1.</strong> The simulation game will evolve around a fictive organization, in which the scenario and situation is as real as possible.</td>
</tr>
<tr>
<td></td>
<td><strong>Organizational Requirement 2.</strong> The simulation game can host participants from different organizations and targets senior-managers, with a max of five decision makers.</td>
</tr>
<tr>
<td></td>
<td><strong>Organizational Requirement 3.</strong> The number of participants will have a maximum of 10 players.</td>
</tr>
<tr>
<td></td>
<td><strong>Organizational Requirement 4.</strong> The simulation game will have a duration of 4 hours.</td>
</tr>
<tr>
<td></td>
<td><strong>Organizational Requirement 5.</strong> Three facilitators will guide the game.</td>
</tr>
<tr>
<td></td>
<td><strong>Organizational Requirement 6.</strong> The game and the subsequent materials should be understandable in a briefing of around 15 minutes.</td>
</tr>
<tr>
<td></td>
<td><strong>Organizational Requirement 7.</strong> The game is location independent.</td>
</tr>
<tr>
<td><strong>Procedural Requirements</strong></td>
<td><strong>Procedural Requirement 1.</strong> The participants of the game decide themselves if they did well in the simulation session.</td>
</tr>
<tr>
<td></td>
<td><strong>Procedural Requirement 2.</strong> The game will guide the participants through discrete time steps of decision-making moments during cyber crisis.</td>
</tr>
</tbody>
</table>
**Procedural Requirement 3.** Participants will be able and are expected to take on different roles than their own in real-life.

**Procedural Requirement 4.** Participants will cooperatively make decisions to limit the faced consequences.

**Procedural Requirement 5.** The game balances between patronizing and explaining background information.
7. Simulation Game Design: from Requirements, Inputs and Models to Prototype

All previous chapters contributed to this most important chapter, the simulation game design. This chapter ties everything together that has been discussed so far. Chapters 3 until 6 described the models, concepts, theories and perceptions which are the input for the final design. In this chapter, the different designs for the simulation game are given and explicated. This chapter starts with explaining the method used in designing the simulation game in paragraph 7.1. It follows by discussing the conceptual design, the design literally based on the models and other inputs from the previous chapters (7.2). All elements are discussed as well as a reflection on the requirements described in Chapter 6. From there on, it is time to start field testing the simulation game. However, a simulation game cannot be tested purely from a conceptual design, therefore a first prototype is created, based on the conceptual design and will be discussed in paragraph 7.3. It is this moment where the simulation game will not be further informed by models from theory and practice, but will depend on the observations during test sessions. Version 2 of the game will be an improvement based on the observations in test session 1 and will be described in paragraph 7.4. Subsequently, based on this second test session, a final version is given and described in paragraph 7.5. Finally, this final version of the simulation game will be evaluated against the requirements in paragraph 7.6. In the very last paragraph of this chapter (7.7.), the most important decisions made for the simulation game design are discussed.

7.1 Method

Before heading to the description of the game elements, it is good to provide some sort of overview of the steps conducted to get from the requirements to the final design. The seven steps from Stoppelenburg et al. (2012) are given in Chapter 1. In this chapter, the steps 4, 5, 6 and 7 are explained. To remind you which ones they were:

4. Define a Simulation Statement of Requirements
5. Construct the Prototype
6. Test the Prototype
7. Refine and Prepare the Game for Use

The four steps enumerated above will be implemented in this simulation game design as follows:

- Step 4 is a short exercise, where all elements that have been created are summed up in a summary of the game. This summary will be the guidance for the designer to reflect back upon.
- Step 5 is the translation from all the concepts given in previous chapters to a first prototype. First, a conceptual design is given, which is a selection of all elements discussed so far in a conceptual version of the game. This version is not playable yet. In a decision-meeting with the facilitators, choices are made based on reality, feasibility and playability. This results in the first prototype.
- Step 6, is then to take the prototype and test it with a group of participants. This results in observations from both participants, facilitators and designer. This forms the input for some changes to made to the prototype.
- Step 7 is where the changes are implemented and a second game session is held, with different participants. This second version also yields insights, on which the next changes are based upon. Finally, based on the insights from the second game session a final version is described. This step is completed by reflecting the conceptual and final game design upon the requirements described in Chapter 6.
The steps from Stoppelenburg et al. (2012) are strictly of practical use. What needs explicit mentioning is that the simulation game design is not only based upon scientific methods and sources, but following Hevner (2007) also provides insights that can be fed back to the knowledge base. Therefore, a final paragraph is added which discusses the most important decisions made for the simulation game design, these will be further discussed in the evaluation chapter.

7.2 Conceptual Design

After understanding the most important processes and mechanisms, it is time to translate the described processes and mechanisms to simulation game elements. In other words, it is the conceptual design of the game. Duke (1980), which Stoppenlenberg et al (2012) use, mentions twelve game elements as building blocks for game design. These are *format, rules, policy, scenarios, events, roles, decisions, indicators, game steps, symbols and models*. Even though these building blocks cannot always be seen separate from each other, it offers a clear overview of the translation from the schemas and models to a conceptual game. The inputs for the simulation game from Chapters 3 to 6 are used in this chapter and subsequently grouped in Appendix C for overview. This appendix can serve as a reference guide, as it notes the paragraphs from which the consideration has been discussed.

7.2.1 Simulation Statement of Requirements

In this paragraph, as discussed in the methods section, the simulation statement of requirements is given. This simulation statement of requirements is a summary of the most important aspects that this game has to contain based on all the gathered input and is discussed with experts. This summary serves as guidance for both designer and client organizations to reflect back upon in later stages. In other words, this summary can serve as an agreement which reminds the involved what the agreements were. The simulation statement of requirements is as follows:

**Simulation Game Dynamics and Scenario**

The designed simulation game aims to be a realistic representation of a cyber crisis situation (SG1, SG2, SG3, SG4, FReq5). As decided in a decision workshop with experts the simulated environment is a financial organization that has been hacked (OREq1), all explained by a narrative (NAR1). The details of what happened will remain unknown until uncovered by the crisis team, which are responses from facilitators based on participant’s actions. This dynamic mimics the process of situation awareness (SA1, SA6) and plays with continually changing conditions (DM2). Based on the provided information and their situation awareness, the crisis team is responsible for guiding their organization through the crisis, by taking actions and communicating with the public or internally (SA2, SA3). Specifically, the focus lies on protecting the organization’s reputation, while under large external scrutiny (Sce7, Sce10, Exp6).

The above mentioned information could still be any crisis situation. To create a cybersecurity game, the scenario as well as the events and tasks which stem from the scenario are based on found cybersecurity concepts in Chapter 4. The first characteristic is that it takes place in cyberspace (CS1). As mentioned above, the idea is that the start scenario leaves in the middle what actually happens, which enables the decision-making loops. As cybersecurity can be about anything, from information, to machines to computers controlling those machines, all assets are possible targets (CS3). Important that in cybersecurity there is an adversary present (CS2). How the adversaries are worked out will be described in later stages this chapter based on CS5-9. Finally, based on a decision made in a decision workshop, the scenario will focus more on confidentiality than on integrity, availability and resilience (CS4). However, to enhance the uncertainty, this will not be clear from the start. These are important cybersecurity aspects, but there are processes geared towards cyber crisis. Experts were asked about the most important processes and stakeholders. All details on the scenarios and processes are given later in this chapter.
Decision-making under uncertainty

As experts have mentioned during interviews, there are many questions that arise during such situations about the either situations or about actions that the crisis team has to conduct (Exp10, Exp11). To enable this mechanism, an information system that mimics the situation awareness decision-making loop (SA6) is implemented. This information system offers facilitators as well as participants with flexibility for questions that pop up at any moment (Exp13).

Decisions will mostly be based on recognition primed decisions (DM4) which leans on recognizing and classifying the situations and respond to it in the way they deem effective (DM5). To replicate uncertainty situation, the game builds on team situation awareness (TSA1). Different team members will be provided different pieces of information through different sources (Inf1). Combined with other pieces of information, provided to all participants, this will create uncertainty (UN1).

By providing participants with feedback on their decisions the simulation game enables building on the participant’s experience for future situations (DM6). For this reason, the simulation game will not contain any prescriptive models on decision making (DM3), and has as goal to study and reflect upon the decisions made by participants.

In other words, it simulates the crisis processes identified earlier. These processes include stakeholders like shareholders and customers, but most importantly has a role for the media. This media, in a general sense, puts the participants under heavy pressure, to be able to get their story. (DM1)

Learning

Participants will be repeatedly put in the above mentioned decision-making cycle. These repeated cycles enhance the learning for the participants (Learn2). This learning can happen on different aspects, and depends on where the participant lacks experience in (Learn4). In the end, the taken actions from the organization including the articles posted by the media together create a timeline of what went on in the simulation game. In other words, the participants create their own narrative while playing the game. However, it is the reflective action which will complete the learning cycles (Learn3, Learn6). Therefore, an emphasis lies on the debriefing, which addresses not only the decision-making but also emotions (Learn5) and group processes (GrU1). During the simulation game there is not much interference from the facilitators (FAC1), however during debriefing the facilitator plays the important role of going through decisions, group dynamics and emotions, especially when they are dysfunctional (FAC3). This again closes the loop for the learning, by bringing participants back to the situation.

Note that not every aspect or requirement is covered in the above. It serves merely as a summary, which will be elaborated in more detail in the following paragraphs. Given the above mentioned main features of the simulation game, the following paragraphs will focus on ten specific game elements. These are format, rules, policy, scenarios, events, roles, decisions, steps and symbols.

7.2.2 Format: four distinctive phases

The format of a simulation game is the structure of the game (Stoppelenberg, 2012). The simulation game’s format will evolve around Kolb’s (2014) learning cycles (Learn2) and consists of two main phases, similar to the earlier identified processes and mechanisms. For clarity purposes, the description on format is per phase, without specifically specifying the game steps in between. More detail on these will be described in 7.2.8 Decisions and 7.2.10 Game Steps.

As described in Chapter 3, Kolb (and subsequently Thatcher (1990)) use a learning cycle which has four different phases: having a concrete experience, followed by observation of and reflection of that experience, which leads to formation of abstract concepts (analysis) and generalizations (conclusions), which are then used to test hypothesis in further situations, resulting in new experiences. By repeating
this cycle, the new learned behavior can be internalized (Learn2). Learn3 also addresses that within simulation games, the debriefing is of utmost important. Following this theory, the simulation game consists of a briefing, going into the first phase once (first response), is followed by a number of rounds of the second phase (managing the media) and will end with the important briefing round. The four distinct phases are discussed as follows:

**Briefing.** After a short welcome word with the participants, two groups are formed. The first team is the crisis team and the second is the media team. Both teams are guided to their rooms, and will be briefed separately, as both will not be aware of the goals and objectives of the others. In the briefing, both teams are provided with all kinds of information about the situation. These information packages are different, to provide the status quo of the situation of that moment, but not including all details. The decision was made during a decision workshop, in which the experts found it important that preconceptions and objectives were minimally influenced (SA5). Additionally, these different packages create an initial for the need for team situation awareness (TSA1).

**Phase I: Discovery and First Response.** After the briefing, the simulation game starts. The first phase is the discovery and first response as depicted in Figure 19, derived from the interview with the crisis management expert. However, not all aspects of the depicted first phase are translated to the simulation game. In the figure there is a discovery and escalation step, after which a crisis team is assembled. However, as the simulation game starts with having two teams in two rooms, these sub-steps are rather illogical from a scenario point of view. Therefore, the game jumps right in the moment where the crisis team assembles.

Phase I can be seen as a warm up phase. In general, the idea of the decision-making is similar to the second phase, however, the difference is that the participants are offered warm up time to get accustomed to the simulation game and its elements. The game increases in chaos when participants are deemed ready.

The discovery and first response phase is built around the idea that crisis is a perception and introduces participants with crisis characteristics and the feelings involved by using scenarios, events and tasks (NAR1). The goal for both teams is to communicate about the situation with the limited information available, and by doing so form the general public’s opinion. This decision already requires some form of situation awareness from the participants (SA1). In other words: who will gain the public opinion’s first trust? Both have to come up with a first response (crisis team) or publish an exclusive article (media). The idea behind this forcing of action is to recreate three of the four mentioned emotions: uncertainty, intuitive action and nervousness (Exp35).

**Phase II: Managing the Media.** After the first response, the crisis team and media team go into the second phase. This phase aims to simulate the situation awareness aspects (SA6). The simulation game can have one or multiple rounds of this phase (Learn2), where both parties need to gather the needed information (Exp10), from multiple sources (Inf1), set up the new plans (SA2) and communicating these to internal stakeholders and external stakeholders. This is not one particular round, but comprises of multiple cycles of the Kolb’s learning cycle. More detailed information is described in 7.2.10 Game steps.

**Debriefing.** In the debriefing phase, the facilitator guides the participants through their decisions and communications along the way, but do not interfere during play (FAC1). The facilitators then follow the returning to the experience, attending to the feelings and re-evaluating the experience cycle (Learn6). The evaluation is conducted by the participants themselves, by using a designed self-evaluation questionnaire (Learn7). This fits within the naturalistic decision making approach that a crisis situation has to not have prescriptive models (DM3). The main focus of the debriefing will focus on the timeline which is created by the participants (NAR1), which shows the communication between the parties, seen from an external point of view.
7.2.3 Rules

Stoppelenberg et al. (2012) describe rules as elements which cannot be changed by the players. These rules demarcate the simulation game. This section describes the elements which are provided to the
participants as such and in which they have to live by during the simulation game. The rules, as laws for
the game are categorized in these three categories: rules and behavior, Flow of the game and Resources.

Roles and Behavior
Participants do not share the contents of their briefing packages. Players receive a personal
packages containing their role description, objectives, personal coins and knowledge base. All of these
elements, except for the personal coins, are kept secret at any time. This secrecy is to stimulate a situation
in certain participants do have information where the other does not and vice versa. This stimulates
uncertainty (UN1) as well as it creates the need to have look for team situation awareness (TSA1). Personal objectives are strived by the infidel participants, additionally to the shared objectives. This
conflict between objectives is meant to add discomfort and enhance group dynamics different than
cooperative ones (GrU1).

Teams are unaware of the other team's objectives and of the personal ones from team members.
This rule mirrors unknowing the internal goals that any of the teams (might) have, and that this is left
open for speculation (Decided in decision workshop with experts).

Participants are not allowed in each other's rooms. It is not allowed for players to enter the other
team’s room. This reflects the reality of not being able to cross office buildings untimely. However, this
rule is less enforced than others, as would reflect in real life situations (Decided in decision workshop
with experts).

Every communication between both teams are “on the record”. Players are allowed to talk to each
other during the game, but only in the “free zone”. This zone is symbolizing the reality of interviewing
someone on the streets. All of the talks participants will be “on the record” and can be used as wished.
(Decided in decision workshop with experts).

Interviews are held in the “free zone”. There is an area prepared in which scheduled interviews are
held. This makes sure that the facilitator can observe the communication between the participants.
(Decided in decision workshop with experts).

Flow of the Game
There are set moments in time in which actions are enforced. A general timeline is present and
enforced, which introduces events outside the emerging ones. This requires participants to make act,
even though they might not be ready. This general timeline has to be obeyed. This rule lies in line with
that others will tell the story for the company, true or not (Sce10).

When certain actions have not been taken before the specified time, the team is penalized. When
the timeline is not obeyed, subsequent penalties are given to either the team or the individual participant.
Even though the deliverables are not met in time, they are still required (unless specified differently). This
rule is to enforce the above rule.

Resources
Both teams are able to use the advisor pool. There is a common pool of advisors available for both
teams, as depicted by Figure 16 in Chapter 5. These have as function to answer specific questions
regarding the situation. These are represented by documents (described later in the roles, models and
symbols). Both teams are able to tap from this shared pool, however require different actions to get to
the wished information, as this reflects real-life situations. The information provided to both teams will
differ, depending on who asks them. This difference mimics the situation that a colleague would ask instead of a journalist. (Decided in decision workshop with experts).

**Every action costs in a document specified number of resources (symbolized by coins).** No action is free in this game. To put some recognizable value to it, everything will be translated into working with coins. This does not necessarily symbolize money, but the more generalized efforts and efforts to conduct the action. A pricelist is available to indicate the prices for the actions. The actions are paid immediately. The presence of costs is introduced to strengthen the differing personal objectives between participants, as some will receive more and some will receive less resources to spend, shifting power between players.

### 7.2.4 Policy

Stoppelenburg et al. (2012) describe policies similar to rules, however the main difference is that policies can be adjusted by the participants. In general, participants have a lot of freedom as long they are playing within the rules. To illustrate this freedom, five important ones are mentioned briefly. All freedoms were derived during a decision workshop with experts.

**Freedom to use anything that is provided to them.** There are many documents and other sources of information provided to them, either from the start or during play. It is up to the teams to decide what to use and what not, whom to trust or not etc. This fits a situation which could happen in real life.

**Freedom to determine and execute the strategy.** The teams are free to choose their strategy, actions and communication. This can be similar to the crisis documents provided to them, but also completely different. There is no right or wrong in this, neither a ‘best practice’ provided from the facilitators (DM2, DM3).

**Freedom to communicate in the way and to the persons/organizations they wish.** Different ways of communication can have different results. However, what is important is that there are many stakeholders in the participant’s ecosystem that need to be considered. Restricting this would not be realistic. Including this complex network of communication requires simplification in some form. This will be achieved by adding the effect of the action, including the chance effect of not happening as expected, on the pricelist.

**Freedom to decide the timing of the actions.** Both teams are free to publish or communicate their messages and actions when they want. This adds to the dynamics of the game and creates certain unexpected events for the other party. All of these steps have influence on the external parties therefore influencing the status quo which is created by earlier actions.

**Freedom to prioritize goals.** As indicated earlier, there is no definite right or wrong in playing this game. Therefore, there is absolute freedom to prioritize goals. However, individual players are personally being punished for not meeting their own objectives. But within these boundaries, the dynamics of the teams should distill the prioritization of the participants (SA3).

### 7.2.5 Scenarios

As discussed earlier, this game consists of a crisis team and a media team. Even though separated by rooms, there is a shared reason that both groups are involved. In this case, it is the scenario of the crisis team’s company. However, the simulation game can also be seen as two separate games which influence each other. Subsequently, both parts of the game should get their own identity (also to have equal value for time in both rooms). This also involves making the media part of the crisis team’s world and the other way around. Therefore, two separate scenarios are presented to the separate teams. Therefore, the
scenario is described in two different ways: crisis team and media team. Before this, a general description of what exactly happened is given first. But of course, there are events as well. These events go further than the scenarios and disrupt the entire balance of scenario. These events are described under 7.2.6. Events. Note that the scenarios and events are purely fictitious, and (some parts) based on the mental models, cybersecurity concepts, scenario considerations and expert perceptions discussed in chapters 4 to 6.

How did the hack happen? Secret General Scenario

The hackers entered the systems in a very simple, yet patient way. Attackers, which are unknown so far, have entered the systems through spear-phishing. In other words, they targeted a trading manager, sent an email stating it was from the chief of the department with a malicious executable document. As unaware as people sometimes are, the employee clicked and ran the software. This was a piece of malware, that gave certain access to the computer of this particular employee, including e-mail.

The reason why the trading manager was a perfect target, was because it was the main responsible person for 3rd party application called FinAmp, used by all employees to manage trade transactions and administer every detail on these. Importantly, FinAmp was mostly configured by the company itself to stay in control but is developed and maintained by the 3rd party provider.

Even though the trading manager had no specific knowledge of IT systems, she could elevate rights by requesting them to the 3rd party provider by e-mail. The attackers saw their chance, and through e-mail, they requested the elevation to Fines for a number of accounts belonging to lower staff, they had already compromised earlier through normal phishing. Subsequently, they added the confirmation e-mail address to the spam filter so the trading manager would never receive confirmations (or at least, too late).

As before they went into this they had gathered intelligence on the systems and people of the target company, it was very obvious that FinAmp contained vulnerabilities. The attackers would use one of the admin right accounts to install modules to the application, creating a backdoor on the application. This allowed the attackers to get into the systems without having to log in anymore. Here is where the misery started..

Crisis Team Scenario

Fictitious Company. FinCorp. is a Dutch Financial Services Provider, with a stellar reputation among its customers and partners. Everybody loves to do business with FinCorp and business has never been so good. Within the Netherlands it is one of the best known in Commercial Banking, providing a complete range of financial services to companies with at least a yearly revenue of €5 million. Customers often praise the combination of personalized services, expertise and ‘do as you promise’-approach that the company has, making their reputation almost impeccable. Services include all traditional banking activities like lending, supporting transactions but also cash and liquidity management, trade services and treasury-solutions. With their 925 employees, they yield in approximately €145 million last year with a profit of €36.1 million.

It is not all about the money for this Financial Services Provider. Employees and customers relate to FinCorp. due to its presence in society, for example in their sports sponsoring and sustainability. This of course fits in their slogan of Our Reputation is your Asset. This value pays off, this shows by the long list of clients, who mostly have been with FinCorp for decades.

Incident Recovery. After the morning exercise the CEO of FinCorp turns on his phone and received a very interesting call from one of his trusted advisors: “Sir, you might want to see this… I’ve sent you the link via e-mail”. And there it was, a link to Pastebin, saying: “FinCorp, we have your data. You will hear
from us again soon, and we have demands. – Yours Sincerely, Anarchy Angels”. With the link are some example data samples, to back up the claim. The CEO calls the CISO: “Have you seen this? And what is this?”. “Yes... we might have a small crisis here. I’m not sure how serious this it, but it is definitely parts of our data posted”, he says with an absent tone. The CEO acts immediately and decides to get his crisis team together and the CISO. Better be safe than sorry, he thinks.

**Details to be (soon) discovered.** What the crisis team does not know yet is that the media is on their tail, with their own “exclusive” information. What is showing clearly when the event shows up, is that there is murmur inside the company. Also they have heard rumors about that there possibly might have happened something, thinking: “Do the execs even know? Are they hiding something from us?”

The systems seem OK, at least at first. As any Financial Service Organization, there is heavy reliance on IT systems. But they are pretty certain that systems are well-protected. They were not reported any deficiencies in their IT audits for years, and do not expect this to change in the short-term, not with current leadership.

Clearly, the threat level is very uncertain at the moment. There is little information on who it was, where it came from and what they did to our systems. Additionally, when thinking about the CIA-triad, it is definitely not sure if we can assure confidentiality, integrity or availability. We are not sure if the attackers are actually eavesdropping our servers, if they have not tampered our systems or not? What we do know that our systems are still up and running. However, if there is no certainty about the first, the last is worth nothing. But guess what? The attackers are still on the systems.

**Media Team Scenario**

**Fictitious News Paper.** Finance Daily, the most renowned newspaper with focus on economy and business. They were founded in 1812 and by far the leading paper in financial news coverage. However, the turbulent digital era of today has brought sales to decline. It is not only the decline which is visible, but also the editors notice the switch to digital in their work. Everything needs to be read and published as soon as possible. “News spreads so quick, that when you leave your desk for a coffee, it’s old news...” This leaves us in a painful split situation, in which we do have sales targets, but we also want to cover correct news. This correctness cannot be underestimated, because this newspaper has existed for over 200 years, and are being seen as the most reliable source of financial information. Everybody in the financial world reads it, but it is also an often cited source for other newspapers, blogs, tweets etc. In other words, Finance Daily has the challenge to remain high in reputation, but not to fall behind on the “news” in the financial world.

**Youngsters Eager to break through.** To compete in the digital age, not only IT systems were implemented lighting quick, there was a HR strategy switch. Every department would have 2 or 3 traineeship spots to be filled with young and eager talent, to help these departments in news coverage. This on itself does not sound new at all, but what was special about their approach was that these trainees were put on the exact same assignments. At first, the departments were demonstrating, mainly over inefficiency. But as time progressed, it got more clear to them that this worked. The reporters in these traineeship positions were forced to think about, do I work together or take my own path here? Also it raised the level of competition through the roof, news was often quick and correct. Being slow had no rewards, but being fast and incorrect was the worst you could do. This emerging success was implemented through all reporting ranks of Finance Daily, which it strives by today. This changed the culture from a hierarchical newspaper, to a network structured company. All reporters now fall under a small group of editors, which edit and publish the news.

**An unexpected message.** The Internet News department within Finance Daily received the same Pastebin link through e-mail. Knowing Finance Daily’s reputation, this is never going to be enough to
even get a line published. We don’t know who it is, if it’s real or anything... “let’s not get going with this hunch, but you three keep your eyes open on this item. We should not play with FinCorp’s reputation unless we really have something on them” the editor said. The same day, an anonymous e-mail pops up. It is a download request from WeTransfer, 2GB in total, with the message: “I trust you. FinCorp is wrong. Look at the Data, it’s theirs. You get 3 days’ exclusive rights, use it wisely. – Anarchy Angels”.

7.2.6 Events

In Stoppelenburg et al.’s (2012) book, events are seen as disruptions of daily activities of the simulation game. In other words, they are an update of the scenario. In the designed simulation game, there are three kinds of events: 1) general events, 2) events for the specific team and 3) events that are generated by teams that occur as events for the other. These three are discussed in this section, in the form of General Events, Crisis Team Events and Media Events. For an overview, see Figure 20.

General Events

General events are events that are set in stone to happen. As described in the rules section, there are events incorporated to improve the flow of the simulation game. In other words, these events ensure that actions are taken and are provided to both teams (sometimes in different forms).

Rumor has it. (Based on Sce1) External stakeholders are uncertain about their business due to FinCorp’s insecurity and lack of security. This builds up in the first couple of days, including loss in business and increased number of customers threatening to go to competitors. First, they will try to talk with FinCorp but, as uncertainty increases they will keep a very close eye on Finance Daily for their information.

Attackers drip information through public channels. (Based on Sce3) As the information is put online without any limitations, it is up for the grabs. Any source either included in the participants as role or not can access, read and report on this information. Also this can change perception of these roles. It is unclear when it will stop.

Attackers reveal what they want. (Based on Sce5) The hacking group, Anarchy Angels, originate from Russia. However, this is a mystery for all. The main target for the attackers is money. This is not revealed until later in the simulation game, after there is a lot of proof that they hold a lot of data. And as they are not in direct contact with the executives, they are forced to make the claim public, adding a untraceable Bitcoin account.

Imposters make claims. (Based on Sce5) However, imposters who claim to be Anarchy Angels make demands for something else. Think of partnership termination, stepping down of an executive etc.). It will be a challenge for both teams to access the claim of the imposters. Yet again, a Bitcoin account is added.

General Press Conference. At the end of the simulation game, both parties are summoned for a general press release. For both teams, this is the final moment in which they can influence stakeholders. Every participant will have to prepare for this event. This is also the end of the simulation game.

Crisis Team Events

Crisis team events are also come from either the general event line or the media event line, however, these are specifically delivered to the crisis team. Some of these events will take place more often, to repeat to the crisis team that action is still required. What it all boils down to is that these events will give
deadlines to certain actions. All actions have their punishments attached when not acted upon before the deadlines.

**Regulators knock doors.** (Based on *Exp19*) Dutch Regulators keep their eyes open on what happened. According to the ‘meld Licht datalekken’, Dutch organizations need to notify the regulators of data leaks before 72 hours, specifically when the data contained login credentials, financial records, copies of IDs, school or work records, records about religious believes or sexual orientation, and records on a person’s health. When not done in time, a fine of either Euro 820.000 or 10% of the yearly revenue is given.

**Clients get anxious due to rumors.** (Based on *Sce1*) Due to the uncertainty created by the rumors, investors and clients are worried about the situation. They demand information, quick. There will be a questioning of provisioning future contracts. They do not want to do business when certain people are in leadership.

**Media demands answers.** (Based on *Sce7*) Media will definitely talk with the crisis team. If you did not speak to them, they will blame you.

**Systems are shut down.** (Based on *Sce4*) Quite soon in the game, key systems from FinCorp are shut down by the attackers. This event is included to create some internal pressure before the press releases anything. They need to get this running again, next to their crisis management actions.

**Employees need guidance.** (Based on *Sce1*) Employees are also being confronted by clients, media and even friends. But there has been little communication from the executives so far… They are not sure what to do, but sometimes just act as they think is best for the company.

**Media Events**

Similarly, to crisis team events, media events are events that are specifically influencing the media team. Again, these events can happen multiple times. Also punishments are implemented when not adhering to deadlines for some events (where making sense).

**Exclusive information.** (Based on *Sce3*) Attackers sometimes give exclusive information to either the media as a group or individually. Think of private e-mails between several company leaders, or information about what actually happened. Sometimes they will sell the information to them. However, what is clear is that this information is not known to the crisis team (yet). Media can take advantage of this information.

**Doubts over integrity.** Several other credible newspapers and channels have started doubting the involvement of Financial Daily in this story. How do they get this information? Why does nobody else get this insight on the company? Also, they are accused of heavy speculation by some. This might bring the pressure of the crisis team.

**Editors begin to nag.** Editors of Financial Daily see competing newspapers win the battle for news coverage. He promises a big bonus (in the form of reputation) for the one that comes up with a sensational article soon! This needs to be exclusive, true but also quick. The timer starts to run... tick tock.

**Crisis team acts.** Every time the crisis team takes action, the media is there to report upon it. Together, they form a timeline in which readers can follow it continuously. In the end, the timeline is what received a lot of praise from the followers, if done correctly.
Overview of Events

As discussed under the sections the events are not necessarily single events, but can occur more than once in different intensities. It is advice that these events are agreed upon among the facilitators before the simulation game commences. It is even possible that different events occur at the same time. Figure 20 shows how a possible event timeline looks like for the simulation game.

![Event Timeline](image)

**Figure 20: Timelines with Events (example)**

7.2.7 Roles

This section describes the roles involved in the simulation game. In comparison to the schema which was presented in earlier chapters, the following set of characters has been reduced to a set which can be played by a maximum of 10 players. However, the ideal number of players in this case is 8. Similar to the stakeholder schema, the crisis team consists of five characters (Exp15). Additionally, the media team consists of three team members as was decided in a decision workshop. A third category of players in the game are the Non-playable characters. This set of characters are not actually played by participants, but are represented in a symbolized way. These include the internal advisors as well as the external world (Exp16, Exp17).

At last, the stakeholders that are present in the stakeholder map (Figure 15) but not mentioned in these three categories are implicitly involved in the scenarios or events, but do not play an active role in the simulation game. In the following sections the three types of characters are mentioned, especially in terms of description, responsibility (objectives) and knowledge base.

Crisis Team

During crisis the first things need to be managed first, especially if it involves human lives. However, after your first response there are goals that needs to be managed. During crisis situations everything cries for attention, however not everything can be addressed with the same priority. The crisis team has to decide, either upfront or on the spot, in which way and which goals are more important than others. The
following role descriptions are used. Note that the roles are based on the crisis management expert interview, however that the content of each role is fictional and discussed during a decision workshop.

**CEO.**
*Description*
The CEO of FinCorp is a respected leader in the financial world. Most remarkable is that the CEO has during his fifteen-year tenure has never been put into doubt by his people. This while driving the company only forward, making strong decisions every time it was needed.

*Main objective during the game*
The CEO’s responsibility is to keep the reputation at an acceptable level, without depleting the cash reserves that the company has.

**Board-Member.**
*Description*
The board-member in question is a prominent member of the financial world. Several high status positions prepared the Board-member perfectly for this job. This person is the shareholders favorite, as this BM always works hard to cut costs and increases revenue to keep profits up for this year.

*Main objective during the game*
- Communicate to the shareholder as good as possible

**CISO.**
*Description*
The CISO is a security person in heart and soul. Started from a very technical role, the Chief Information Security Officer is now an accepted and very respected governing function within FinCorp. The CISO has been with the company for over 10 years, in different positions. The IT security has never let them down too much. However, there has been drastic changes over the last 10 years in terms of IT decisions, that made the CISO’s job more complex. In other words, some actions have been out of the CISO’s control. Many functions were outsourced, there was a movement from legacy systems to an API (application programmer interface) way of running applications and new infrastructural changes like cloud and VPN were implemented.

*Main objective during the game*
- Ensure that the attackers are not in the systems anymore
- Loose no more than $x million due to the crisis

**Communication / PR.**
*Description*
The communication / PR person is the chief of the communications department. This person has 20+ years experience in press communications and public relations. Over the years, the reputation of FinCorp has definitely been partly due to the great work from the communications department, in which minor events could be reframed into positive messages. However, there has never been a real crisis in this organization. This crisis will be a challenge to keep up with the media out there.

*Main objective during the game*
- End up with a higher reputation than the media.
- Communicate to the outside world as good as possible.
Business Leader.

Description
This person is a true super star within the management ranks of the company. Speculations arise that this client facing leader has what it takes to become the next CEO after the current one will step down. Even though the business leader has been with the company relatively short, he/she managed to go from a starters position to the level just under C-level. What makes this business leader so great is the client-friendly approach. This even resulted in being on the fast-dial for many business leaders. An interesting feature is that this leader thinks about both the long-term business objectives and the short-term objectives, making the business leader also popular among shareholders.

Main objective during the game
- Keep the 2020 business value prediction higher than 90% of contracts
- Keep this year’s revenue at least at 60% of last year’s
- Communicate to the clients as good as possible

Media Team

Media.
As described earlier, Finance Daily is the number one newspaper which focuses on the economy and business. Reputation is most important for them, as sales strive when information is correct. However, this does not necessarily mean that everyone always adheres to this. The three team members that are assigned to this assignment have another price in their mind: Financial Reporter of the Year.

Their Shared objective is to have a higher reputation than FinCorp, by covering this story in a respected way. The end goal is also to create a realistic timeline on what happened during the period the game is played. These will be presented by the media group in the end. Followed with a press conference.

Individual contributions are raised by addressing objectives to be achieved. When completed individually, the full points are awarded to that person. When cooperated for the story, the same amount is added with a bonus and the total is then divided (how they agree) between the authors of the article. An example list:
- Get the first exclusive interview
- Get the first scoop with at least 3 new facts
- Get one depth story: at least 5 new facts
- Release a sensational story with 2 new facts and 1 speculation
- Release at least three articles with at least 2 new facts and 0 speculations
- Bribe an advisor + publish an (anonymous) article about the interview
- Beat the competition when asked to
- Interview a team member in the “free zone” without an appointment (at least one question with an answer)

7.2.8 Decisions
Not all decisions in the game are specifically bound to a specific moment during the simulation game. This depends on the decision to make at hand. As the decision-making in this game is more fluent of nature, and does not follow the same logical path, the decisions are equally unexpected as emphasis is put on naturalistic decision making (DM4). However, there are decisions that each game will have to take for sure. This can be either implicitly or explicitly mentioned during the game. From the expert’s perception hose include:
- Who gets which role?
- Are we in crisis? In other words, do the processes need to be started?
• What is the first response?
• What is most important to protect?
• Are we taking a strategy?
• What information do we require?
• Who do we contact for what?

Because of the fluent nature of the decision-making during this game, it might be more helpful to discuss the options chosen for the participants. As explained in chapter 3, the game will include an action list for each team. On this action list, the actions they can take are included with the resources that they cost. More detail on the action lists are given in version 1. However, Figure 21 shows the decisions that both teams can take.
7.2.9 Game Steps
As explained in the format of the game, game runs exist of four different phases. After the briefing the game starts out with asking participants to decide on next steps and forming a strategy, if they like. From there on, the game follows in a fluent game play, in which there are no distinct rounds. This follows the process as described in chapter 4, as Crisis management is more of a complex communicative process instead of a logical one. The facilitator plays an important role in this, where they are the main sources of information. Additionally, keeping the game rounds flexible has another advantage. Having this, the facilitators keep the freedom to decide when the game should end, and decide to go into the final steps. The last step during the simulation game is always the same, it is a forced press conference. This press conference forces them to synthesize their actions and information and to present it to the general public. Finally, it ends with the debriefing as explained in the format.

7.2.10 Symbols
Symbols according to Stoppelenberg et al. (2012) are representations of reality, but are symbolized in an abstract way by objects in the simulation game. This game has two main symbols.

**Action List.** There are two things that the action lists symbolize. The first is the knowledge that decision-makers have on which actions they can take. Participants might not have experience with taking decisions at this level at all. Therefore, to guide these participants without being too much dependent on participants with experience, options are included. However, the game keeps the option to improvise in decisions as well. The second thing it symbolizes is the resources it takes to do certain actions.

**Coins.** Coins represent the resources and efforts it takes to conduct a certain action. To clarify, coins do not necessarily represent money. These coins also have a limit, which shows participants that they cannot do it all. Additionally, coins give participants hold different values of coins from the beginning. With this it is possible to control the power that participants hold in decisions.

7.3 Version 1: building a Prototype
In a decision-making session with the focal organization, the conceptual design was discussed with two to be facilitators. Important factors for them were realism, feasibility and playability. Therefore, these are main factors in which the implemented elements were discussed against. These factors are all qualitatively discussed. The result of this discussion is the first prototype, to be tested with a group of participants. Followed are the observations made during the game. In the end, the needed changes are mentioned. This paragraph, as well as the next do not go into detail on the elements again, but mention them briefly not to repeat elements all the time. The final design describes the included elements in all detail.

7.3.1 Prototype Design
Simply put, the conceptual design is not a prototype. It does represent all the models from theory and reality but, has no playable form at all. To translate the concepts into a playable game, an abstraction needs to be made from the conceptual design. The first step is to determine which physical game elements are required to play the actual game. The short description of what they contain and how they differ from the conceptual design is given. The following list of elements is derived from the game elements given in the previous conceptual design:

**CEO briefing.** The CEO briefing involves only the information given by the CEO. This information is provided to the player, outside of the Crisis room. This CEO is also the most senior participant from the group. This person then can be an example for the other participants. This person receives the additional
information verbally, and needs to communicate this with the Crisis team members in their own way. This is the start of the simulation game, from which the facilitators take a more conservative role from. The information is part of the facilitators document.

**Crisis Management Documents.** Already located in the Crisis room. These documents are a copy of their own company. A general fictitious one is taken when participants are from different organizations. These documents include emergency planning, business continuity planning and impact assessment documents. Participants are free to use these.

**Action List.** The possible decisions and their relative costs are given with this list. They represent the decision model given in the previous paragraph. After a discussion, this list only contains the number of coins – which means money and efforts and not necessarily money only. The list is simplified as the facilitators were afraid that the game would become too complex. All given prices are relative. During the decision-session a base number was given. When evaluating the other decisions, a relative number was agreed.

**Company description.** The company descriptions are read to them by the facilitators before heading into the game. By doing this, both teams understand the other’s background a bit more. With this, a level playing field is created. This symbolizes the knowledge that they have from the other organization.

**Role Descriptions.** Role descriptions are the five roles that are included into the game. They include their background, role, their objectives and the number of coins they own. The goal is to include objectives that are in competition with each other, while striving for the same general objective as well.

**Coins.** These are owned by the Crisis team to conduct their actions. The first version of the game has exactly 50 coins in play. This is relatively taken next to the action list. The decision was taken to be able to limit the amount of actions that the Crisis team can take during the game and therefore have to think about their actions. The coins are represented as poker chips in the prototype.

**Leaked information.** These are four folders containing extra leaked information. In this first session, they are only provided to the media team, as exclusive information. They include account information, credit card numbers, customer data, HR data, loans data, personal transactions, certificate lists, devices lists, ftp credentials, server credentials, financial models, draft financial reports and an email string. These are all based on the Sony hack as example of which information could be stolen but generated randomly from scratch.

**Facilitators document.** The facilitators document contains the general structure of the game, Room setup, the needed documents for the participants, logging templates and a debriefing guide. They provide the facilitators with all the information that is required to guide the game. These include the theoretical frameworks for logging events.

**Action Log.** This is to document the decisions taken by the participants. This action log is held by the facilitator in the free zone, as this person receives and gives the information to the participants.

**Self-evaluation.** This document is meant for participants to evaluate themselves and the team, before going into the actual debriefing. This brings them to a mindset in which they have thought about their performance before it is lost in the larger discussion. Additionally, this document also contains an evaluation form for the game in general.

**Rules List.** This is a one-pager, containing all rules of the game. The rules of the game are handed out to each participant, as well as available on the Crisis team table.
**Information System.** Instead of cards, like initially thought of for the communication, an information system is implemented that supports the communication between the facilitator and the participants and participants among each other.

**Event Document.** Events are documented in a general document, held by the facilitator dealing with the information flow. This facilitator uses the information system to provide information in the form of an event to the participants. Here, the actions from the participants decide the consequences for the Crisis team. This is far from perfect from the start, therefore another category is included.

**Advisor Pool Information.** A start has been made towards an advisor pool information document. However, it was clear that the number of options were so fast, that this might have been done based on how the game commences. Therefore, there is a large role for the facilitator that provides and receives information from the participants, as this person has to “wing it” from time to time.

**Room Setup**
Ideally, the following set up is chosen for the simulation game. The game requires three separate rooms: *Crisis room, media room and a Free zone.*

![Room Setup during play](image)

**7.3.2 Test Run 1**
With the above elements, the first prototype testing is conducted. This section starts with describing the participants, the location is given which creates a contextual view on the test run. Following this are the changes that are made due to the number of participants and the location. Concluding this section, a reflection is made on each of the mentioned elements and ends with the changes which are needed for the next prototype version.
Participants
In total six participants joined the first test session. This was one less than planned, due to last minute cancellations. Therefore, it was decided that the media room facilitator would join the media team and form a team together with this media player. Most important was to test how the role of the media would feel from a Crisis team perspective. In the end this was not a bad thing, but more on the function of the media in the observations section.

This session had five people with a couple of months of working experience to a maximum of 5 years. They are all from the same department in the organization, but do have different focus in their work. This can differ from manager in the Cyber Security practice, to general IT Risk Assurance (IT Audit).

7.3.3 Observations

Game elements that work well

CEO Briefing. By letting the CEO inform the other team members and take the lead from the start, everybody seemed to take the situation very serious. It is important to make the most senior person CEO.

Action List. The action list was adopted as reality quite soon, including the prices. This Crisis team used the action list also to check what were possible actions to take. It seemed to keep the game flowing. A small addition is that the action should change to opening a line of communication cost $ amounts of coins.

Company Description. Did the job well. Both teams got the feeling of what the other team was trying to portray. Additionally, it set the scene and did not raise any questions.

Self-evaluation. The self-evaluation was fine. During the debriefing they were all speaking and talking about choices and emotions.

Rules List. The simulation game does not seem so strict that rules need to be enforced that much. The game felt more like real-life than a game from an observer point of view. There is no reason to doubt the rule list, however, it might be the case that it is not necessary at all.

Advisor Pool Information. The strongest point, also praised by participants is the interactive nature of the simulation game. This was increased due to the information system present. By having this, the facilitator was able to jump into any information request that participants had. This made the lacking of an advisor pool document better.

Game elements that did not work well

Role Description. Some of the roles seem to be too similar to each other. For example, the board-member and the business-leader seemed to want the same things, not adding any complexity to the actual game. They missed the CFO in this story. Therefore, the board-member will be replaced with the CFO. Additionally, the objectives need to be adjusted to be more contrasting.

Coins. The coins were the biggest discussion point after the game session. The main point was that it was unclear that the coins represented more than just money. This can be because they are represented by poker chips, but it was also not well explained during the game sessions. This should be added to the list, and explicitly mentioned as well. Additionally, the participants wanted to see to which categories they have spent the coins, as discussed in the conceptual design.

Facilitators Document. The facilitators document in the first draft is 17 pages long. Most of these pages are theoretical concepts based on chapter 3. However, during the game it seemed impossible to fill
all these logs in. The facilitator was even forced to take notes in a different document. Therefore, the template needs serious restructuring which helps the facilitator during a hectic game.

**Action Log.** The action log was not used at all due to the chaos in the game. Luckily the information system logs the actions taken by the Crisis team. Therefore, the action log should be removed altogether.

**Game elements that need another run**

**Leaked information.** The many documents were provided to the media team. However, unfortunately these were not used that much. Perhaps this was due to the fact that only one person played the media team. However, next time these should be open to the Crisis team as well.

**Event Document.** It is not particularly the contents of the events, but the way participants are informed about the events. Because of information overload, some events just do not get enough attention. All information was provided through the information system. This should be mixed with telephone calls.

One important addition is that it should be enforced that when participants do not act after an event, they get penalized. From time to time, there was chaos with the facilitators as well, not being able to even enforce on the threats made. In other words, provide less information.

**Crisis Management Documents.** The players skimmed the provided documents provided by them quite some times. The documents used were from their own organization. However, they did not find anything useful. This withheld them from using the documents at all.

### 7.3.4 Changes for version 2

Based on the above observations, a couple of changes need to be made on the prototype. Additional changes are made based on discussions with the facilitators afterwards, these include smaller detailed changes. For the second version of the prototype, the following changes are made:

**CEO briefing.** An extra line of assignment is added: *you are very risk averse, therefore you will ask the team to think of the worst case scenario and prepare for that just in case. This prepares them to at least think about the next steps. However, this will not be enforced.*

**Role Description.** There are quite some smaller changes:

- Lowered the amount of coins owned by the CEO from 33 to 15. Description is the same.
- Changed the objective of the CISO from *establish the extent of the compromise to control the incident from systems.* Additionally, the CISO received more information about the technical systems of the company, called *Security Fact Sheet.* Finally, the CISO received 2 more coins.
- Business leader did not change. Added 2 coins.
- Communications / PR receives one different objective. *Be in control of the message the company conveys (internally and externally) is changed to Open lines of communications with the most important stakeholders and keep them informed.* Also received 2 more coins.
- Board-member is replaced with the CFO: the CFO shares the objective of *keeping the business up and running (retain revenue creation) and as well as retain at least 10 coins.* The CFO gets 15 coins.

**Rule list.** The rule list changes to create more clarity.

- Rule 2 becomes: *Everybody has their own objectives & different amount of coins available to them.*
- Rule 4 becomes: *Every Communication with the outside are “on the record”*
- Rule 5 removed
- Rule 8: *Every action costs a specified number of resources (symbolized by coins). Note this is not just money, but efforts as well.*
Action list. Added are:

- Categories which the spending is decomposed to. These are financial, assets and reputation additional to coins.
- Add a line to the action list: opening a line of communication cost $x$ amounts of coins.
- Action list for the media is completely removed

Media team.

- The media team becomes a facilitators function, as it is not as fun as playing the Crisis team. Additionally, at a certain moment the media was completely ignored. This made this function obsolete at times.
- Becoming a facilitators role, pre-defined events are introduced with the media team, with the articles that have been posted in the first game as basis.

Way of messaging. This is not a game element; however, it is crucial for the communication between the stakeholders.

- In the first session only one laptop was used for the information system. This was instructed as so. However, it seems that more is also possible. In the second version, we ask them to use as much as they deem necessary.
- Additionally, there were personal messages send to them by the information system. However, they did not seem to consider any of these. The second game will introduce calling the participants by telephone instead of sending messages.

Leaked data. Because the disappearance of the media team, the leaked data will be given to the Crisis team as well, so they can assess which data is stolen and what the extent of the breach might be. These are given either as event or after a request from the Crisis team.

Logging template. This is an easier one. The first one might be more following the academic concepts earlier described, but did not prove very helpful in the first test session. The rest of the facilitator document is repeated.

Action log. Removed.

Events. After discussion with the facilitators, it was concluded that the events should be a bit clearer, so that everyone would be able to facilitate the game. Based on some of the events in the first game, the events are more detailed. Giving a message and a deadline for the players. By doing this a time element is included.

7.4 Testing version 2

Given the changes described above, a second version is created. With this version a second a second test session is organized in the exact same way. However, the large change is that the media team is replaced by a facilitator. Therefore, the entire game element of the media team is removed from the game.

7.4.1 Participants

This test session included five participants, all playing in the Crisis team. All participants have over 3 years’ experience, except for one participants, which had 1-year experience. This session hosted two external participants, two founders of a small multi-media company. Important was that there was also one senior-manager who participated from the company’s Cyber Security practice. So during this game session a couple of things can be tested:

- Does the game work for external stakeholders from a different domain?
• Does the game work for senior managers?
• Did the game improve compared to the last version?

7.4.2 Observations on changes

This section does not repeat all the elements again. It only mentions the elements that were changed in the last paragraph, unless specific non-changed elements require revisioning.

CEO briefing. Addition was fine. However, there was a bit confusion in the briefing versus the information available. The description says that the CISO have seen the data, but the CISO does not hold any of the data. This needs to be changed in the scenario.

Role Description. Again the biggest discussion point. Balancing the roles and their objectives is still a challenging task. In this game, some players even felt paralyzed due to the received number of coins against the number of coins that something costs. Especially the CISO, where the technical actions take quite some coins against the low number that this player receives. Additionally, when comparing to the last session, the players were more geared towards their personal objectives instead of helping. In the previous session, the players seemed to care less about their own objectives.

In hindsight, the CFO got too much coins. As the objective was to remain a certain amount of coins, this person’s only task was to hold on to his or her own coins. The number of coins need to be shifted.

Rule list. Good Addition. No further comments.

Action list. The addition does not work. First, the participants do not matter that much during the game. Secondly, it requires another facilitator to log these actions. Therefore, the action list should be the same as it was. The prices do seem to make sense for the participants, as they played along with them without asking questions about it.

Media team. Good Addition. The media is clearly a facilitators function.

Way of messaging. By adding telephone calls to convey events, it added an extra layer of complexity. However, this did challenge the Crisis Team a lot more, as they could not just leave the telephone ringing. This addition, requires even more well-informed facilitators.

Additionally, adding more screens also raised the level of chaos. The addition made here is that they can have as much screens as they like during the game. They have to manage the situation with it.

Leaked data. Added another dimension, but also created a lot of chaos. This needs to be structured a lot more. It can be replaced with a simulation of a hacker that leaks information in different runs instead of all at once.

Logging template. Simplified version worked very well for the facilitator.

Events. The new events worked well. The challenge though is to not be too much busy as facilitators.

7.4.3 Changes for the Final Version

The changes made from version 1 to version 2 seem to be good additions. The biggest concern still are the roles and their power compared to each other. There is quite some shifting still needed to balance it out. This might be an aspect that is never perfect. However, this can be improved after each session.
However, for the scope of this thesis, no next test is being done. The following adjustments are made for the final game:

- **Shifting of the coins.** CISO should get more, and the CFO should get less.
- **Change the coins.** The poker chips too much resemble money.
- **Action list.** Return to the old format, with the same decisions as the version 2 one.
- **Change the scenario to which it closes the loop.** The discovery of the event should be via the media, and not internally.
- **Leaked data.** Structure in such a way that it seems like a hacker leaking data in different runs. These will be broken down into four parts: 1) accounts, credit card, customer, HR, loans, and a couple of personal data documents, 2) Technical data documents, 3) Financial Models and 4) An embarrassing e-mail string.

### 7.5 Final Version: Cyber Crisis Simulation Game

The above mentioned changes are incorporated and discussed in this paragraph.

#### 7.5.1 Game objective

The designed simulation game focuses on preparing senior-managers for cyber crisis, by offering them a safe environment to practice decision-making in and create awareness. This awareness is for the concepts and consequences of cyber crisis decision-making. Additionally, this game offers participants to practice their decision-making under crisis characteristics. This effect is modelled by immersing participants into a new world, in which a cyber crisis has occurred. The crisis team is asked to steer their organization out of the crisis and take crucial decisions, taking them through the process of crisis and crisis management. However, information is not readily available and pressure from outside is very high. The simulation game leans heavily on interaction between participants and the ‘outside world’ creating chaos and inducing the feelings involved in Crisis situations.

#### 7.5.2 Game Session

The game is played with five players plus three facilitators. The game is situated in two separate rooms. The first room is for the Crisis team, where they sit around a table. The second room is for the facilitator playing the media team. The role of the three facilitators are as follows:

- **Facilitator in Crisis Room.** Observes the game and guides the learning process during debriefing. Actions during the game are limited to rule enforcement and receiving coins.
- **Facilitator controlling the information.** An intensive role, responsible for communicating events, tasks and responses based on the actions taken by the Crisis team. Also situated in the Crisis room. In other words, this facilitator is responsible for keeping the game flowing.
- **Facilitator playing the media.** Situated in the media room. Is responsible for simulating the media, and the ‘outside world’ by making telephone calls.

The game session is depicted in the game session storyboard on page 126. The game starts with a general briefing. First words of welcome are given, including the purpose of the game. The rules are introduced which after the company descriptions are read out loud to the participants by the facilitator in the Crisis Room. Followed is a quick explanation on the information system, stating that they have the freedom to display it with the number of computers they wish.
Participants choose their role. However, the CEO has been selected beforehand, which will be taken apart by the Crisis room facilitator to give the CEO briefing. From this point on, the participants are in the lead of the simulation game. This is where the game starts.

The crisis team goes into Phase I: Discovery and First action. Little additional information is provided to them. Here they can decide to conduct a strategy or to gather more information. They are unaware about the objectives and actions that will follow from the Media Room. Facilitators can then decide when to drop the first article. When this article is published, the game flows into the next phase.

Phase II: Managing the Media starts. Different events and tasks are given to them including phone calls, messages and other news articles. This is a fluent process, in which the facilitator responsible for the information is responding to what happens in the Crisis room and Media room. This person has the responsibility to keep the game flowing.

When it is time, facilitators can communicate that a final press conference is planned, where the participants will have to explain to the general public what happened. This is the end of the simulation game. Before the actual press release takes place, the participants fill in the self-evaluation, to prepare them for the debriefing afterwards. After the press release ends, the debriefing starts. The Crisis team goes through the created timelines and discuss the tasks, procedures and methods, process (or interaction) and emotions. This involves all the observations made including the self-reflection which is done by the participants. An important theoretical cycle to address by the facilitator is: returning to the experience, attending to feelings and re-evaluating the experience.
The game starts with a general briefing. First words of welcome are given, including the purpose of the game. The rules are introduced which after the company descriptions are read out loud to the participants by the facilitator in the crisis room.
PHASE 1: DISCOVERY & FIRST ACTION

I received a message that raised my concern.

CEO takes the lead and communicates about received information.

Is it our data... who is affected...

Finance Daily publishes first article about the hack.

You're only concerned about yourself.

We need to protect the A-list clients.
PHASE II: MANAGING THE MEDIA

PRESSURE FROM OUTSIDE: the news has reached the public. The crisis team is overwhelmed with phone calls, messages and emails from concerned customers, partners and employees.

INTERNAL DISCUSSIONS: the team has to decide what the priorities are and which demands they will meet. This does not come easy as everybody has their own agenda.

DECISION MAKING: the team is forced to take action even though under heavy pressure, uncertainty and competing interests. Be careful, there will be consequences.

PRESS CONFERENCE

Notification of press conference

Prepare for press conference

Giving a press conference
DEBRIEFING

Before the actual debriefing starts the participants fill in a self-evaluation form. They are forced to think about the topics before they head into the debriefing phase.

The facilitator guides the participants to the actions, decisions and emotions that were observed during the simulation game as well as the important topics raised by the participants.

The participants leave the crisis room more experienced and aware of cyber crisis.
7.5.3 Game Scenarios

How did the hack happen? General Scenario (for facilitators)

The hackers entered the systems in a very simple, yet patient way. Attackers, which are unknown so far, have entered the systems through spear-phishing. In other words, they targeted a trading manager, sent an email stating it was from the chief of the department with a malicious executable document. As unaware as people sometimes are, the employee clicked and ran the software. This was a piece of malware, that gave certain access to the computer of this particular employee, including e-mail.

The reason why the trading manager was a perfect target, was because it was the main responsible person for 3rd party application called FinAmp, used by all employees to manage trade transactions and administer every detail on these. Importantly, FinAmp was mostly configured by the company itself to stay in control but is developed and maintained by the 3rd party provider.

Even though the trading manager had no specific knowledge of IT systems, she could elevate rights by requesting them to the 3rd party provider by e-mail. The attackers saw their chance, and through e-mail, they requested the elevation to FinAmp for a number of accounts belonging to lower staff, they had already compromised earlier through normal phishing. Subsequently, they added the confirmation e-mail address to the spam filter so the trading manager would never receive confirmations (or at least, too late).

As before they went into this they had gathered intelligence on the systems and people of the target company, it was very obvious that FinAmp contained vulnerabilities. The attackers would use one of the admin right accounts to install modules to the application, creating a backdoor on the application. This allowed the attackers to get into the systems without having to log in anymore. Here is where the misery started.

Details to be (soon) discovered. What the crisis team does not know yet is that the media is on their tail, with their own “exclusive” information. What is showing clearly when the event shows up, is that there is murmur inside the company. Also they have heard rumors about that there possibly might have happened something, thinking: “Do the execs even know? Are they hiding something from us?”

The systems seem OK, at least at first. As any Financial Service Organization, there is heavy reliance on IT systems. But they are pretty certain that systems are well-protected. They were not reported any deficiencies in their IT audits for years, and do not expect this to change in the short-term, not with current leadership.

Clearly, the threat level is very uncertain at the moment. There is little information on who it was, where it came from and what they did to our systems. Additionally, when thinking about the CIA-triad, it is definitely not sure if we can assure confidentiality, integrity or availability. We are not sure if the attackers are actually eavesdropping our servers, if they have not tampered our systems or not? What we do know that our systems are still up and running. However, if there is no certainty about the first, the last is worth nothing. But guess what? The attackers are still on the systems.

Crisis Team Scenario

Fictitious Company. FinCorp. is a Dutch Financial Services Provider, with a stellar reputation among its customers and partners. Everybody loves to do business with FinCorp and business has never been so good. Within the Netherlands it is one of the best known in Commercial Banking, providing a complete range of financial services to companies with at least a yearly revenue of €5 million. Customers often praise the combination of personalized services, expertise and ‘do as you promise’-approach that the company has, making their reputation almost impeccable. Services include all traditional banking activities like lending, supporting transactions but also cash and liquidity management, trade services and treasury-
solutions. With their 925 employees, they yield in approximately €145 million last year with a profit of €36.1 million.

It is not all about the money for this Financial Services Provider. Employees and customers relate to FinCorp due to its presence in society, for example in their sports sponsoring and sustainability. This of course fits in their slogan of Our Reputation is your Asset. This value pays off, this shows by the long list of clients, who mostly have been with FinCorp for decades.

**CEO briefing.** After the morning exercise the CEO of FinCorp turns on his/her phone and received a very interesting call from one of his/her trusted advisors: “You might want to see this… I've sent you the link via e-mail”. And there it was, a link to Pastebin, saying: “FinCorp, we have your data. You will hear from us again soon, and we have demands. – Yours Sincerely, Anarchy Angels”. With the link are some example data samples, to back up the claim. The CEO calls the CISO: “Have you seen this? And what is this?” “No I have no idea…! I'm not sure how serious this it, but we have to do something about it”, he says with an absent tone. The CEO acts immediately and decides to get his crisis team together and the CISO. Better be safe than sorry, he thinks.

**Assignment:** You are very risk averse, therefore you will ask the team to think of the worst case scenario and prepare for that just in case.

**Media Team Scenario**

**Fictitious News Paper.** Finance Daily, the most renowned newspaper with focus on economy and business. They were founded in 1812 and by far the leading paper in financial news coverage. However, the turbulent digital era of today has brought sales to decline. It is not only the decline which is visible, but also the editors notice the switch to digital in their work. Everything needs to be read and published as soon as possible. “News spreads so quick, that when you leave your desk for a coffee, it’s old news...” This leaves us in a painful split situation, in which we do have sales targets, but we also want to cover correct news. This correctness cannot be underestimated, because this newspaper has existed for over 200 years, and are being seen as the most reliable source of financial information. Everybody in the financial world reads it, but it is also an often cited source for other newspapers, blogs, tweets etc. In other words, Finance Daily has the challenge to remain high in reputation, but not to fall behind on the “news” in the financial world.

7.5.4 **Rules**

1. Participants do not share the contents of their briefing packages.
2. Everybody has their own objectives & different amount of coins available to them.
3. Every communication with the outside world are “on the record”.
4. When certain actions have not been taken before the specified time, the team is penalized.
5. Every action costs a specific number of resources (symbolized by coins. Note that these do not only represent money, but also efforts).
6. The action list is not exhaustive. You are free to conduct in a natural way. Facilitators are free to put a price on the actions.

7.5.5 **Role Description and objectives**

The following role descriptions are provided by the players. All are required to keep the contents of their envelopes secret.

**Chief Executive Officer (CEO)**
Description. The CEO of FinCorp is a respected leader in the financial world. Most remarkable is that the CEO has during his fifteen-year tenure has never been put into doubt by his people. This while driving the company only forward, making strong decisions every time it was needed.

Objectives.
1. Retain an acceptable Reputation

Coins. 15

Chief Information Security Officer (CISO)
Description. The CISO is a security person in heart and soul. Started from a very technical role, the Chief Information Security Officer is now an accepted and very respected governing function within FinCorp. The CISO has been with the company for over 10 years, in different positions. The IT security has never let them down too much. However, some actions have been out of the CISO’s control due to increasing complexity.

Objectives.
1. Control the Incident (from Systems)

Coins. 15

Business Leader
Description. This person is a true super star within the management ranks of the company. Speculations arise that this client facing leader has what it takes to become the next CEO after the current one will step down. What makes this business leader so great is the client-friendly approach. This even resulted in being on the fast-dial for many business leaders. An interesting feature is that this leader thinks about both the long-term business objectives and the short-term objectives, making the business leader also popular among shareholders.

Objectives.
1. Establish a line of communication to the clients (make sure they are not neglected)
2. Protect client confidentiality

Coins. 5

Communication / PR
Description. The communication / PR person is the chief of the communications department. This person has 20+ year’s experience in press communications and public relations. Over the years, the reputation of FinCorp has definitely been partly due to the great work from the communications department, in which minor events could be reframed into positive messages.

Objectives.
1. Create an honest and open image
2. Open lines of communication with the most important stakeholders and keep them informed

Coins. 5
Chief Financial Officer (CFO)

Description. The CFO in question is a prominent member of the financial world. Several high status positions prepared the CFO perfectly for this job. This person is the shareholders favorite, as this CFO always works hard to cut costs and increases revenue to keep profits up for this year.

Objectives.
1. Keep the business up and running (retain revenue creation)
2. Retain at least 15 coins (all combined)

Coins. 10

7.5.6 Events / Tasks

A number of events are present in the game. The events are provided by the facilitator responsible for the information. There is complete freedom from the facilitator to throw the events, except for the first and the last. These two are always the same for each game session. It can be even the case that due to the flow of the game, not all events are passed. An important condition is that they have to make sense at the time of playing.

Rumor has it (definitely the first).

<table>
<thead>
<tr>
<th>Provide to:</th>
<th>Crisis Team - CEO</th>
</tr>
</thead>
<tbody>
<tr>
<td>Message:</td>
<td>Give the CEO the briefing. This will contain the information which require the situation. The CEO has to explain why the team is called together. They receive their first message, from the business that customers are emailing and calling to ask what / if there is something going on...</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Action</th>
<th>Response</th>
<th>Time Delay</th>
</tr>
</thead>
<tbody>
<tr>
<td>Wait</td>
<td>Nothing</td>
<td>None</td>
</tr>
<tr>
<td>Request Information</td>
<td>Nobody knows about anything... so response is short and brief...</td>
<td>5 minutes</td>
</tr>
<tr>
<td>Other</td>
<td>Depending on the situation</td>
<td>Depending on the situation</td>
</tr>
</tbody>
</table>

Note: the media team already has more information and started their research

Customers and Partners complain

<table>
<thead>
<tr>
<th>Provide to:</th>
<th>Crisis Team – Business Leader</th>
</tr>
</thead>
<tbody>
<tr>
<td>Message:</td>
<td>Pressure from the outside. Call the business leader, with the message: “Hello …, your secretary here... I have been called 40 times already from our biggest accounts. They want to know what information is available. What do I tell them?? Please communicate this through the communication portal. You have 15 minutes. Please act.”</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Action</th>
<th>Response</th>
<th>Time Delay</th>
</tr>
</thead>
<tbody>
<tr>
<td>Passing</td>
<td>A sigh of relieve...</td>
<td>None</td>
</tr>
<tr>
<td>Failing</td>
<td>The team will lose 5 coins</td>
<td>15 minutes</td>
</tr>
</tbody>
</table>

Note: This should increase pressure from the participants.

3rd Party message: Sorry that we did not inform you
Provide to: Crisis Team – CISO

Message:
One piece of information. Call the CISO, with the message: “Hey this is Tech Daily. We’ve developed and maintain the following applications for you: SWAN, FINAMP, BROW and MCTH. They all use the same backbone, and we found out that there are some vulnerabilities in all of them that haven’t been spotted earlier. Sorry that we have mentioned so late. Hope this is fine.”

SWAN: communications tool with deliveries (partner portal)
FINAMP: Predictive financial models. (Internal)
BROW: clients check their investments through this portal (client-facing)
MCTH: links several personal identifiable documents together (internal)

Shut these down until the situation is stabilized! You have 20 minutes

<table>
<thead>
<tr>
<th>Action</th>
<th>Response</th>
<th>Time Delay</th>
</tr>
</thead>
<tbody>
<tr>
<td>Passing</td>
<td>A sigh of relieve..</td>
<td>None</td>
</tr>
<tr>
<td>Failing</td>
<td>The team will lose 7 coins</td>
<td>20 minutes</td>
</tr>
</tbody>
</table>

Note: This guides them into a certain direction.

Shareholder Pressure

Provide to: Crisis Team – CFO

Message:
Pressure from the outside. Call the CFO, with the message: “Hello …, your secretary here... I have been called 40 times already from our shareholders. They want to know how bad the situations is? What do I tell them?? Please communicate this through the communication portal. You have 15 minutes. Please act.”

<table>
<thead>
<tr>
<th>Action</th>
<th>Response</th>
<th>Time Delay</th>
</tr>
</thead>
<tbody>
<tr>
<td>Passing</td>
<td>A sigh of relieve..</td>
<td>None</td>
</tr>
<tr>
<td>Failing</td>
<td>The team will lose 5 coins</td>
<td>15 minutes</td>
</tr>
</tbody>
</table>

Note: This should increase pressure from the participants.

Internal employees ask how to handle

Provide to: Crisis Team – Communication / PR

Message:
“Hi…., This is your deputy calling. We receive a lot of calls regarding a statement from your side. But we do not know which way to respond. What do we have to tell them and which message do you want to convey??” You have 15 minutes – communicate through the portal.

<table>
<thead>
<tr>
<th>Action</th>
<th>Response</th>
<th>Time Delay</th>
</tr>
</thead>
<tbody>
<tr>
<td>Wait</td>
<td>Nothing</td>
<td>None</td>
</tr>
<tr>
<td>Offer information</td>
<td>The communication will continue like this. And any other communication should be weighted with this one.</td>
<td>15 minutes</td>
</tr>
<tr>
<td>None provided</td>
<td>Lose 7 coins. There is more uncertainty inside the information.</td>
<td>15 minutes</td>
</tr>
</tbody>
</table>
Note: Asks them to communicate their strategy.

Attackers reveal what they want

Provide to: Crisis Team & Media Team

Message:

We have shown you want we have.. you might be wondering WHY?? Well you have money, we want it. Simple as that. Transfer 300 coins in bitcoins to 0d10bf887eb68afa422ba799a7ee38e59a422ecd. We give you 15 minutes to decide what to do. We will stop if you do.. otherwise.. we will keep going.

<table>
<thead>
<tr>
<th>Action</th>
<th>Response</th>
<th>Time Delay</th>
</tr>
</thead>
<tbody>
<tr>
<td>Wait</td>
<td>Drop another data bomb</td>
<td>20 minutes</td>
</tr>
<tr>
<td>Pay</td>
<td>Say thanks! But still drop a bomb after 25 minutes</td>
<td>25 minutes</td>
</tr>
<tr>
<td>Request Information</td>
<td>Nobody knows about anything... so response is short and brief.</td>
<td>5 minutes</td>
</tr>
<tr>
<td>Investigate internally</td>
<td>We have no idea what they have.. it could be everything, but could be nothing</td>
<td>15 minutes</td>
</tr>
<tr>
<td>Communicate</td>
<td>Depends on the situation</td>
<td>Depending on the situation</td>
</tr>
<tr>
<td>Other</td>
<td>Depends on the situation</td>
<td>Depending on the situation</td>
</tr>
</tbody>
</table>

Note:

Imposters make claims

Provide to: Crisis Team & Media Team

Message:

This might be an interesting proposition to you. We have seen you are investing heavily in Nucleon. But they are crooks! They provide weapons for war zones. Even though it seems that you make quite a bit of money on them, we want you to quit your collaboration. Call them now, to cancel your contract.. otherwise we will continue the terror.

<table>
<thead>
<tr>
<th>Action</th>
<th>Response</th>
<th>Time Delay</th>
</tr>
</thead>
<tbody>
<tr>
<td>Wait</td>
<td>Nothing</td>
<td>None</td>
</tr>
<tr>
<td>Call Nucleo</td>
<td>Nucleo gets mad and walks to the media</td>
<td>10 minutes</td>
</tr>
<tr>
<td>Request Information</td>
<td>Provide them with the relationship with Nucleo. They are clearly not the best relationship you have. But you make over 10 million euros yearly only on this account.</td>
<td>5 minutes</td>
</tr>
<tr>
<td>Communicate</td>
<td>Depends on the situation</td>
<td>Depending on the situation</td>
</tr>
<tr>
<td>Other</td>
<td>Depends on the situation</td>
<td>Depending on the situation</td>
</tr>
</tbody>
</table>

Note:

Prepare for the Press Release

Provide to: Crisis Team & Media Team

Message:
We cannot wait any longer. Press is on our tail and we really need to provide some answers to the general public.

Everybody has to write up a press release! They all need to be ready for the questions. Media prepares 5 questions each.

<table>
<thead>
<tr>
<th>Action</th>
<th>Response</th>
<th>Time Delay</th>
</tr>
</thead>
<tbody>
<tr>
<td>They have to prepare</td>
<td>We decide randomly who has to give the press release</td>
<td>15 minutes</td>
</tr>
</tbody>
</table>

Note:

Regulators knock doors

Provide to: Crisis Team (CEO)

Message:

Shouldn’t you notify us??????? If this turns out to be huge, you will hear from us soon. You have 10 minutes.

<table>
<thead>
<tr>
<th>Action</th>
<th>Response</th>
<th>Time Delay</th>
</tr>
</thead>
<tbody>
<tr>
<td>Wait</td>
<td>Nothing</td>
<td>Fine! 10% of their coins</td>
</tr>
<tr>
<td>Inform</td>
<td>Provide which information</td>
<td>5 minutes</td>
</tr>
<tr>
<td>Other</td>
<td>Depending on the situation</td>
<td>Depending on the situation</td>
</tr>
</tbody>
</table>

Note: This is something they should do!

Regulators knock doors

➢ Media Demands answers

Provide to: Crisis Team – Communications / PR

Message:

What's going on!? We know this is happening, but they haven't informed anybody about ANYTHING.. we suspect that something deeper is going on. Please elaborate. (Phone call)

<table>
<thead>
<tr>
<th>Action</th>
<th>Response</th>
<th>Time Delay</th>
</tr>
</thead>
<tbody>
<tr>
<td>Wait</td>
<td>Media is free to speculate</td>
<td>Depends on MT</td>
</tr>
<tr>
<td>Inform</td>
<td>Good – Media can take that into account</td>
<td>Depends on MT</td>
</tr>
<tr>
<td>Other</td>
<td>Depending on the situation</td>
<td>Depending on the situation</td>
</tr>
</tbody>
</table>

Note:

7.5.7 Decisions

Getting advice from anyone in the advisor pool (internal). This action opens up a communication line with the person they wish. Who they want to speak about what is for them to decide. The facilitator responsible for the information provides them with the wished information, based on the general scenario of the hack. This sounds vague, however this proved very effective, as it is a flexible way to keep the game going without having to determine all information up front.
**Hire a 3rd – party advisor.** The Crisis team has to negotiate with a 3rd party advisor of their wishing, to conduct an activity as they like. A realistic response needs to be given.

**Investigate Internally.** A call for internal actions to investigate the problem. They have to specify who and what they want to have investigated. The response is a bullet point style executive summary about the problem.

**Shut Systems Down.** This shuts down the entire network from the internet. Response is that all internal and external services are down, following a big storm from media, clients, customers and partners

**Isolate Systems Partially.** This shuts down certain parts of the network. This makes sense when they have received part of the leaked data and the event on which application might be a problem. Again, response is internal and external services going down (only not all), following a smaller storm from media, clients, customers and partners (depends on who is effected).

**Issue an embargoed press release.** This means buying time for the Crisis team. With this action, the Crisis team shares exclusive information with the press in exchange for a delay of publication. The terms need to be decided in negotiation.

**Respond to open letter to newspaper.** This is in response to any article posted by the media team. Responses from internal and external stakeholders depend on the contents of the open letter.

**Request Exclusive interview with the media to tell your story (you reserve the right to edit the message).** This gives the participants the opportunity to tell their story, as well as give the media team an exclusive, which they really want.

**Release Press release on own website.** This is a communication tool for them to communicate to many stakeholders at the same time. Again, responses depend on the contents of the message.

**Any other communication.** This gives them the opportunity to go outside the given options. So when their experience or gut feeling tells them they should do something else, this is possible.

### 7.5.8 Information System

A very important aspect of this simulation game is the information system, used to support communication between the facilitators and participants. This information system simulates pressure from outside, from the media and informs them while they are making decisions. This is a dynamic alternative for playing cards.

The Crisis team, the facilitator in the media room and the facilitator controlling the information all have their own portal from which they can communicate from. This communication tool has the form of a web application, which can be accessed from anywhere with any computer, mobile phone or tablet (assuming there is internet). There are seven different “views” which can be used by the participants, depicted in Figure 23. For the screenshots of the views, see Appendix D.
Crisis team views

1. **Crisis team messages.** These are the messages received from the facilitator. These are color coded on the sort information received.
2. **Crisis Center.** This view enables to communicate their actions to the facilitators. They specify what they want and can add comments.

Media room views

3. **Media Center.** The facilitator can write up articles about the FinCorp hack here and publish them.
4. **Separate Articles.** Once published, the there is an automatic link created to the separate article. This article is then reachable publicly.
5. **FinCorp Hack Timeline.** Once published, the article is also added to the FinCorp hack timeline, which contains all the articles.

Facilitator controlling information views

6. **Received Messages from Crisis Team.** Here the facilitators receive the actions taken by the Crisis team.
7. **Facilitator Center.** The facilitator can write messages to both the Crisis team as well as the media team. This is the main information sharing tool.

### 7.6 Reflection on Requirements

This chapter described the game elements that are designed based on the vast input given in the previous chapters. It is a translation from the conceptual to an actual playable simulation game. Important is how the final game design addresses the requirements derived in chapter 4.
Functional Requirements

**Functional Requirement 1.** The simulation game offers participants to test and assess the effectiveness of the team and preparation plans, during times of cyber crisis.

**PASS / FAIL.** A simulation environment has been created that simulates reality. To be able to test and assess the preparation plans, Crisis management documents are added. Ideally, these are the ones from the test group’s organization. However, given the chaos of the situation, most of the participants did not take a look at the documents at all. To actually test the plans, the game should focus more on the steps inside the plans instead of the situation. In other words, if the game was issued from a crisis management department, it would focus more on going through the different steps.

Additionally, from the start of the game the crisis team is asked to take decisions. They are challenged by events and tasks which are thrown at them. Again, there are no prescriptive decision making models provided by them, as this fits the naturalistic decision making. During the debriefing there is a strong focus on reflecting the decision making by the participants. Also here more focus could be on the actual decision making steps.

Taking both together, this simulation game does meet the requirement where it creates the possibility to assess and test both aspects. However, the clear choice is taken to not force participants within a certain direction, but to have the situation as fluent and realistic as possible. As an effect this game in itself cannot provide conclusive answers on if either an organization’s crisis team or preparation plans are effective, and requires adjustments.

**Functional Requirement 2.** Participants are introduced to the complexities linked to cyber crises and decision-making.

**PASS.** The simulation game aims to mimic the mechanisms and procedures as realistic as possible. The following elements within the game aim to offer complexity to participants:

*Advisor Pool Information*
The participants are free to open even line of communication to any department in their company, and subsequently ask for additional information. This mimics the internal information gathering involved with crisis. However, answers are delayed, not fully true or completely wrong. This asks participants to also weigh these answers from the advisor’s pool before they take actions.

*Event Document*
The event document adds more complexity to the situation as it disrupts the situation awareness or decision making at the moment an event is pushed. These events require action under time pressure, which sometimes means that the task they had at hand needs to be dropped or is forgotten altogether.

*Leaked Information*
More complexity is added by dripping the leaked information in stages. These packages of information offer insights in what has happened, however they also take away resources from the crisis team.

*Role Description*
The secretive personal objectives, with their resources are introduced to increase the complexity on a group decision making level. By adding these, a “second agenda” is created for each participant. Therefore, it becomes not purely a cooperative game, but also has competitive aspects in them.

*Coins*
Another element that adds to the complexity of decision making is having coins. These coins represent both resources, not necessarily financial but also time and effort. These coins limit the possibilities for the participants, as everything has a price and therefore not all options can be pursued. Having coins
therefore adds complexity in the crisis team decision making, as it forces them to prioritize both actions as objectives.

Information System
The final element that adds to complexity is the information system. This system connects the crisis team with the “outside world”, including the media company. Through the messaging system they will receive constant updates on the system (mimicking the decision-making loop from Endsley), as well as access to news articles written about the hack.

Functional Requirement 3. Participants take notion of the many consequences evolved from their decisions, and that the public opinion takes a major role.
PASS. This requirement is ingrained in the dynamics of this simulation game. When there is action from the crisis team, there is a suited response. This is a piece of flexibility that challenges facilitators, but also the participants by giving them information that fits their actions. This all happens through the information system and by angry phone calls, messages and news articles.

Functional Requirement 4. The simulation game involves group dynamics and emotions.
PASS. The simulation game, the roles, the tasks, the events and the narrative are all focused on being in a group process and aim to induce the emotions described earlier. These all, again, should aim for the highest level of realism, including the information that is returned from the actions conducted by the participants. Included into the game is that role descriptions have a certain level of slightly contradictory objectives and different power levels.

Functional Requirement 5. The Simulation game is grounded in reality and provides practice for future situations.
PASS. This is an aspect which received a lot of attention during previous chapters. Every aspect so far tries to build onto a level of realism for participants. This includes models, concepts and feelings. Participants found the simulation game very realistic, especially due to the interactivity that the simulation game brings.

Functional Requirement 6. Participants learn from each other during debriefing. Specifically, focusing on why and how they made decisions during the situation and their consequences.
PASS. This is more a requirement which form follows function. In other words, the structure of the game is influenced by this requirement. The game therefore, is set up in a way that participants have control and have the main say in the debriefing.

Organizational Requirements
Organizational Requirement 1. The simulation game will evolve around a fictive organization, in which the scenario and situation is as real as possible.
PASS. The narratives, events and tasks all evolve around a fictitious organization, data roles etc. These are all informed by the details of cyber security, the Sony hack and the interviews with experts.

Organizational Requirement 2. The simulation game can host participants from different organizations and targets senior-managers, with a max of five decision makers.
PASS. The game focuses on roles that are senior-managers in the fictitious organization, including their role within a crisis situation. However, this does not particularly say that the game cannot be played by other types of participants, therefore this it is also suitable for participants from different organizations.

Organizational Requirement 3. The number of participants will have a maximum of 10 players.
PASS. However, important to know that with the removal of the media team, there are less slots available. When there are more players involved, then they form a team to play a particular role. For
example, if there is a sixth player, this player will share the role of CISO. After testing the simulation game, the game is still optimally played with exactly five participants.

Organizational Requirement 4. The simulation game will have a duration of 4 hours.
PASS. The simulation in the proposed form has a duration between 3.5 and 4 hours in total. First the game starts with a general briefing, which takes about 15 minutes. Secondly, the CEO is taken out of the room and is briefed separately. At the same time, the participants are explained how the information system works. These two simultaneous steps take about 15 minutes. The main part of the game, are multiple decision-making rounds which adds up to about 2 hours and ends with a press conference, which takes about 15 minutes. This leaves around 75 minutes for the debriefing, which is suitable as the main learning takes place here.

Organizational Requirement 5. Three facilitators will guide the game.
PASS. In the conceptual design three different facilitators should be part of the game. The first one facilitates in the crisis room, noting the decisions etc. The second facilitates the media room, which controls the information given to the media team and the third is the one responsible for conveying the information from and to both teams. This includes additional information, responses to their actions and general messages. With the final design, it will be very hard to facilitate this game with less facilitators.

Organizational Requirement 6. The game and the subsequent materials should be understandable in a briefing of around 15 minutes.
PASS. The scenarios and role descriptions are designed to be short narratives, which should bring the participants right in the simulated environment. During both test sessions, little questions were raised about the scenario. However, the role descriptions seem more challenging. The descriptions do seem to work but sometimes prove to need tweaking, which has to continually be done after more testing.

Organizational Requirement 7. The game will be location independent.
PASS. To be able to carry this game to different organizations, instead of relying on one physical location, the game should be portable. Therefore, the games setup is that all the elements of the game can be carried. Additionally, any business meeting room would be fine, as long as all participants are able to sit in a room for the debriefing. Additionally, the web application requires no extra carrying of stuff. The only things that are required is a stack of paper (with all manuals), coins and a couple of computers to run the information system. The information system is a web application; therefore, Internet is also required.

Procedural Requirements
Procedural Requirement 1. The participants of the game decide themselves if they did well in simulation game.
PASS. This requirement structures the game from the start. The format of this game, therefore, is structured like this. This openness in evaluation of the process also gets them thinking about their personal but also the team’s performance. It starts with a self-evaluation, which follows with a general discussion about decision-making, emotions and group processes.

Procedural Requirement 2. The game will guide the participants through the discrete time steps of decision-making moments during Cyber Crisis.
FAIL. From the findings in both the theoretical and the application domain, it seems a wrong assumption to take the decision-making in crisis as discrete steps. Therefore, as shown by the processes from experts, these will be continuous, as this is more natural for this type of problems.

Procedural Requirement 3. Participants will be able and are expected to take on different roles than their own in real-life.
PASS. Every role description is set up in a way that this creates a different personality than they are themselves. It contains a general story of this character in the company and what their responsibilities are. These are aimed that the participant forgets their own assumptions on certain things and adopt this character internally. This requirement is strongly up for prototype testing.

Procedural Requirement 4. Participants will cooperatively make decisions to limit the faced consequences.
PASS. In simulating the real process this requirement is inevitable. The participants are put into this scenario from the start. This requirement is inherently present in the game setup. In the end, the participants have the shared goal to get their organization out of crisis and to save the organization’s reputation. Additionally, there are competitive additions like personal goals. These are meant to spice up the group discussions.

Procedural Requirement 4. The game balances between patronizing and explaining background information.
PASS. The simulation game includes different levels of implicit knowledge. These are input from the application domain. Elements that contain background information implicitly are: 1) the action lists, which contain the decisions and their relative costs, 2) narratives that tell the story in a more general and business manner than more technical and 3) the role descriptions have background information for their particular role.

### 7.7 Conclusion: Simulation Game Design

This chapter focused on the design of the simulation game from concept to actual prototype. Most of the requirements discussed in Chapter 6 are met by the design. Adding to meeting these are the design choices made. The previous paragraphs contain numerous design aspects, which are too abundant to reflect upon in this conclusive section. Even though there are many choices made, which influence the design in some way or another, there is one design key design choice that deserves more attention here. It is realism versus control. This is a decision between two aspects that have proven a lot of tension in the design of the simulation game. From simulation game literature as well as indicated by experts, realism is one of the most important aspects of such a simulation game. Therefore, a lot of focus has been put on this feature. After two tests the realism in the game is praised by participants. This realism is created by many elements in the game. First there is the complexity, which is incorporated in many different ways as the events, coins, secrecy of documents and role descriptions among others. Second, interactivity is created by adding a media team, having stakeholders represented by facilitators and communications through the information system. Third, flexibility is created by enabling decision making in their way, like communicating to departments in the way they feel is best. This fits the naturalistic decision making described in Chapter 3. Last that add up to the realism is emotions. The scenarios and many events have been geared towards creating emotions for participants. One example is where the facilitator acts as an angry client in a direct phone call to one of the decision-makers.

However, this choice to incorporate realism has a downside: loss of control. This loss of control can be seen in many ways. The first is that there is the loss of control over how participants make decisions. There are no particular models incorporated, and leave the participants open for decision-making which they are familiar with. Also there is no control over which steps they take to solve the crisis, as well as the documents and information they use to do so. This is not necessarily a bad thing, but it does mean that there is no control over what participants actually learn. In other words, even though there is learning involved, there are no insights in which aspects are actually learned. Therefore, only an assumption exists that when participants note they have learned something, the game has served its goal. An additional loss of control due to the realism is the loss of control over the game by the facilitators. The increased interactivity and complexity makes it a tough game to facilitate, for all three. They have to switch activities constantly and keep up with the
crisis team. Facilitators have the opportunity to send events and force action, participants still control the speed of the game by their actions.

The realism might be the greatest strength of this simulation game. The lack of control might be the greatest weakness of this simulation game. To find out how the game is actually perceived by the participants a self-evaluation is conducted. The first aspect is the perceived usefulness for the participants. The second aspect is to find out if the mechanisms are present in the game as designed and how these are observed by facilitators.

8. Evaluation of test sessions

As discussed in earlier chapters, a designed artifact is only useful when it is implemented in the right way. So even though the requirements are met, it is important to evaluate the product by playing the actual game. The idea for the evaluation stems from Klabbers (2009). In his view on usefulness, a simulation game is both assessed on how well it simulates and models reality as well as on how well it induces the learning. Therefore, the simulation game is evaluated on its perceived usefulness. In other words, how the participants see the usefulness of the simulation game.

For the perceived dynamics a self-evaluation form is used. This form can be found in the Appendix on page 179. This particular form has been composed based on the theoretical concepts, mostly based on learning in Chapter 3. After the test game sessions, the participants filled in a self-evaluation form. This form is first of all used to prepare the participants for the debriefing. As some of the answers from the participants are very short, the answers are enriched with observations made during the play of the simulation game. In total ten participants played the sessions. This chapter discusses the results of the self-evaluation.

8.1 Perceived Usefulness

The usefulness of the game is only practically useful, when it is perceived this way by participants (Winter, 2008). In other words, do the participants think this game helps in preparing senior-managers for cyber crisis? Some of the answers from the participants are quite short. These answers are enriched with the observations made during playing the simulation game. Therefore, there are two observations used 1) from the participants from the self-evaluation form and 2) from the facilitators observations during the simulation game.

8.1.1 Emotions

Emotions were mentioned as very important by different scholars (Learn5, NAR3). Both game test sessions were taking place in the same physical location, even the rooms were exactly the same. However, both game test sessions could not be more different in terms of emotions. It is likely that given that there are five completely different participants present, that the situation is going to be different as well. However, what nine out of ten participants agreed upon was that emotions were part of the experience. In their answers, the participants mostly mentioned pressure, stress and chaos. As the two test sessions were very different in emotions, both are mentioned separately here. These examples show that in both occasions, the emotions were definitely present.

Test session 1.
In test session 1, the crisis team formed a team from the start. This can be because they all know each other and have worked together before, as well as they only had one laptop for the communication and a big screen which they used for the incoming information. When the CEO entered the room, the discussion immediately started on what kind of data was stolen. Knowing that they should have acted, the uncertainty seems to increase the stress level as well. Especially, when the first news article was posted,
nervousness was sensible in the room. They were unsure how to handle this situation, especially what the “best decision” was. Discussions included many different lines of reasoning going at the same time, creating more uncertainty. At certain moments the crisis team made promises, however did not follow up and just forgot about the promises. A nice moment was when someone said “I don’t know that much”, which caused irritation with the other team members. When technical details were uncovered by the team, they had to make a decision on shutting down the entire network or just partially. This cause a big conflict inside the room. Two participants were in favor of one option where the other two participants were in favor of the other. The CEO at that moment was called away, which made the situation even more heated. In this conflict the two parties were shouting at each other why their option would be the best, however in the end no decisions were taken. The nervousness came back again when it was announced they had to prepare a press release, where again they were uncertain about what they could use and say.

Test session 2.
The second test session seemed a lot more chaotic and disorganized. First of all, the team composition was different from the previous session. This time, two external participants joined, which had no experience in IT risk in any form. This session also started with the uncertainty about the type of data and if it was really theirs. However, the discussion at the beginning was about team mates explaining that certain stuff was just not possible. An example was: “Can’t we just take the information from the internet? That solves the problem right?” The unknowingness of some participants caused a bit of irritation with the CEO, which wanted to solve the question instead of organizing his team.

A new element compared to the first test session are the phone calls, which were disrupting the Crisis team’s discussions. This element caused even more uncertainty, as the person had to transfer the information from the phone to the other team members. During the phone call, again annoyance stating things like “Is he making a press statement?” Followed was an absolute surprise when they read in an article: “We asked a number of Financial Institutions if this situation was theirs, all denied, except for FinCorp. They stated that they are investigating the situation”. This increased watchfulness for the communication.

During the game, players were confused now and then, mostly because they wondered how the puzzle pieces would fit together to formulate what actually happened. This was also caused by the CISO who got hung up on technical details. In the end, the CEO and the CFO met outside the Crisis room to discuss if the CISO should have been fired or not, as they thought he did not do his job correctly. But on the other hand, the CISO felt he was paralyzed in his actions due to the low number of resources.

8.1.2 Experienced based decision making
In crisis situations the decision-making moves to a more naturalistic decision making style (DM2). In such dynamic situations strategies often change due to changing information (DM3). This naturalistic style of decision-making was seen in the first test session. The participants also indicated that they based their decisions on the information given, and less on experience. The result was that the first test session was drastically more responsive to the events than the second session. However, the second group used a more recognition primed decision making style, where they mostly used their experience to classify the situation (DM5) rather than discussing options. The participants in the second session all answered that they used their experience rather than the information received. It was expected that these styles of decision-making would be present, as discussed in Chapters 3 and 7.

This difference could be because of the way information is provided to them. In the first session, the information was purely communicated through the information system. In the second, telephone calls were added to the mix. When comparing the two games, the first crisis team was more organized where
the second was disorganized and chaotic. The difference here is that because of the single point of information, the first crisis team was mostly responsive and acted upon anything that was given to them.

The second session was forced to prioritize and structure the information more due to the large amounts of information. But as one participant mentioned “[I acted] Mostly on information given and what seems logical to do.” And it is exactly this implicit recognizing a situation and deciding, what is aimed to simulate (recognition primed decisions).

8.1.3 Enjoyability

An important factor for playing this game is having fun playing the game. This keeps them motivated, and should not feel they are doing work. All participants mentioned in the questionnaire that they had fun during the game. However different answers were given why. Some addressed their feelings, like just felt good, nervous, stress as discussed in the emotions section. Others enjoyed the learning experience. Others liked the fact that in comparison with a lot of simulation games they have played in the past that this one had a high level of interaction, realism and action. One liked the challenge of the puzzle that needs to be resolved. In observation, no participant seemed to be bored in the process and sometimes needed a break from the intensity. As participants were from different organizations, and have different backgrounds and experience, it can be concluded that it is an enjoyable game for all types of participants.

Interestingly, no particular participant evaluated that they did a good job in guiding their organization out of crisis. The two CEO’s were the most positive about their performance giving themselves a 6.5 on average (out of 10). So it is hard to imagine that their perceived performance contributes to the enjoyability of the simulation game.

8.1.4 Engagement

Next to enjoyability is asked how engaged they were during the game. Both sessions seemed very engaged from start to end, but differently. As discussed earlier, in the first test session the crisis team acted more as one team. All players participated in discussions and decision-making. In their evaluation they mentioned the realism and growing into their role as factors that increased their engagement. However, one critical observation was that this first session was also distracted by doing other activities like personal work, and walking away to take personal calls. Even though this happened only a couple of times, it did seem like some were not completely focused on the simulation game.

The second session was completely different in how engaged people were. Nobody was doing other things, and were busy with the game and its elements for the entire time. However, their answers were different on the question regarding engagement. As explained earlier, this test session was more chaotic and disorganized. This was reflected in their answers, as their answers were in a large range of perceptions compared to the first session. However, there was one particular participant that felt paralyzed for the actions he had to take, where nobody would help and chip in to pay for the action. At a certain moment, this had a reflection on his engagement. In other words, the roles descriptions and decision power of participants can have a large influence on the individual engagement levels.

8.1.5 Challenge Level

Another aspect included in the questionnaire was the perceived challenge level. This seems an aspect which they all agree upon: it is very challenging. The participants mention new experience containing many aspects, tough due to the interactivity, a lot of changes within the game, managing people. Additionally, people mentioned going into the skin of a certain role challenged them as well including stepping into this new world, which brings them outside of their comfort zone. From observations, participants and teams did seem challenged, where this sometimes even lead to frustration, as things did not go perfectly for them. Additionally, when the debriefing starts, there is a sigh of relieve going through the room. What can be
concluded in combination with what has been mentioned above is that the challenge level is at the level that it is still enjoyable.

8.1.6 Awareness

One of the main goals is to increase awareness of cyber crisis concepts. In this research, these concepts are found in part II. But did the participants actually gained any knowledge about the concepts or stakeholders that would be involved during playing this simulation game? Important to know is that it is not logged which of the concepts or aspects are learned by the participants nor discussed, merely if they perceive it as happened or not. The below statistics discuss the different concepts linked to the awareness. What becomes clear is that the simulation game definitely raises awareness on concepts. However, it is impossible with this evaluation method to know which aspects increased for participants.

Cyber Security Concepts / Stakeholders. Seven out of ten participants evaluated that they have learned about Cyber Security concepts and Stakeholders.

Crisis Management Concepts / Stakeholders. Nine out of ten participants evaluated that they have learned about Crisis Management Concepts / Stakeholders.

Crisis Management process. All ten participants evaluated that they have learned at least some aspects of the Crisis Management process.

In the literature review in chapter 3, the following aspects were found to learn about regarding decision-making aspects:

- **Potential consequences.** Seven out of ten participants evaluated that they learned about potential consequences of their decision making.
- **Uncertainty.** Six out of ten participants evaluated that they learned about uncertainty of decision making.
- **Risks of decision-making.** Eight out of ten participants evaluated that they learned about the risks of decision-making.
- **Potential Rewards.** Zero out of ten participants evaluated that they learned about potential rewards of decision-making.
- **Benefits.** Zero out of ten participants evaluated that they learned about benefits of decision-making.
- **Risks.** Four out of ten participants evaluated that they learned about risks.

8.1.7 Would they approach the game differently the next time?

Aimed with this question is to see if in reflection, they have learned anything from their actions as a group. By answering yes, there is some form of awareness created. Again, this is implied as there is no control over what has been learned by evaluating the simulation game this way. All of the participants answered that they would approach the game differently the second time they would play it. Answers predominantly include structure of the crisis management process. Examples are splitting roles better and think things through, too much time is spent on debating on what is happening instead of actions, more structured and some approach need to be more specific. And it is this question that sparks quite some discussion during the debriefing. Reflecting on the team offers them an opportunity to discuss what went wrong, without specifically talking about themselves individually. Therefore, the debriefing is a great tool to discuss the lessons learned, which confirms Thatcher (1990).
8.1.8 Realism
All participants perceived the simulation as very realistic, even though there were game elements included like paper instructions, poker coins and action lists. It was the interactivity in decision-making, created by the information system and phone calls to participants that seem to pull them right into the new created world. It can be assumed that the models are then implemented in the correct manner. From observation there is little to add to this, except that everything from the start has been to simulate a cyber crisis as realistic as possible, which was only just created by adding layers of complexity, like the information system, instead of the company information etc. All participants agreed that the game materials were very attractive and simulated a sense of reality. Even the information system, which was not particularly something they have seen before was adopted immediately after explanation and was seen by participants as similar to e-mail messaging. Additionally, when looking at the large solution space, it is very good to keep flexibility in the responses from the facilitators. By doing this, the responses are in line with what participants expect. This realism has a price though, the game is very facilitator intensive, and requires serious briefing for these facilitators.

8.1.9 Would you recommend others to play this game?
The final question discussed in the evaluation is if the participants would recommend the game to others. Indirectly, this question asks the participants, if they think that this simulation game should be offered to other parties as well or not. It also gives insights into on what they think the key strengths are of the simulation game. All participants answered yes to this question. Most answered this question with using useful and insightful. A couple of reasons why they would recommend it to others are:

- **Group Dynamics and Interactivity.** This seems to be the number one reason for participants to recommend the game. These group dynamics included emotions, use of information for decision-making and dynamics in responses.
- **Awareness for Important Aspects.** As insightful is used a couple of times, it can be assumed that something is learned during playing the game, which is also mentioned by one participant. Also there is awareness for Cyber Crisis aspects, which is translated in an experience for participants, by using scenarios and events.
- **Fun & Learning Combination.** Participants mentioned during debriefing that the combination of having fun but also learning is a very important aspect, which you forget the time for a moment, but did not feel like a waste of time afterwards.
- **Decision-making skills.** All participants evaluated that they would have approached the situation differently the next time playing.

8.1.10 Conclusion: Perceived Usefulness
This chapter discussed the perceived usefulness of the simulation game by using a self-evaluation form after each session. In other words, this chapter discussed the perception of individual participants regarding the ability of the simulation game to help senior-managers to prepare for cyber crises. Following are the most important findings:

**Emotions are successfully simulated.** Nine out of ten participants agreed upon that emotions were part of the experience. Their answers included the feelings of pressure, stress and chaos.

**The simulation game seems to be suited for participants from different experience levels, backgrounds and companies.** The ten participants were from different ages, background, experience levels and even from (two) different organizations. However, in both games at least one cybersecurity expert was present. In the session in which two non-cybersecurity participants joined, the warm-up phase was longer as the participants needed to catch up. Therefore, additional tests with different participants need to be conducted.
Bad performance and high challenge were marked enjoyable. All ten participants marked the simulation game as enjoyable. On the other hand, they marked their performance as low as well as challenge to be high. Challenging aspects of the game were: *new experience containing many aspects, tough due to the interactivity, a lot of changes within the game and managing people.* Therefore, it can be concluded that the simulation game has a right level of challenge, which still makes the game enjoyable.

Interactivity is crucial in this simulation game. The interactivity; including the phone calls, messages, pressure from outside and the group decision making; disrupts the decision-making at hand. It also adds to a dependency among participants and adds chaos to the situation. This interactivity mimics 1) situation awareness, enabled by the information system, 2) team situation awareness, by adding secrecy as well as personal phone calls to the game and 3) sources of information, for which different stakeholders, systems are simulated like the newspaper, external parties, hackers etc.

Elements that challenge group dynamics are effective. The combination of elements that have been added to challenge group dynamics have proven very effective. These elements include the role descriptions, coins, action list, leaked information, information system and events. These elements have the potential to disrupt the status quo and possibly change the state of the environment.

The simulation game is a good tool for observing activities. The simulation game proves as a good tool to observe both group dynamics as well as decision making activities. Both sessions had different group dynamics as well as different decision making approaches. This also leaves room for different theories or approaches to be tested and observed.

The game raises awareness for cyber crisis concepts, but has a downside. One of the goals of this simulation game is to raise awareness for the cyber crisis decision making concepts. Important to know is that it is not logged which of the concepts or aspects are learned by the participants nor discussed, merely if they perceive it to be happened or not. With the taken approach it is not possible to track the concepts that have been learned by the participants. This is a major downside. This assuming of the learning also goes for decision-making aspects.

Incorporating flexibility increases realism. Incorporating flexibility in the simulation game proves to be very helpful. By doing this, the responses are in line with what the participants expect. This increased realism has a price, the game is very facilitator intensive, and requires serious briefing of these facilitators.

The participants would recommend others to play the game for the same reason as it is designed for. Participants mention the following reason to recommend this game to others: *group dynamics and interactivity, awareness of important aspects, fun and learning combination and decision-making skills.*

In conclusion, the simulation game is perceived as useful by participants. However, the above remarks give the impression that the simulation game is all positive. However, as also mentioned in the conclusion of the design chapter, there is also a downside in this chapter. The downside is that many of the discussed points are implied. In other words, it is not known for example for which aspects the awareness has been raised, just that it has. This leaves the conclusions on these points on the surface of the aspects. The findings discussed above as well as the downside of the evaluation will return in Chapter 9.
9. Conclusion and Discussion

In the last decade, data breaches and other information security incidents seem to be recurring headliners of major newspapers. These situations involving information systems can be called "cyber crises", and have internal as well as external consequences that need to be dealt with by the senior-managers within these organizations.

Unfortunately, simulation game design for the purpose of preparing senior-managers for cyber crises is still poorly understood. Three main gaps are found in reviewing the cybersecurity simulation game literature: 1) practical cybersecurity game design is poorly explained, conceptualized or justified, 2) existing cybersecurity simulation games focus on preventive training and awareness, not on crisis response and 3) the target group for cybersecurity simulation games are mostly teenagers, children or security operational personnel.

When taking the above perspective into consideration, a tension exists in the cybersecurity simulation game research field. On the one hand, there are two indicators that a cyber crisis simulation game has justification: 1) each crisis asks for different considerations and requires a customized set of actions, and 2) that simulation games are an often used method to prepare for crises. However, when looking at the cybersecurity simulation game literature no evidence of any cybersecurity simulation game exists that focuses on preparing senior-managers for crisis response, let alone research that explicate how to design such games. The presumption here is that cyber crises have characteristics that challenge the translation into a crisis management simulation game. In order to address the lack of a cyber crisis simulation game which prepares senior-managers for future cyber crises, this thesis focuses on exploring these characteristics involved with cyber crises by going through a simulation game design cycle.

Based on the above section, the main research question is formulated as:

**How to support senior-managers in preparing for cyber crisis decision making by means of crisis simulation games?**

This research question serves a greater objective. Crisis situations, require critical decision making under high uncertainty and time pressure. In other words, these decisions can impact an organization internally and externally when remained unhandled. However, due to the rarity of crisis events, there is a lack of training on the job. A designed simulation game should offer a training methodology which takes crisis characteristics into consideration, include cyber domain considerations and offer a safe environment to practice decision-making in. This simulation game then offers participants an opportunity to transfer knowledge into real-world scenarios. A designed simulation game should offer a training methodology which takes crisis characteristics into consideration, include cyber domain considerations and offer a safe environment to practice decision-making in. This simulation game then offers participants an opportunity to transfer knowledge into real-world scenarios.

9.1 Main Conclusions of this Research

From interviews with both crisis management experts as well as cybersecurity experts, it can be concluded that crisis definitions do not differ that much from the general crisis model. Importantly, the experts note that *cyber is merely the domain in which crisis takes place or originates from*. Experts note that after the immediate cyber threat is tackled, the situation evolves into something that is not different from other crisis types. Cyber events in isolation are then not by definition crises, but serve merely as a trigger for potential crisis. Subsequently, a simulation game specifically designed for cyber crisis decision making,
might in essence not be that different from a “regular” crisis simulation game, except for the simulated environment (scenarios, events and tasks) and processes which the game represents.

It is therefore that the blueprint of a conceptual model designed is geared towards a simulation game that focuses on dealing with general crisis. In other words, it focuses on simulation games, learning and decision making under uncertainty, including all their basic mechanisms. Important aspects for internalizing the learning are the de-briefing phase and narratives. Simulated models from theory include situation awareness, recognition primed decisions and uncertainty in decision-making.

The simulation game becomes a cyber crisis simulation game when the focus of the scenarios, events and tasks are designed towards cyber crisis. In other words, the simulated environment in which participants are placed with the simulation game should feel like a cyber crisis.

In brief, the proposed simulation game has the following key characteristics:

The crisis team needs to steer their organization out of the crisis situation and take crucial decisions. Participants are required to gather and assess information provided or found. This dynamic mimics the situation awareness decision making loop. Based on their situation awareness the participants have to decide on actions. The response is fed back to the participants, changing the state of the environment. The lack of information forces participants to act partly on experience and recognition, forcing the team members to cooperate. In other words, it requires recognition primed decisions. However, participants hold different pieces of information, either received verbally or through their role description. Therefore, next to their individual situation awareness, the team situation awareness is essential for their performance.

The game revolves around a fictitious company in which a cyber crisis occurred. The narrative revolves around a fictitious financial services provider in which a hack has occurred, and is under heavy public scrutiny. Experts describe a high fear of reputational damage, which according to them the most important to protect. All interviewed experts indicated that managing the media is a crucial aspect of cyber crisis situations. Therefore, a facilitator simulating the media and other outside stakeholders play a crucial role in the simulation game. To fill out the details on the scenario and events, the Sony hack in 2014 informs the narrative from a media point of view. To create a more realistic environment, the simulation game includes different non-playable internal and external stakeholders, represented by a facilitator.

The game takes the five decision makers through the process of crisis and crisis management. The game takes the participants through two phases of Crisis management: Phase I: Discovery & First Response and Phase II: Managing the Media. These phases are derived from expert interviews. When a crisis has immediate (or threat towards) a significant impact on the financial or reputational, decisions are made on the executive level. A crisis team regularly consists of five people. For a cyber crisis it would exist of the following roles: CEO, Senior Business Leader, CISO, Communications / PR, CFO. Finally, the simulation game follows the crisis model, starting from incubation period, to trigger event, immediate consequences, decision making, long-term consequences and finally to returning to normalcy.

Uncertainty is very high, with information coming from everywhere. Experts explain that crisis decision making is a chaotic environment in which situation awareness is determined by gathering facts. They have to make decisions in light of uncertainty, continuously asking for details and finding out what happened and additional questions arise for details. This information is provided to the crisis team from two different sources: 1) an information system, which is the main communication tool which represents the outside world. 2) through verbal and non-verbal communication with team members.

The game leans heavily on interaction between participants and the ‘outside world’ creating chaos and inducing the feelings involved in Crisis situations. Emotions that were important
According to experts were uncertainty, intuitive action, nervousness and pressure from outside. It is emotions which bring an actual game to life. Therefore, it is a crucial aspect to address. Different measures are implemented in the simulation game including yelling customers through the phone, threats of consequences, media interviews and press releases.

After testing the prototype, there is one key design variable that was most important during the design: realism versus control. The realism is created by a combination of many elements in the game and is praised by participants. Key elements are the information system, role descriptions, coins and pressure from outside. Included in the realism are the complexity, interactivity and flexibility that the configuration of the game elements bring. However, this choice leads to a loss of control. This also means that there is also no control over what participants actually learn. In other words, even though there is learning involved, there are not insights in which aspects are actually learned. Therefore, only an assumption exists that when participants note they have learned something, the game has served its goal.

The presumption used in this thesis is that cyber crises have characteristics that challenge the translation into a crisis management simulation game. However, as earlier described, according to experts, cyber crisis is not different from regular crisis except for the environment in takes place in or originates from. In this case, it is cyberspace. This of course does not mean that cyber crises do not have their own characterizing aspects to take into consideration, but after the initial trigger event takes place, regular crisis management activities are conducted by organizations. When supporting senior-managers in preparing for cyber crisis decision making by means of crisis simulation games, the simulation game design requires 1) components of crisis decision-making under uncertainty like situation awareness and recognized primed decisions, 2) learning components like the Kolb cycles, debriefing and the use of narratives and 3) scenarios, events and tasks that are geared towards cyber crises. However, the complexity of designing the proposed simulation game lies creating a realistic as possible environment, without losing control over the game. It is the combination of the game elements, that pull participants into the world of cyber crisis and its chaos.

The evaluation of the test sessions yielded a couple of findings which offer possible insights for future designs when supporting senior-managers for cyber crisis by means of a simulation game:

Participants enjoy a challenging game elements. All ten participants marked the simulation game as enjoyable. On the other hand, they marked their performance as low as well as challenge to be high. Challenging aspects of the game were: new experience containing many aspects, tough due to the interactivity, a lot of changes within the game and managing people. Therefore, it can be concluded that the simulation game has a right level of challenge, which still made the game enjoyable.

Interactivity is crucial in a complex decision-making game. The interactivity; including the phone calls, messages, pressure from outside and the group decision making; disrupts the decision-making at hand. It also adds to a dependency among participants and adds chaos to the situation. This interactivity mimics 1) situation awareness, enabled by the information system, 2) team situation awareness, by adding secrecy as well as personal phone calls to the game and 3) sources of information, for which different stakeholders, systems are simulated like the newspaper, external parties, hackers etc.

Elements that challenge group dynamics disrupt decision-making during play. The combination of elements that have been added to challenge group dynamics have proven very effective. These elements include the role descriptions, coins, action list, leaked information, information system and events. These elements have the potential to disrupt the status quo and possibly change the state of the environment.

Measuring awareness for cyber crisis concepts requires more than a self-evaluation. One of the goals of this simulation game is to raise awareness for the cyber crisis decision making concepts.
Important to know is that it is not logged which of the concepts or aspects are learned by the participants nor discussed, merely if they perceive it to be happened or not. With the taken approach it is not possible to monitor the concepts that have been learned by the participants. This is a major downside.

**Incorporating flexibility increases realism.** Incorporating flexibility in the simulation game proves to be very helpful. By doing this, the responses are in line with what the participants expect. This increased realism has a price, the game is very facilitator intensive, and requires extensive briefing of these facilitators.

### 9.2 Limitations of this Research

1. **The simulation game is untested with the Target group.**

   This simulation is designed for senior-managers of commercial companies. These include individual similar to the roles included in the simulation game, being CEO, CISO, Senior Business Leader, CFO or Communications / PR. Both test sessions had a different set of participants, but only one can be included in the category of senior-manager. Having limited senior-managers available was mostly due to last minute cancellations. Additionally, rescheduling the sessions was not feasible due to time constraints. Therefore, several participants have been replaced with non-senior participants. In the first session the participant group existed of management consultants, with an experience ranging between one and five years. The second session had one senior-manager, but on averaged about three years more in experience than the first group. These participants were both management consultants as well as media company owners. Both test sessions groups were ideal to measure playability of the simulation as well as the dynamics. However, the findings on perceived usefulness have no confidence for the senior-managers group. In other words, it is not possible to say if the simulation game actually supports senior-managers for cyber crisis. However, expected is that when replaced with the actual target group, the changes in design would remain similar as well as the findings on playability. Therefore, this limitation is resolved when conducted another test in which the perceived usefulness is tested again.

2. **The Simulation Game is perceived useful, but that’s all we know.**

   A second limitation of this research is the perceived usefulness as well as the self-reported learning effects. As described in paragraph 9.1 there is only an assumed perceived usefulness as well as an assumed learning effect. The limitation then lies in the fact that with the taken approach it is not possible to measure or monitor what is useful about the game and what the actual participants have learned. This limitation exists due to time constraints. In this research the design efforts and testing were very time intensive, especially because little information exists in the literature on cyber crisis simulation games. Therefore, the approach of a self-evaluation fits within the scope of a graduation thesis research. However, this approach is definitely not sufficient when measuring actual learning efforts. The simulation game as it exists does have the potential to foster for different approaches to incorporate more extensive models and evaluations. These can include evaluation methods which test certain knowledge beforehand and afterwards, evaluation methods which require a longitudinal approach, or where participants are put through another session of the simulation game.

3. **The Simulation Game is complex and intense, also for facilitators.**

   As discussed in Chapter 7, the key design variable was realism versus control. The choice has been predominantly made towards realism to meet the requirements as well as the perception from experts. Therefore, the game has become complex due to its interactivity, flexibility and large range of solutions to deal with the crisis at hand. This requires a lot from the facilitators, to have that knowledge and creativity to respond to participants in a way that makes sense and does not halt the game. Additionally, documenting all actions from the start is nearly impossible for the facilitator due to the chaos during the test sessions. The limitation however is temporarily within each new organization that deploys the
solution. As the number of the game sessions increase, the database of actions and responses increase, which eventually makes it easier to choose and pick from for the facilitators.

### 9.3 Main Contributions of this Research

Despite the mentioned limitations, the insights that have been generated with respect to designing a simulation game for cyber crisis decision making are still interesting. As discussed in Chapter 2, no existing simulation game is found in the literature that focuses on the areas of simulation games for cyber crisis decision making for senior-managers. The chosen framework combines a generic, well-known design science approach with game design, resulting in a new research approach. By taking a design approach that builds a simulation game model that consists of multiple smaller models, the simulation game is completely geared towards the problem at hand. This now makes it possible to conduct experiments with the simulation game. This modular approach also gives game designers the opportunity to mix-and-match parts that are less relevant for their research and replace them with components that are more suitable for their purpose. The research community can use, adjust and complement the existing game as well. Its use includes testing hypotheses or theories as well as observing team dynamics, decision making and communication efforts, without duplicating the design process.

This thesis predominantly focuses on filling the cyber crisis simulation game gap from a design perspective. In other words, the thesis focuses on designing and creating a simulation game to be able to offer insights into the design process as well as it provides key elements for a simulation game specifically for cyber crises. The explanation, conceptualization and justification on cyber crises simulation design assist future simulation game designers to use and build upon in their own designs, but also to review, discuss and citizen approaches, choices and propose improvements for future research.

The societal relevance lies mainly in the effects of the use of the game itself. As a result of playing the game, participants are more aware of the concepts and consequences of their decision-making within the cyber crisis domain. Ideally, senior-managers are better prepared for future cyber crises by practicing decision making in this specific domain and therefore are well-equipped to keep consequences to a minimum. Additionally, practitioners from the simulation gaming field can use the proposed cyber crisis game as a blueprint and adjust and complement the contents to their purposes.

### 9.4 Contextualize the research in the Literature

In the previous section, the answer to the main research question was given. But how do the two sides of this research find itself in the literature? When coming back to the literature reviewed in Chapter 2, the contributions fits one field of literature specifically. This is the crisis management field.

As discussed earlier in Chapter 2, crisis management simulations training is an often used method to prepare for Crisis situations (Bergstrom et al., 2012). This research offers another training methodology for crisis simulations, which can be added to the toolbox. More specifically, this game type offers a tool in which naturalistic decision making can be simulated and offers an environment in which participants can practice their decision-making. Importantly, is that not only the game itself is a contribution, it is foremost the conceptual blueprint as described in Chapter 3, called A conceptual blueprint for Crisis Management Simulation Games under Uncertainty. Other designers, be it practitioners or scientists can build on top of this blueprint, to customize towards the application domain or problem they wish. This fits specifically in Yang et al (2013) vision, that every Crisis requires its own awareness of different considerations and requirements and therefore a customized set of actions. Therefore, the conceptual blueprint created in chapter three can be used over and over again, as long as the simulated problem is similar.
There are several conditions for using the conceptual blueprint. The first condition is that the to be simulated Crisis is similar to the one presented in this research, and that the event is not the Crisis, but requires a perception of it. Simulating 9/11 would not be suitable using this design. This approach includes a one-room style of decision-making under a lot of stress and uncertainty from outside stakeholders, where the Crisis details still need to be uncovered. The second is that it involves naturalistic decision-making situations. Third, it fits the Coping with Crisis phase (Dayton, 2004).

Zooming out, the approach fits Gestwicki and Stumbaugh (2015) as well as the theory on Situation Awareness from Endsley (1995), it is a system in which transfer of knowledge occurs – what follows is that what they learn in one context can be applied in another.

9.5 Suggestions for Further Work

A simulation game in which participants are trained for cyber crisis decision making, is where this research has ended. However, this research leaves a couple of components which can be added to future work. These are either practical or scientific. Two are specifically highlighted:

1. **Create a complete learning experience.** From a practical point of view, the simulation game offers a tool to practice cyber crisis decision making. However, this can be strengthened by creating a comprehensive learning experience. For example, this can be done by creating an extensive course which the participants go through before the game session, which is reflected upon after the simulation game. The learning does not have to stop there. Simulation game findings can be communicated in an analysis received afterwards, in which the participant can reflect once more on the decision making.

2. **Take the existing game and use it to test specific theories and models.** Researchers can take the completed simulation game as a tool to test specific theories and models. For example, when a different form of decision-making is required, this can be replaced by the wished one. By doing this, one does not have to go through the design effort again, but can immediately test the dynamics or mechanisms. This does not limit itself to cyber crisis, as the scenarios can be replaced fairly easily.
References


A. Exploring Design-Research Approaches in depth

In Appendix A two specific design-research approaches are explored which fit in the design research philosophy of Winter (2008). Generally, both approaches focus on constructing a relevant artifact for a specific application domain, while keeping scientific rigor in consideration. There are numerous design approaches that focus on this balance, however a small selection has been made on just two design research approaches. Specifically, there is a need for a structuring method which fits the creation of Cyber crisis simulation game which focuses on training and awareness to prepare board-members for future situations.

A discussion of two approaches of their fitness are explicated in relation to this research. The three approaches selected are:

1. A three Cycle View of Design Science Research (Hevner, 2007)
2. Action Design Research (Sein et al., 2011)

A.1. A three Cycle View of Design Science Research (Hevner, 2007)

One common approach within design-research is the Three Cycle View of Design Science Research proposed by Hevner (2007). Hevner states design research as the embodiment of three cycles of closely related activities as depicted in Figure 24. The first is the Relevance cycle, in which the activities results in input requirements from the contextual environment into the research and feedbacks the artifact back into the environmental field. The second cycle, the Rigor cycle, provides theories and methods combined with experience and expertise from foundations into the research and adds newly generated knowledge into the knowledge base. The third central loop, the Design cycle supports creating and evaluating of the design artifacts and processes.

![Three Cycle View of Design Science Research (Hevner, 2007)](image)

Advantages of this method is that it structures the design processes in a loosely coupled manner. As it provides freedom for the designer in using the cycles. However, this freedom also poses challenges in the design. Using this method standalone will not result in providing the answers to the research questions. This method is especially useful as a structure, but not provides methods for filling the knowledge voids. Therefore, more methodologies have to be included in the list of research methodologies.
A.2. Action Design Research (Sein et al., 2011)

Sein et al.’s (2011) Action Design Research (ADR) approach shares the philosophy that information systems research has a dual mission: to make theoretical contributions but also assist in solving a problem in a specific environment. They argue that Hevner’s (2007) approach, discussed above, is too much construction-oriented and is centered around stage-gate style designing and building phases. Or more generally, in most design-research efforts, the problem definition precedes the development of the artifact, followed by evaluation. These research approaches focus on utility of the problem identified at the beginning of the research project.

Sein et al (2011) emphasize the importance of co-creation of the environment of the artefact. In other words, they believe that the other approaches do not reflect the incorporation of emergence from an organizational context. Sein et al (2011) propose ADR, a solution which requires design-research method builds an artifact in an organizational context and learns from the intervention while addressing a problematic situation. Their approach is a design-research method that draws on action research (AR), which focuses mostly on organizational interventions. ADR main stress point is that the influence of the relevance cycle by providing explicit guidance for combining building, intervention, and evaluation in a concerted research effort. As an implication, only the initial design is guided by the researcher. The consequent changes in the design are a reflection of intended and unintended organizational consequences. Figure 25 shows the design ADR method; consisting of its stages and subsequent guiding principles. It should be noted that Sein’s approach does not work in cycles but is more stepwise in nature.

![Figure 25: ADR method: Stages and Principles (Sein et al., 2011)](image)

A.3. Discussing Suitability and Limitations of the Approaches

Even though both of the design-research approaches discussed above are quite similar and derived from the same philosophy, there are some differences and limitations which become apparent when taking the need and characteristics of this research into consideration. The main gap in approach and need for this particular research is not located on the rigor side of the approaches. Both approaches agree that the design of the artifact needs to stem from theory, knowledge and experience. They both leave open to the designer how to establish the scientific rigor, which makes sense to remain generalizable and therefore applicable for any design problem.
Also, both approaches agree that a design approach should start from problems or opportunities from a practical point of view. Sein et al. (2011) prioritize it by identifying this need as principle 1. Hevner (2007) describes it as part of the relevance cycle and starting point of the design-research, which is defined as problems and opportunities.

The main difference between the two approaches lies in how relevance is integrated into the approach. In Hevner’s (2007) three cycle view, the environment provides for requirements, which is followed by building and evaluation. Finally, by field testing the artifact the effectiveness of the design is evaluated by the participants. Sein et al. (2011) approach this from a different point of view. They believe that to make an artifact relevant, practitioners and end-users have to be part of the design of the artifact and see their artifacts as emergent systems. This significant difference in approach requires either a researcher lead or a user lead design. Additionally, Hevner’s approach asks the solution to be somewhat complete from the moment field testing is started, on the other hand Sein et al. (2011) require the artifact to be of emergent nature, to be tested first with practitioners (experts) and subsequently with end-users. This can be either intentional or unintentional.

Another major difference between the two approaches is the focus of evaluation. Hevner (2007) separates evaluation of design and effectiveness of the artifact. The latter is done by participants, which influence the design indirectly. Sein et al. (2011) argue that any evaluation has direct effect on the design of the artifact, be it from practitioners or end-users. This research requires separate evaluation from experts and participants. The experts evaluate on design and validity. Participants evaluate on playability and usefulness.

When looking at the end products of both approaches, these also seem to differ slightly. Sein et al. (2011) approach the artefact as continuously emerging, which they formalize in step 3: Reflection and Learning and step 4: Formalizing of Learning. The products resulting from ADR are then subsequently threefold: 1) the design itself, 2) learnings of the interventions and emergence and 3) the use of the artifact. Hevner (2007) on the other hand, seem to focus on the effectiveness of the artifact and consequently its products limit to two products: 1) the design of the artifact and 2) the use of the artifact.

The goal of this research is to prepare board-members for a crisis in the future, by the design of a training and awareness simulation game. This objective uncovers the biggest limitation for both approaches for reaching this goal. Both approaches are derived for the information systems research, in which it is necessary to strongly incorporate the environment to optimize intervention power of the designed artifact (Hevner, 2007; Sein et al., 2011). Information Systems design have much more interaction with the environment than simulation games do, think of dependencies of other systems, data streamlining and users. Therefore, Information Systems require much more integration efforts than simulation games. For this research particularly, it is of much more importance that the domain is translated well and realistically in the design of the game and are easily changed without organizational consequences.

Table 1 provides a summary of the comparison and discussions done in this paragraph. Concluding, given the needs that the research objective provides, Hevner’s (2007) Three Cycle View of Design Science Research is the most suitable approach for this research. Differentiators are specifically, evaluation of the effectiveness of the game requires a (nearly) completed artifact and evaluation needs to be separated between experts and participants. Also Hevner's (2007) focus on the construction of the artifact focuses more on the research goal, instead of Sein et al. (2011) urge to optimize organizational fit. One clear limitation of the approach for this research is the application domain which stems from Information Systems research. Adjustment necessary to fit this research project’s need is the realistic translation of the domain into a simulation game, which requires less organizational integration.

An addition to this discussion of suitability is that both approaches are no specific approaches for creating simulation games, but serve as a structured design approach to build a relevant artifact while
keeping scientific rigor into consideration. However, the generalizability of Hevner’s approach provides room for specific game design theory and approaches to be incorporated in the rigor cycle. In the next paragraph an addition is made to Hevner’s (2007) design cycle to fits the need of this project.

Table 6: Comparison of two design-research approaches

|-----------------|---------------|-------------------|------------|
| Scientific Rigor | - Scientific Theories & Methods  
- Experience & Expertise  
- Meta-Artifacts (Design Products & Design Processes)  
- Using the above give grounding and add to knowledge base | - Theory-Ingained Artifact as a principle  | - There is little difference between the two approaches  
- The approaches leave it to the designer how to establish the scientific rigor |
| Integrating Relevance | - Design should start from problems or opportunities  
- Environment provides requirements and evaluates the artifact by field testing  
- Effectiveness of artifact for solving stated problem is key | - Prioritize by putting practice-inspired research first  
- Practitioners and end-users are part of the design process  
- Consist emergent artifacts | - Both agree design research starts from a practical problem  
- These approaches differ strongly in their relevance integration. Hevner has a designer-led approach and Sein et al has a designer-initiated but co-created by emergence |
| Building | - Start from requirements to design, to building and evaluating designs to evaluating effectiveness  
- Require (near) complete products when field testing | *Emergent design and prototyping* | - For this research, the goal is to evaluate the effectiveness for prepuatals. Therefore it requires a more complete design and product before evaluating the artifact |
| Evaluation | - Separation between designs and effectiveness of the artifact  
- Two separate groups of evaluators (experts and participants)  
- Participants have indirect impact on design | *Evaluation is done by both practitioners and end-users*  
*All have direct influence on the design* | *The research objectives require separate evaluation from experts and participants. The experts evaluate on design and validity. Participants evaluate on usability and usefulness* |
| Environment | - Provides requirements  
- Plays a role in field testing  
- People, organizational systems, technical systems | *Form the most important and continuous input for the design*  
*Environments co-create designs and are equally important as a source for change as the designer* | *Form the biggest limitation for this project. Both approaches seem from EI research, which necessitates incorporating the environment to optimize intervention power of the artifact*  
*This research requires realistic translation into a game* |
| Learning | - Focus more on the artifact, therefore effectiveness is more important than intervention power. Result is that a formalised learning is lacking | *Continuous learning and formalising as two important steps in the design approach* | *The goal is to prepare managers for future Cyber crisis. Therefore focus needs to be on evaluating the effectiveness of the artifact* |
| Products | - The design itself  
- Use of the artifact | - The design itself  
- Learnings of the interventions and emergence  
- Use of the artifact | *Learning in this research will be especially incorporated in adjustments in the artifact, learning by evaluating its usability is so specific, it will be hard to generalise* |
B. Input References

<table>
<thead>
<tr>
<th>No.</th>
<th>Theoretical Concepts</th>
<th>Source</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Simulation Game</td>
<td></td>
</tr>
<tr>
<td>SG1</td>
<td>Simulation games offer a flexible and safe environment in which rare and uncertain situations can be simulated.</td>
<td>Borodzicz &amp; van Haperen (2002)</td>
</tr>
<tr>
<td>SG2</td>
<td>Simulation games use models to represent the processes and objects and how they relate to their environment.</td>
<td>Stoppelenburg et al. (2012), Klabbers (2009)</td>
</tr>
<tr>
<td>SG3</td>
<td>SG is a model that replicates the dynamics of a system and to analyze the system at interest.</td>
<td>Stoppelenburg et al. (2012)</td>
</tr>
<tr>
<td>SG4</td>
<td>Simulation game: there is a (simulated) model of a (real or conceptual) system and there are actors, having different roles, which try to achieve specific goals within a set of rules.</td>
<td>Klabbers (2009)</td>
</tr>
<tr>
<td></td>
<td>Learning from Simulation Games</td>
<td></td>
</tr>
<tr>
<td>Learn1</td>
<td>Within simulation games, the learning preference of participate, practice and exploration are simulated and developed. Additionally, when simulation games are played in a group in a single room, the learning preference of adopting best practices is also added.</td>
<td>Simmons (2008)</td>
</tr>
<tr>
<td>Learn2</td>
<td>Learning happens through four different phases in a cycle: having a concrete experience, followed by observation of and reflection on that experience, which leads to formation of abstract concepts (analysis) and generalizations (conclusions), which are then used to test hypothesis in further situations, resulting in new experiences. By repeating this cycle, the new learned behavior can be internalized.</td>
<td>Kolb (2014), Thatcher (1990)</td>
</tr>
<tr>
<td>Learn3</td>
<td>The number of Kolb cycles, together with the very important debriefing form the whole experience.</td>
<td>Thatcher (1990)</td>
</tr>
<tr>
<td>Learn4</td>
<td>Three types of learning are present in simulations: learning the facts, learning the process and learning the relative costs and benefits.</td>
<td>Thatcher (1990)</td>
</tr>
<tr>
<td>Learn5</td>
<td>Emotions are an important aspect for learning in simulations</td>
<td>Thatcher (1990)</td>
</tr>
<tr>
<td>Learn6</td>
<td>Three important stages exist within the process of reflection: returning to the experience, attending to feelings and re-evaluating the experience.</td>
<td>Boud, Keogh and Walker (2013)</td>
</tr>
<tr>
<td>Learn7</td>
<td>Having a designed response self-evaluation questionnaire available, forces participants to consider important points to simulation, before their experience is under snowed during general discussion.</td>
<td>Thatcher (1990)</td>
</tr>
<tr>
<td></td>
<td>The role of the facilitator</td>
<td></td>
</tr>
<tr>
<td>FAC1</td>
<td>The facilitator has to learn not to interfere.</td>
<td>Thatcher (1990)</td>
</tr>
<tr>
<td>FAC2</td>
<td>Sometimes the facilitator is needed to guide participants to new aspects of the game. But most importantly, facilitators have to intervene when problems occur, that lie beyond the control of the participants, which could halt learning.</td>
<td>Stoppelenburg et al. (2012)</td>
</tr>
<tr>
<td>FAC3</td>
<td>It is the task of facilitators to recognize dysfunctional patterns and discuss these, to create a safe environment for participants.</td>
<td>Stoppelenburg et al. (2012)</td>
</tr>
<tr>
<td></td>
<td>Creating a realistic and safe environment with narratives</td>
<td></td>
</tr>
<tr>
<td>NAR1</td>
<td>Simulation games are a narrative space. Within this narrative space the two worlds of the narrator and the participants will meet and an exchange of ideas, experiences and feelings happen.</td>
<td>Bruer (2008)</td>
</tr>
<tr>
<td>NAR2</td>
<td>Favorable characteristics from working with narratives: equality between</td>
<td>Abma (2006)</td>
</tr>
<tr>
<td><strong>NAR3</strong></td>
<td>The evolvement of concern, emotions, wants and needs keep people involved.</td>
<td>Abma (2006)</td>
</tr>
<tr>
<td><strong>Situation Awareness</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>SA1</strong></td>
<td>Situation awareness: “The perception of the elements in the environment within a volume of time and space, the comprehension of their meaning and the projection of their status in the future.”</td>
<td>Endsley (1995)</td>
</tr>
<tr>
<td><strong>SA2</strong></td>
<td>It is the situations specifics, that determine which mental model is created and also the following problem-solving strategy.</td>
<td>Endsley (1995)</td>
</tr>
<tr>
<td><strong>SA3</strong></td>
<td>SA is more than the mere perception of information about the environment. It also involves comprehending the meaning of that information in a holistic form, taking goals into consideration, and providing projected future status of the environment that are valuable for decision-making.</td>
<td>Endsley (1995)</td>
</tr>
</tbody>
</table>
| **SA4** | Two important considerations, relating to SA.  
3. SA is not the same as taking action or performance.  
4. SA is only applicable in dynamic situations where variables are changing | Wickens (2008) |
| **SA5** | The individual can have certain preconceptions and objectives that can act and filter the environment in forming SA. More skilled individuals are able to go through the SA levels a lot quicker than less skilled equivalents. | Randel et al (1996) |
| **SA6** | In the SA model, the loop starts with state of the system then goes into SA followed by decision-making, where the performance of the actions changes the state of the system again through feedback. | Endsley (1995) |
| **SA7** | In terms of Task Factors, stress and workload and complexity are mentioned as factors which influence the loop discussed in SA6. | Endsley (1995) |
| **Team Situation Awareness** |  |  |
| **TSA1** | Team SA goes beyond the collective average or sum of SA for the individuals that make up the team. Overlap between each team member’s SA will exist. And this combination or a subset of information constitutes much of the team coordination. This coordination can happen in different ways like verbal, written etc. But most important it is the shared Situation Awareness of the state of the environment which determines the quality of the team coordination. | Gorman, Cooke & Winner (2006); Cooke, Gorman, Winner & Durso (2007) and Cooke, Salas, Kiekel & Bell (2004) |
| **Sources of Information** |  |  |
| **Inf1** | Cues can be received through visual, aural, tactical, olfactory or taste receptors. SA comes from three different sources:  
4. Direct observation from the real world  
5. Through any Display system  
6. Through verbal and non-verbal communication with team members and others | Endsley and Robbertain (2000) |
| **Decision-making under Uncertainty** |  |  |
| **DM1** | Important characteristics of Naturalistic Decision-making are time pressure, uncertainty, vague goals, high stakes, group and organizational constraints, changing conditions, and varying amounts of experience. | Marold et al. (2012) |
| **DM2** | Naturalistic decision making is dynamic and has continually changing conditions. Since conditions are dynamic, goals and objectives are likely to change with new information, this possibly also includes priorities. | Randel et al. (1996) |
| **DM3** | Essential for NDM is studying the information people are looking for and arguments used instead of using abstract models and empirical | Randel et al. (1996) |
Decisions within the Recognition Primed Decisions model are made based on experiences and knowledge from the decision-makers, which as the name pertains is about recognizing a situation as typical and recall the appropriate decision to deal with it effectively.

RPD is not particularly focused on generating different types of options but that there is a strong focus on classification of the situation.

Intuitive decision-making, based on pattern matching and recognition of familiar and typical cases, can be trained by increasing the decision-maker’s experience and knowledge base.

Uncertainty: “a sense of doubt that blocks or delays action”. These doubts can be specified in three broad dimensions: issues, sources and inclusiveness and subjectiveness.

When decision-making moves from the individual level to the group level, social interactions and contexts can influence uncertainty and decision-making. Social influence is the process in which individual judgments, behavior and attitudes change in presence of other people. These include: assess or make predictions about the expertise of other group members, decision-making biases and dealing with uncertainty.

Security is the safe-guarding against adversaries, by implementing security procedures which influence the feeling of safety, stability and anxiety. Once this safe-guarding is challenged, one desires to return to a state of safety. Returning to a feeling of safety can be an end-goal.

In cybersecurity all assets that should be protected need to be protected because of the vulnerabilities that exist as a result of the use of IT systems that form the basis of cyberspace. The definition of cybersecurity is: “the protection of cyberspace itself, the electronic information, the ICTs that support cyberspace, and the users of cyberspace in their personal, societal and national capacity, including any of their interests, either tangible or intangible that are vulnerable to attacks originating in cyberspace”.

Confidentiality, integrity, availability and resilience provide the simulation game possible themes which it can focus on.

Many different things can happen on an organizations network, but the important notion is that this has to be done by someone. There are a wide range of adversary types. First, they differ strongly in skill and sophistication (capabilities), there is a wide range of motivations for
their actions, due to the difference in skill level they apply different (sets) of tools and some are more hazardous than others.

**CS6** Cybersecurity and the crisis model share an important characteristic: threat. The concept of threat summarizes the actions that an adversary takes while attacking an organization. It starts with goals or objectives. From there, vulnerabilities are sought and when found exploited with the actor's capabilities, to conduct malicious actions to reach their ultimate goal.

Friedman and Singer (2014)

**CS7** A vulnerability is “a weakness in an asset or group of assets. These are weaknesses in either systems, configurations, designs, people etc. which can be exploited by attackers to serve their goals. Four main ones are identified: 1) human vulnerability, 2) application vulnerability, 3) software vulnerability and 4) system level vulnerability.


**CS8** There exist a range of different types of adversaries to consider. They can be classified by skill level, maliciousness, motivation and method. The following types were identified: 1) script kiddies, newbies, novices, 2) hacktivists, political activists, 3) cyber punks, crashers, thugs, 4) insiders, 5) coders, writers, 6) white hat hackers, old guard, sneakers, 7) black hat hackers, professionals, elite and 8) cyber terrorists.

Meyers et al (2009)

**CS9** An attack can encompass “attack vectors, operating systems, hardware and software targets, access schemes, attacker objectives, specific implementation and design vulnerabilities, and the attack payload”. The following attack classes are deployed by adversaries to exploit vulnerabilities: 1) viruses, 2) worms, 3) Trojans, 4) buffer overflows, 5) denial of service, 6) network attacks, 7) password attacks / user compromise and 8) information gathering / resource misuse.

Meyers et al (2009)

<table>
<thead>
<tr>
<th>No.</th>
<th>Scenario Considerations</th>
</tr>
</thead>
<tbody>
<tr>
<td>Sce1</td>
<td><strong>Crisis starts when there is the perception of it.</strong> The hackers were on the network for a time period between six months and a year. This however, was no crisis on itself. When the networks were actually down, warning signals were shown company wide and the data was leaked on data sharing websites, then there was crisis.</td>
</tr>
<tr>
<td>Sce2</td>
<td><strong>The vulnerability could come from third party service providers.</strong> Sony was breached through a third-party software service called SpiritWorld. This could be the case for any company, as many organizations rely on many third-party services.</td>
</tr>
<tr>
<td>Sce3</td>
<td><strong>The Story can be kept alive for weeks.</strong> Hackers dripped information, instead of dumping it all at once. This kept this stories going for weeks. This caused uncertainty about the duration of the hack. Additionally, there is uncertainty about which information is compromised. In this case the information included non-released materials, personal information including medical records of personnel, password credentials for services and lists of existing machines and servers.</td>
</tr>
<tr>
<td>Sce4</td>
<td><strong>The only real short-term consequence is operational discontinuity.</strong> The only decisions that seems to require immediate and quick handling is bringing back the systems to continue activities. The need to bring it back as soon as possible depends on the dependence on the systems and data.</td>
</tr>
</tbody>
</table>
| Sce5 | **Threats can come from anyone, claiming anything.** There were multiple claims for either money, taking down the movie, or even physical threats. But the GOP never showed who they
were. This leaves involved wondering each and every moment uncertain over the credibility of the claims.

**Sce6**  
**Financial consequences can be large, when not insured.** It can be expected that a large company like Sony is insured to any possible events. However, when firms get smaller and smaller, it might be different. Costs in the Sony hack involved investigative and sanitary costs. However, one can also calculate loss by taking the loss in ticket pricing or other loss of sales as well.

**Sce7**  
**Reputational damage is created by the media.** In terms of reputational damage, it was the heavy media coverage over the leaked e-mail conversations between Amy Pascal and Scott Rudin that got the public involved, specifically over its racist contents. This shows that not only the company should be wary of the reputational damages, but single senior managers as well. One side-note is that it was the second time Sony got hacked. Apparently, for Sony these hacks were not critically affecting their core business.

**Sce8**  
**Attribution is hard, and speculation seems to lead the discussion.** Many different news sources entered the attribution game. Was it North Korea? Was it China? Anonymous? Speculations on reasons why or why not a particular actor could be the attacker seemed to be the most interesting discussion.

**Sce9**  
**Investigative and sanitary work can take a while, without answers.** In any company with the size of Sony, one can imagine how long it takes to investigate and sanitize all the networks, systems, devices and anything else that is part of their ecosystem. If the attacker is skilled, they erase their tracks or put investigators on side-trails. There is no guarantee that investigations offer answers.

**Sce10**  
**Externals will tell the story for you. True or not.** As access was obtained through a phishing e-mail, one can imagine that the hack was not extremely complicated (not saying it was easy). However, the story took flight, also due to media and government. These external parties have influence on events but especially the public opinion. But still, many believed that claims made by governments were not based on truth, but assumptions on red flags. Additionally, involvement from parties like governments as well as ex-employees suing the company also forms the story in some way.

**Sce11**  
**Hiring third parties can result in losing the public’s sympathy.** As it is a large hack, people might feel sorry for Sony. Especially, because it was not the first time. However, when they hired litigator David Boies, making all kinds of threats, people could lose their sympathy for Sony. Additionally, what is forbidden might be more interesting for people as well.

<table>
<thead>
<tr>
<th>No.</th>
<th>Expert Perception Considerations</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Cyber Crisis According to Experts</strong></td>
<td></td>
</tr>
<tr>
<td><strong>Exp1</strong></td>
<td>All Crisis definitions from experts fit the described crisis model. But focus more on discontinuity.</td>
</tr>
<tr>
<td><strong>Exp2</strong></td>
<td>Crisis perception starts with an event, moment or situation (<em>trigger event</em>).</td>
</tr>
<tr>
<td><strong>Exp3</strong></td>
<td>Cyber is merely the domain in which crisis takes place or originate from. Therefore, a cyber incident is just a trigger for crisis.</td>
</tr>
<tr>
<td><strong>Exp4</strong></td>
<td>After the immediate cyber threat is tackled, the situation evolves into something that is not different from other crisis types. Cyber events in isolation are not by definition crises.</td>
</tr>
<tr>
<td><strong>Exp5</strong></td>
<td>Each company has a different value to protect. This can be a combination of anything, be it reputational, financial or assets.</td>
</tr>
<tr>
<td><strong>Exp6</strong></td>
<td>There is a high fear of reputational damage. Often it is not the trigger event which escalate a crisis, but the events that follow. Anything that noticeably gives motivation for any outside stakeholder to impact the company’s reputation can force a company out of business.</td>
</tr>
</tbody>
</table>
Exp7. They see reputational damage as the most important one to protect. The external world has a very large impact on crises situations, where the perception of crisis internally is also determined by what happens outside the organization, including media, clients and public opinion.

Exp8. A small incident can become a (major) crisis.

Exp9. Who deals with the crisis depends on perceived severity. An impact assessment is often made before a crisis team assembled.

**Decision-making and SA questions during a Cyber Crisis**

Exp10. Scenario related questions are questions related to the details of the situation. The goal is to gather information for decision-making.

Exp11. Action related questions are question for which the crisis team has to provide answers for. These are the decisions which the crisis team has to take during the game, and have to ask scenario related questions for as well.

Exp12. To keep the flow of the simulation game going questions from participants should be followed by answers. Therefore, answers and detail to these questions should be readily available to the facilitators in charge of providing information to the participants, but still have some flexibility to be altered.

Exp13. Scenario questions that can be detailed out in the scenario are: where does it occur? When did it happen? Which part of the organization is affected? Who is affected by the situation? The other questions require the given background information in the cybersecurity domain.

**Stakeholders**

Exp14. Every emergency or crisis has its own responsible team, depending on the scale. When a crisis has immediate (or threat towards a) significant impact on the financial or reputational, decisions are made on the executive level.

Exp15. A team consists of five people in which the members and their responsibilities differ in different situations. For a cyber crisis on a national level the following five members are proposed: CEO, Senior Business Leader, CISO, Communications/PR and Board-member.

Exp16. As senior-managers do not have all the knowledge of the problem or domain, the decision-makers are accompanied by their own chosen subject matter experts. Experts mention the following internal functions as important source of information during a cyber crisis situation: IT/Security, SOC, Company branches, Group incident management, Risk/BCM, HR, Communications and Finance.

Exp17. There are 3rd-party advisors/teams involved. Which parties get involved depend on what the decision-makers want and need at the moment. This can be communications, research, legal etc.

Exp18. One of the three important phases mentioned by the crisis management expert is managing the media. And is even mentioned as very important. Experts mention it is the fear of the consequences of the media which executives truly feared.

Exp19. Important regarding regulatory compliance in case of a data breach is the mandatory data breach notification. Organizations which are breached need to report this to the national privacy regulator. Failures to notify in a timely manner will face a fine of maximum Eur. 820,000 or 10% of the company’s annual net turnover per violation, whichever is higher.

Exp20. Shareholders and clients are perceived as important stakeholders. They are “on a notify basis”, which means it is important to keep them informed during crisis. Experts say that fear can have a domino effect, where clients and shareholders lose trust.

Exp21. Within the “IT ecosystems” of companies, there are many providers of services, either hardware or software. Any vulnerability within this ecosystem can become a vulnerability for all organizations connected through these services.

Exp22. The general public is mentioned by practitioners as stakeholders that have no financial or emotional connection with the organization. These are the customers, partners, shareholders.
etc. However, the general public can influence and be influenced by any media or other persons.

**Process during Crisis**

**Exp23** Attackers are the ones attacking the organization. Sometimes they also use the media to share demands with the organization, and the outside world.

**Exp24** On the lowest level, a local office can have an emergency plan (ERP). This ERP has two parts, the first is the paper emergency response plan. Here leaders understand the actions they need to take during the crisis. This includes priorities. Secondly, the ERP assists crisis managers to assess the situation.

**Exp25** When a crisis has immediate (or threat towards) a significant impact on the financial or reputational, decisions are made on the executive level. The team would include the CEO, the CISO, and other members of the executive board. The members of the crisis team then pull in their significant subject matter experts.

**Exp26** Three important phases of crisis management are: 1) getting control of the incident, 2) forensics to find out if the problem is actually solved, and find out what happened exactly and 3) media management. This includes communication and marketing, focused to protect an organization’s reputation (showing control of crisis). Managing this media is a very important aspect.

**Exp27** The crisis often starts as a perception of we have to protect the business and reputation. Then It follows into a more logical process: we want to know! But this is still perception driven. Important is putting in all resources to plug the breach.

**Exp28** The preparation plans at this moment are mostly reactive in nature and follow a triggering event (the crisis event). But in reality, protocols are less strict and defined. There are too many people involved, for which having a protocol is not effective. The decision-makers however, are advised by experts on crisis situations. Often these experts act 50% on experience, and 50% are protocol driven.

**Additions from cybersecurity experts on Decision-making Processes**

**Exp29** The discovery of the incident often happens by a person most often from the operational ranks of the organization. This person needs to figure out if the incident needs to be escalated to higher management. There is a trade-off between efficiency and effectiveness here.

**Exp30** When a situation immediately appears serious, the incident needs to be escalated at once. But this should only happen when there is plenty of information available, otherwise decisions will be made based on nothing but hunches. The information is used by the crisis management team to determine if the organization is actually in crisis or not.

**Exp31** The first response contains the first actions taken by the crisis team after the incident is discovered and an impact assessment is conducted. The first response can be divided into first internal action and first communication.

**Exp32** During the first internal actions, activities are conducted that create more understanding or solve the problem. Important is to examine the causes of the crisis. Specifically, in the case of cyber, when there is a crisis most important is 1) to close the gap / vulnerability and 2) ensure that the perpetrators do not have access any more.

**Exp33** Current networks are well-equipped to detect malicious actions on networks. Otherwise, the organization should shut the network down. If they fail to do this, it creates uncertainty, both internally and externally.

**Exp34** Informing the ones that need to be informed is crucial, both internal and external. There are considerations when informing stakeholders. For example, with what information and at which time. Not informing has possible consequences, like uncertainty and public unrest. Informing too quickly can leave open spots or include unjust stories.
<table>
<thead>
<tr>
<th>Exp35</th>
<th>Basic principles are the same across different crises however each specific case is different. Therefore, a general guideline is expected in the planning. Without these guidelines, important aspects of crisis management could be forgotten, as one cannot foresee all the needed actions during such chaotic situations.</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Emotions during crisis</strong></td>
<td></td>
</tr>
<tr>
<td>Exp35</td>
<td>Four sets of emotions are mentioned by experts: 1) uncertainty, 2) intuitive action, 3) nervousness and 4) pressure from outside.</td>
</tr>
</tbody>
</table>
C. Impressions from the test sessions

C.1 Test Session 1
C.2 Test Session 2
D. Final Game Elements

D.1 Scenarios

How did the hack happen? General Scenario (for facilitators)

The hackers entered the systems in a very simple, yet patient way. Attackers, which are unknown so far, have entered the systems through spear-phishing. In other words, they targeted a trading manager, sent an email stating it was from the chief of the department with a malicious executable document. As unaware as people sometimes are, the employee clicked and ran the software. This was a piece of malware, that gave certain access to the computer of this particular employee, including e-mail.

The reason why the trading manager was a perfect target, was because it was the main responsible person for 3rd party application called FinAmp, used by all employees to manage trade transactions and administer every detail on these. Importantly, FinAmp was mostly configured by the company itself to stay in control but is developed and maintained by the 3rd party provider.

Even though the trading manager had no specific knowledge of IT systems, she could elevate rights by requesting them to the 3rd party provider by e-mail. The attackers saw their chance, and through e-mail, they requested the elevation to FinAmp for a number of accounts belonging to lower staff, they had already compromised earlier through normal phishing. Subsequently, they added the confirmation e-mail address to the spam filter so the trading manager would never receive confirmations (or at least, too late).

As before they went into this they had gathered intelligence on the systems and people of the target company, it was very obvious that FinAmp contained vulnerabilities. The attackers would use one of the admin right accounts to install modules to the application, creating a backdoor on the application. This allowed the attackers to get into the systems without having to log in anymore. Here is where the misery started.

Details to be (soon) discovered. What the crisis team does not know yet is that the media is on their tail, with their own “exclusive” information. What is showing clearly when the event shows up, is that there is murmur inside the company. Also they have heard rumors about that there possibly might have happened something, thinking: “Do the execs even know? Are they hiding something from us?”

The systems seem OK, at least at first. As any Financial Service Organization, there is heavy reliance on IT systems. But they are pretty certain that systems are well-protected. They were not reported any deficiencies in their IT audits for years, and do not expect this to change in the short-term, not with current leadership.

Clearly, the threat level is very uncertain at the moment. There is little information on who it was, where it came from and what they did to our systems. Additionally, when thinking about the CIA-triad, it is definitely not sure if we can assure confidentiality, integrity or availability. We are not sure if the attackers are actually eavesdropping our servers, if they have not tampered our systems or not? What we do know that our systems are still up and running. However, if there is no certainty about the first, the last is worth nothing. But guess what? The attackers are still on the systems.
Crisis Team Scenario

Fictitious Company. FinCorp. is a Dutch Financial Services Provider, with a stellar reputation among its customers and partners. Everybody loves to do business with FinCorp and business has never been so good. Within the Netherlands it is one of the best known in Commercial Banking, providing a complete range of financial services to companies with at least a yearly revenue of €5 million. Customers often praise the combination of personalized services, expertise and ‘do as you promise’-approach that the company has, making their reputation almost impeccable. Services include all traditional banking activities like lending, supporting transactions but also cash and liquidity management, trade services and treasury-solutions. With their 925 employees, they yield in approximately €145 million last year with a profit of €36.1 million.

It is not all about the money for this Financial Services Provider. Employees and customers relate to FinCorp, due to its presence in society, for example in their sports sponsoring and sustainability. This of course fits in their slogan of Our Reputation is your Asset. This value pays off, this shows by the long list of clients, who mostly have been with FinCorp for decades.

CEO briefing. After the morning exercise the CEO of FinCorp turns on his/her phone and received a very interesting call from one of his/her trusted advisors: “You might want to see this… I’ve sent you the link via e-mail”. And there it was, a link to Pastebin, saying: “FinCorp, we have your data. You will hear from us again soon, and we have demands. – Yours Sincerely, Anarchy Angels”. With the link are some example data samples, to back up the claim. The CEO calls the CISO: “Have you seen this? And what is this?”. “No I have no idea…! I’m not sure how serious this it, but we have to do something about it”, he says with an absent tone. The CEO acts immediately and decides to get his crisis team together and the CISO. Better be safe than sorry, he thinks.

Assignment: You are very risk averse, therefore you will ask the team to think of the worst case scenario and prepare for that just in case.

Media Team Scenario

Fictitious News Paper. Finance Daily, the most renowned newspaper with focus on economy and business. They were founded in 1812 and by far the leading paper in financial news coverage. However, the turbulent digital era of today has brought sales to decline. It is not only the decline which is visible, but also the editors notice the switch to digital in their work. Everything needs to be read and published as soon as possible. “News spreads so quick, that when you leave your desk for a coffee, it’s old news...” This leaves us in a painful split situation, in which we do have sales targets, but we also want to cover correct news. This correctness cannot be underestimated, because this newspaper has existed for over 200 years, and are being seen as the most reliable source of financial information. Everybody in the financial world reads it, but it is also an often cited source for other newspapers, blogs, tweets etc. In other words, Finance Daily has the challenge to remain high in reputation, but not to fall behind on the “news” in the financial world.

Media Team Briefing. The Internet News department within Finance Daily received the same Pastebin link through e-mail. Knowing Finance Daily’s reputation, this is never going to be enough to even get a line published. We don’t know who it is, if it’s real or anything... “let’s not get going with this hunch, but you three keep your eyes open on this item. We should not play with FinCorp’s reputation unless we really have something on them” the editor said. The same day, an anonymous e-mail pops up. It is a
download request from WeTransfer, 2GB in total, with the message: “I trust you. FinCorp is wrong. Look at the Data, it’s theirs. You get 3 days’ exclusive rights, use it wisely. – Anarchy Angels”.

D.2 Role Descriptions

**ROLE DESCRIPTION**

<table>
<thead>
<tr>
<th>Role</th>
<th>CEO</th>
</tr>
</thead>
<tbody>
<tr>
<td>Objectives</td>
<td>Retain an acceptable Reputation</td>
</tr>
<tr>
<td>Coins</td>
<td>15</td>
</tr>
</tbody>
</table>

**Description**
The CEO of FinCorp is a respected leader in the financial world. Most remarkable is that the CEO has during his fifteen-year tenure has never been put into doubt by his people. This while driving the company only forward, making strong decisions every time it was needed.

* This Description is Highly Confidential. Do not Share.
Role Description

Role: CISO
Objectives: Control the Incident (from Systems)
Coins: 15

Description
The CISO is a security person in heart and soul. Started from a very technical role, the Chief Information Security Officer is now an accepted and very respected governing function within FinCorp. The CISO has been with the company for over 10 years, in different positions. The IT security has never let them down too much. However, some actions have been out of the CISO’s control due to increasing complexity.
**ROLE DESCRIPTION**

**Role**
Business Leader

**Objectives**
1. Establish a line of communication to the clients (make sure they are not neglected)
2. Protect client confidentiality

**Coins**
5

**Description**
This person is a true superstar within the management ranks of the company. Speculations arise that this client facing leader has what it takes to become the next CEO after the current one will step down. What makes this business leader so great is the client-friendly approach. This even resulted in being on the fast-dial for many business leaders. An interesting feature is that this leader thinks about both the long-term business objectives and the short-term objectives, making the business leader also popular among shareholders.

---

**ROLE DESCRIPTION**

**Role**
Communication / PR

**Objectives**
1. Create an honest and open image
2. Open lines of communications with the most important stakeholders and keep them informed

**Coins**
5

**Description**
The communication / PR person is the chief of the communications department. This person has 20+ years experience in press communications and public relations. Over the years, the reputation of FinCorp has definitely been partly due to the great work from the communications department, in which minor events could be reframed into positive messages.
ROLE DESCRIPTION

Role: CFO

Objectives:
1. Keep the business up and running (retain revenue creation)
2. Retain at least 15 coins (all combined)

Coins: 10

Description:
The CFO in question is a prominent member of the financial world. Several high status positions prepared the CFO perfectly for this job. This person is the shareholders favorite, as this CFO always works hard to cut costs and increases revenue to keep profits up for this year.
## D.3 Action List Crisis Team

<table>
<thead>
<tr>
<th>Actions</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Getting advice from any one in the advisor pool (internal) – specify who and what – Opens up a communication line.</td>
<td>4</td>
</tr>
<tr>
<td>Hire a 3rd party advisor - specify who and what</td>
<td>Negotiate</td>
</tr>
<tr>
<td>Investigate Internally (advisor pool) – specify who and what</td>
<td>6</td>
</tr>
<tr>
<td>Shut Systems Down – specify who, what, how, when</td>
<td>15</td>
</tr>
<tr>
<td>Isolate Systems Partially (specify how) – specify who, what, how, when</td>
<td>10</td>
</tr>
<tr>
<td>Internal Communication stop to the outside, until…- specify the terms</td>
<td>3</td>
</tr>
<tr>
<td>Issue an embargoed press release (provide exclusive information in exchange for a delayed publication) – specify the terms</td>
<td>6</td>
</tr>
<tr>
<td>Respond through open letter to newspaper</td>
<td>4</td>
</tr>
<tr>
<td>Request Exclusive interview with the media to tell your story (you reserve the right to edit the message) – specify when</td>
<td>8</td>
</tr>
<tr>
<td>Release Press Release on own website – specify contents</td>
<td>1</td>
</tr>
<tr>
<td>Any other communication (email etc) – clearly communicate</td>
<td>2</td>
</tr>
</tbody>
</table>
D.4 Facilitators Document

Facilitator’s Role

A very important role in simulations games lie in the hands of the facilitator. When the players are debriefed and introduced to the most important facts, the facilitator has no control over the speed which these materials offered to them are used, nor the order in which the participants use them. An important role for the facilitator then is to be supportive to the flow or dynamic of the simulation game, to facilitate debriefing, and thus promote discussion and reflection, in other words to enable the use of materials as effectively as possible. The facilitator has to learn not to interfere.

During Play. During play, the task of the facilitator is purely to monitor the process, again not interfering and noticing and reflecting on the differences between what is happening and what he or she anticipated would happen or what has happened when the game or simulation was used before. Have the following documents ready: facilitators document and scenarios.

Media Facilitator. This facilitator has the objective to disrupt the crisis team, by calling, pulling them out of the room and write short articles from the press point of view. Have the following documents ready: events.

Debriefing. In debriefing, facilitating take a more active role and assist in raising the surface the points that they observed in the activity and relating them to the points that the participants observed. Facilitators skillfully use questions or other kinds of prompting, reflecting on the process themselves and also prompt the reflection of the participants on the process. Just like they promote learning from experience from the participants, they promote it in themselves.

Prop checklist (all need to be there)

<table>
<thead>
<tr>
<th>#</th>
<th>Document Name</th>
<th>Type</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Application Running on: cyberwargame-hdking.c9users.io/</td>
<td>Web-application.s</td>
</tr>
<tr>
<td></td>
<td>With the following extensions:</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• /media_center  - (to publish articles)</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• /media_messages - (for media team messages)</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• /crisis_center – (for media team messages)</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• /crisis_communications – (to convey crisis team choices)</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• /facilitator_center – (to send the teams messages)</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• /facilitator_messages – (to receive requests from crisis team)</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• /timeline – (published article overview)</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• /articles/#/ - (for complete specific articles published)</td>
<td></td>
</tr>
<tr>
<td>2</td>
<td>2. Briefing Scenarios</td>
<td>word</td>
</tr>
<tr>
<td>3</td>
<td>3. Role Description – put in envelopes</td>
<td>powerpoint</td>
</tr>
<tr>
<td>4</td>
<td>4. Crisis management documents + impact assessment</td>
<td>word</td>
</tr>
<tr>
<td>5</td>
<td>5. Price list Crisis Team</td>
<td>powerpoint</td>
</tr>
<tr>
<td>6</td>
<td>6. Price list Media Team</td>
<td>powerpoint</td>
</tr>
<tr>
<td>7</td>
<td>7. Facilitator Documents (explanation and logging forms) – this document</td>
<td>word</td>
</tr>
<tr>
<td></td>
<td>8. Self-Evaluation Form</td>
<td>word</td>
</tr>
<tr>
<td>---</td>
<td>------------------------</td>
<td>------</td>
</tr>
<tr>
<td>9</td>
<td>9. Action Log (for facilitators table)</td>
<td>word</td>
</tr>
<tr>
<td>10</td>
<td>10. Rules</td>
<td>powerpoint</td>
</tr>
<tr>
<td>11</td>
<td>11. Coins + Coins holder</td>
<td>Physical symbols</td>
</tr>
<tr>
<td>12</td>
<td>12. Events</td>
<td>word</td>
</tr>
<tr>
<td>13</td>
<td>13. Leaked Information</td>
<td>Range of documents</td>
</tr>
<tr>
<td></td>
<td>• FinCorp1: Excel Files with all kinds of PII</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• FinCorp2: List of certificates, devices, ftp passwords, server lists</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• FinCorp3: Draft Q2 Financial Report (send PDF) and financial models</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• FinCorp4: email message (pdf)</td>
<td></td>
</tr>
<tr>
<td>14</td>
<td>14. USB stick</td>
<td>Physical to carry 13 over</td>
</tr>
<tr>
<td>15</td>
<td>15. Internal Security Document</td>
<td>word</td>
</tr>
</tbody>
</table>
Process of the Game

**General Briefing**

<table>
<thead>
<tr>
<th>Action</th>
<th>Prop / docs needed</th>
<th>Notes</th>
</tr>
</thead>
<tbody>
<tr>
<td>Assemble Everyone</td>
<td></td>
<td>Make sure no information is visible for the other team.</td>
</tr>
<tr>
<td>Words of Welcome (including purpose game)</td>
<td></td>
<td>- Welcome &amp; words of thanks</td>
</tr>
<tr>
<td></td>
<td></td>
<td>- You will be immersed in a crisis situation</td>
</tr>
<tr>
<td>Introduce Rules</td>
<td>Printed out rules</td>
<td>Rules are placed on the table.</td>
</tr>
<tr>
<td>Explain role facilitator</td>
<td></td>
<td>Clarify we are not an advisor nor participant but logistical support.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Don't expect too much. Note that this is a prototype, there are glitches which we did not anticipate.</td>
</tr>
<tr>
<td>Provide General Background on FinCorp and Finance Daily</td>
<td>Background Story</td>
<td>Present the background story</td>
</tr>
<tr>
<td>Split into rooms for team-specific briefing</td>
<td></td>
<td>Facilitators to split up.</td>
</tr>
</tbody>
</table>

**Crisis Team (in parallel with media team) – introduce first round**

<table>
<thead>
<tr>
<th>Action</th>
<th>Prop / docs needed</th>
<th>Notes</th>
</tr>
</thead>
<tbody>
<tr>
<td>Provide high-level briefing on their situation</td>
<td>Background story</td>
<td>Everyone in the crisis room gets a copy. Explain that the coins represent effort and money not specifically money. n</td>
</tr>
<tr>
<td>Tell them they will get a role + first task: split the roles</td>
<td>Envelopes with role description</td>
<td>Stress that these are secret envelopes – ‘your hidden agenda’.</td>
</tr>
<tr>
<td>Ask participants to read the roles</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Give last instruction: CEO if you are ready, come to us</td>
<td>Briefing card</td>
<td>Explain the rule of the briefing card + message last time you will hear from us. + form a strategy</td>
</tr>
</tbody>
</table>

**Media Team (in parallel with crisis team) – introduce first round**

<table>
<thead>
<tr>
<th>Action</th>
<th>Prop / docs needed</th>
<th>Notes</th>
</tr>
</thead>
<tbody>
<tr>
<td>Get them into the setting</td>
<td>Background Story</td>
<td>Everyone in the crisis rooms get a copy.</td>
</tr>
<tr>
<td>Brief them about their objectives as a newspaper</td>
<td>Background Story</td>
<td>They should get a grasp</td>
</tr>
<tr>
<td>Provide them the document with the “exclusive information”</td>
<td>Exclusive information Document</td>
<td></td>
</tr>
<tr>
<td>Provide them the assignment on a card</td>
<td>Briefing Card</td>
<td>Read the card + tell them to get it on the table as soon as possible.</td>
</tr>
</tbody>
</table>
(if they hurry) The Media team has time constraint

<table>
<thead>
<tr>
<th></th>
<th>Timer</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Debriefing</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Action</th>
<th>Prop / docs needed</th>
<th>Notes</th>
</tr>
</thead>
<tbody>
<tr>
<td>Press Release</td>
<td></td>
<td>Pull a person from the hat (randomly). The others have to observe which message is conveyed.</td>
</tr>
<tr>
<td>Answer questions</td>
<td>Questions from Media team.</td>
<td>Ask specific persons’ questions. Everyone should answer a question.</td>
</tr>
<tr>
<td>Go into the debriefing on their decisions and discuss their process, emotions and what they could have done better.</td>
<td>Logging forms – it is crucial that you bring them back to the moment that it happened.</td>
<td>Also discuss what you have seen during logging. This is crucial!</td>
</tr>
<tr>
<td>Spend 15 minutes on feedback of the game.</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
Facilitator Logging Form

Before the Game

- Time details of the game

<table>
<thead>
<tr>
<th>Date:</th>
</tr>
</thead>
<tbody>
<tr>
<td>Briefing started (in the room):</td>
</tr>
<tr>
<td>Game started:</td>
</tr>
<tr>
<td>Game ended:</td>
</tr>
</tbody>
</table>

- Notes regarding pre-game issues / observations etc.
## During the Game

### Perception of Crisis

<table>
<thead>
<tr>
<th>Time</th>
<th>Perceived crisis level (1-10)</th>
<th>Notes</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

### Decision Making Under Uncertainty

<table>
<thead>
<tr>
<th>Time</th>
<th>Event</th>
<th>Category of Uncertainty</th>
<th>Source of Uncertainty</th>
<th>Tactics used to cope with uncertainty</th>
<th>Notes</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
Category of Uncertainty:
1. Nature of the Situation
2. Alternative of the decision
3. Potential outcomes

Source of Uncertainty:
1. Incomplete information
2. Inadequate understanding
3. Overwhelming information or undifferentiated alternatives

Tactics used to cope with Uncertainty:
1. Tactics of Reduction: including retrieve additional information or increase predictability.
2. Tactics of acknowledgement: involving taking uncertainty into account in selecting a course of action or preparing to avoid possible risks. (avoiding irreversible action, weighing pros and cons, preempting (generating specific responses to possible negative outcomes).
3. Tactics of Suppression: a denial of uncertainty. Ignoring it, relying on intuition or taking a gamble.

➢ Notes decision-making under uncertainty

➢ Group Decision-making under uncertainty
One aspect is when the individual decision-makers need to assess or make predictions about the expertise of other group members. This particularly is the case when information which is required is not completely accessible and understandable. These kind of situations in uncertainty in group decision making are described by Hanson (1996). In these uncertain situations, decision-makers rely on experts that advise them, which additionally builds up on the uncertainty. In other words, it is unclear for the decision-makers if the information provided from others, especially the experts, is reliable. According to Hanson (1996) there are three different aspects to this uncertainty (see checklist).

A second class in which social influence have effect in decision-making comes from the social psychology, and are called decision-making biases. Jones and Roelofsma (2000) mention several examples of group-decision biases (see checklist).

- **Checklist**

<table>
<thead>
<tr>
<th>Observation</th>
<th>Yes</th>
<th>No</th>
<th>Notes</th>
</tr>
</thead>
<tbody>
<tr>
<td>Experts are recognized but decision-makers disagree</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Experts are not recognized</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Whether experts are reliable at all or not</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>The false consensus effect: the tendency for people to overestimate the degree to which others agree with them</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Groupthink: a type of thought within a deeply cohesive in-group whose members try to minimize conflict and reach consensus without critically testing, analyzing and evaluating ideas</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Group polarization: tendency of people to make decisions that are more extreme when they are in a group as opposed to a decision made alone or independently</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Subjection to leader: need for taking initiative disappears or is not there</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Fight – Flight: defending by fight or flight. “They vs us”. Put the blame somewhere else</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Partnering up, with possibility of splitting group</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
- **Recognition-primed decision making**
  Very important for debrief!

<table>
<thead>
<tr>
<th>Stage</th>
<th>Observation</th>
</tr>
</thead>
<tbody>
<tr>
<td>Impact of the experience of each individual</td>
<td>• CEO ...</td>
</tr>
<tr>
<td></td>
<td>• Board-Member ...</td>
</tr>
<tr>
<td></td>
<td>• CISO ...</td>
</tr>
<tr>
<td></td>
<td>• Communications / PR ...</td>
</tr>
<tr>
<td></td>
<td>• Business Leader ...</td>
</tr>
<tr>
<td>Processes which were developed in the simulation</td>
<td></td>
</tr>
<tr>
<td>Facts, concepts and principles which were used in the simulation</td>
<td></td>
</tr>
<tr>
<td>The ways in which emotion was involved in or figured in the simulation (individually)</td>
<td>• CEO ...</td>
</tr>
<tr>
<td></td>
<td>• Board-Member ...</td>
</tr>
<tr>
<td></td>
<td>• CISO ...</td>
</tr>
<tr>
<td></td>
<td>• Communications / PR ...</td>
</tr>
<tr>
<td></td>
<td>• Business Leader ...</td>
</tr>
<tr>
<td>The ways in which emotion was involved in or figured in the simulation (group)</td>
<td></td>
</tr>
<tr>
<td>Different views which each of the participants formed of the nature of the processes and the experience.</td>
<td>• CEO ...</td>
</tr>
<tr>
<td></td>
<td>• Board-Member ...</td>
</tr>
<tr>
<td></td>
<td>• CISO ...</td>
</tr>
<tr>
<td></td>
<td>• Communications / PR ...</td>
</tr>
<tr>
<td></td>
<td>• Business Leader ...</td>
</tr>
</tbody>
</table>
## Other

<table>
<thead>
<tr>
<th>Observation</th>
<th>Notes</th>
</tr>
</thead>
<tbody>
<tr>
<td>Is there dominance from a particular participant?</td>
<td></td>
</tr>
<tr>
<td>Do people stay in their role?</td>
<td></td>
</tr>
<tr>
<td>How is the decision making? Democratic, Position, functions left out?</td>
<td></td>
</tr>
<tr>
<td>Did their demeanor change during the game?</td>
<td></td>
</tr>
<tr>
<td>Biggest discussion items</td>
<td></td>
</tr>
<tr>
<td>Biggest obstacles (uncertainty, lack of information, disagreement, fear of negative response, over analysis)</td>
<td></td>
</tr>
<tr>
<td>Eagerness or reluctance to act? And what shapes it?</td>
<td></td>
</tr>
<tr>
<td>Main Contributors to spending resources (which are more important)</td>
<td></td>
</tr>
<tr>
<td>Is there a strategy involved?</td>
<td></td>
</tr>
<tr>
<td>-----------------------------</td>
<td>--</td>
</tr>
<tr>
<td>Are people looking for arguments instead of using abstract models and information provided? (in other words, are they using experience instead of awareness?)</td>
<td></td>
</tr>
</tbody>
</table>
➢ Important but not included in the logging form
# Self-Evaluation Form Participants – For Debriefing

<table>
<thead>
<tr>
<th><strong>Name:</strong></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Function:</strong></td>
<td></td>
</tr>
<tr>
<td><strong>Department:</strong></td>
<td></td>
</tr>
<tr>
<td><strong>Years of Experience:</strong></td>
<td></td>
</tr>
<tr>
<td><strong>Which role did you play?</strong></td>
<td></td>
</tr>
<tr>
<td><strong>What were your expectations coming into this simulation session?</strong></td>
<td></td>
</tr>
</tbody>
</table>

## Self-evaluation

| **Were emotions part of participating in this game?** |  |
| **What is your learning preference?** | o Adopting best practices  
o Participate  
o Acquire Knowledge  
o Practice  
o Exploration |
| **Did you rely on experience to base your arguments on rather than the information given?** |  |
| **Would you approach the game differently the second time?** |  |
| **Did you enjoy playing the game? Why?** |  |
| **On a scale from 1-10 how well did you do?** |  |
| **On a scale from 1-10 how well did you achieve your individual objectives?** |  |
(Fill this in after the debriefing) Learning from the Simulation Game

| Learning the Facts: expressed in the game contexts and dynamics (cross whichever applicable) | Cyber Security Concepts / Stakeholders  
|                                                                                                      | Crisis Management Concepts / Stakeholders |
| Learning the crisis management process                                                                 | Some  
|                                                                                                      | Yes  
|                                                                                                      | No |
| Learning decision-making aspects                                                                      | Potential Consequences  
|                                                                                                      | Uncertainty  
|                                                                                                      | Risks of Decision making  
|                                                                                                      | Potential Rewards  
|                                                                                                      | Benefits  
|                                                                                                      | Risks |
| Were the game elements clear by itself? If so how?                                                    | |
| How realistic was the game?                                                                           | |
| The simulation has attractive materials.                                                               | Some  
|                                                                                                      | Yes  
|                                                                                                      | No |
| Would you recommend others to play this game? (why?)                                                  | |
| Any Suggestions to improve the game?                                                                  | |
| How engaged were you in the simulation game (1-10), please explain?                                  | |
| How challenged were you by the simulation game (1-10), please explain?                               | |
Debriefing

In general, the debriefing is done by the participants. However, to remain in structure guidelines are provided in for when the discussions are need a hunch.

**Step 1.** Ask Participants to fill in the self-evaluation form. In this way, individual experiences are not lost in the heat of the general discussion.

**Step 2.** Reflect on the worst case scenarios vs. the actual outcome

**Step 3.** Let them go through the created timelines and discuss the tasks, procedures and methods, process (or interaction) and emotions. This involves all the observations made (above) and the self-reflection which is done by the participants.

**Note.** Use the following theoretical cycle:
1. Returning to the experience: consisting of a recollection of experience, replaying the events, or recalling them to others. In other words, it is the initial perception of what happened from the individual’s perspective
2. Attending to feelings: this involves capitalizing on and using the positive feelings which come from the experience, but also considering the negative feelings. This aspect is a vital part of reflection.
3. Re-evaluating the experience: this involves reexamination of the experience, specifically in the light of the first two stages. The difference between any evaluation during the experience, or immediately after it (or both), is that reevaluation is more considered, leading to the internalization of the new knowledge, skills, or attitudes or mind and mental apparatus of the learner.
D.5 Rules

<table>
<thead>
<tr>
<th>Rules of the Game</th>
</tr>
</thead>
</table>

1. Participants do not share the contents of their briefing packages.

2. Everybody has their own objectives & different amount of coins available to them.

3. Every communication between both teams are “on the record”

6. When certain actions have not been taken before the specified time, the team is penalized

8. Every action costs a specified number of resources (symbolized by coins. Note that these do not only represent money, but also efforts).

6. The action list is not exhaustive. You are free to conduct in a natural way. Facilitators are free to put a price on the actions.
D.6 Events

- Rumor has it (definitely the first)

<table>
<thead>
<tr>
<th>Provide to:</th>
<th>Crisis Team - CEO</th>
</tr>
</thead>
<tbody>
<tr>
<td>Message:</td>
<td>Give the CEO the briefing. This will contain the information which require the situation. The CEO has to explain why the team is called together. They receive their first message, from the business that customers are emailing and calling to ask what / there is something going on.</td>
</tr>
<tr>
<td>Action</td>
<td>Response</td>
</tr>
<tr>
<td>Wait</td>
<td>Nothing</td>
</tr>
<tr>
<td>Request</td>
<td>Nobody knows about anything... so response is short and brief.</td>
</tr>
<tr>
<td>Information</td>
<td></td>
</tr>
<tr>
<td>Other</td>
<td>Depending on the situation</td>
</tr>
</tbody>
</table>

Note: the media team already has more information and started their research

- Customers and partners complains

<table>
<thead>
<tr>
<th>Provide to:</th>
<th>Crisis Team – Business Leader</th>
</tr>
</thead>
<tbody>
<tr>
<td>Message:</td>
<td>Pressure from the outside. Call the business leader, with the message: “Hello …, your secretary here... I have been called 40 times already from our biggest accounts. They want to know what information is available. What do I tell them?? Please communicate this through the communication portal. You have 15 minutes. Please act.”</td>
</tr>
<tr>
<td>Action</td>
<td>Response</td>
</tr>
<tr>
<td>Passing</td>
<td>A sigh of relieve...</td>
</tr>
<tr>
<td>Failing</td>
<td>The team will lose 5 coins</td>
</tr>
</tbody>
</table>

Note: This should increase pressure from the participants.

- 3rd Party Message: Sorry that we did not inform you

<table>
<thead>
<tr>
<th>Provide to:</th>
<th>Crisis Team – CISO</th>
</tr>
</thead>
<tbody>
<tr>
<td>Message:</td>
<td>One piece of information. Call the CISO, with the message: “Hey this is Tech Daily. We’ve developed and maintain the following applications for you: SWAN, FINAMP, BROW and MCTH. They all use the same backbone, and we found out that there are some vulnerabilities in all of them that haven’t been spot earlier. Sorry that we have mentioned so late. Hope this is fine.”</td>
</tr>
</tbody>
</table>

SWAN: communications tool with deliveries (partner portal)
FINAMP: Predictive financial models. (Internal)
BROW: clients check their investments through this portal (client-facing)
MCTH: links several personal identifiable documents together (internal)

Shut these down until the situation is stabilized! You have 20 minutes

<table>
<thead>
<tr>
<th>Action</th>
<th>Response</th>
<th>Time Delay</th>
</tr>
</thead>
<tbody>
<tr>
<td>Passing</td>
<td>A sigh of relieve..</td>
<td>None</td>
</tr>
<tr>
<td>Failing</td>
<td>The team will lose 7 coins</td>
<td>20 minutes</td>
</tr>
</tbody>
</table>

**Note:** This guides them into a certain direction.

- **Shareholder pressure**

  **Provide to:** Crisis Team – CFO

  **Message:**
  Pressure from the outside. Call the CFO, with the message: “Hello …, your secretary here... I have been called 40 times already from our shareholders. They want to know how bad the situations is? What do I tell them?? Please communicate this through the communication portal. You have 15 minutes. Please act.”

<table>
<thead>
<tr>
<th>Action</th>
<th>Response</th>
<th>Time Delay</th>
</tr>
</thead>
<tbody>
<tr>
<td>Passing</td>
<td>A sigh of relieve..</td>
<td>None</td>
</tr>
<tr>
<td>Failing</td>
<td>The team will lose 5 coins</td>
<td>15 minutes</td>
</tr>
</tbody>
</table>

  **Note:** This should increase pressure from the participants.

- **Internal employees ask how to handle**

  **Provide to:** Crisis Team – Communication / PR

  **Message:**
  “Hi…., This is your deputy calling. We receive a lot of calls regarding a statement from your side. But we do not know which way to respond. What do we have to tell them and which message do you want to convey??” You have 15 minutes – communicate through the portal.

<table>
<thead>
<tr>
<th>Action</th>
<th>Response</th>
<th>Time Delay</th>
</tr>
</thead>
<tbody>
<tr>
<td>Wait</td>
<td>Nothing</td>
<td>None</td>
</tr>
<tr>
<td>Offer information</td>
<td>The communication will continue like this. And any other communication should be weighted with this one.</td>
<td>15 minutes</td>
</tr>
<tr>
<td>None provided</td>
<td>Lose 7 coins. There is more uncertainty inside the information.</td>
<td>15 minutes</td>
</tr>
</tbody>
</table>

  **Note:** Asks them to communicate their strategy.

- **Attackers reveal what they want**
Provide to: Crisis Team & Media Team

Message:
We have shown you want we have.. you might be wondering WHY?? Well you have money, we want it. Simple as that. Transfer 300 coins in bitcoins to 0d10bf887eb68afa422ba799a7cc38e59a422ecd. We give you 15 minutes to decide what to do. We will stop if you do.. otherwise.. we will keep going

<table>
<thead>
<tr>
<th>Action</th>
<th>Response</th>
<th>Time Delay</th>
</tr>
</thead>
<tbody>
<tr>
<td>Wait</td>
<td>Drop another data bomb</td>
<td>20 minutes</td>
</tr>
<tr>
<td>Pay</td>
<td>Say thanks! But still drop a bomb after 25 minutes</td>
<td>25 minutes</td>
</tr>
<tr>
<td>Request Information</td>
<td>Nobody knows about anything... so response is short and brief..</td>
<td>5 minutes</td>
</tr>
<tr>
<td>Investigate internally</td>
<td>We have no idea what they have.. it could be everything, but could be nothing</td>
<td>15 minutes</td>
</tr>
<tr>
<td>Communicate</td>
<td>Depends on the situation</td>
<td>Depending on the situation</td>
</tr>
<tr>
<td>Other</td>
<td>Depends on the situation</td>
<td>Depending on the situation</td>
</tr>
</tbody>
</table>

Note:
- Imposters make claims

Provide to: Crisis Team & Media Team

Message:
This might be an interesting proposition to you. We have seen you are investing heavily in Nucleo. But they are crooks! They provide weapons for war zones. Even though it seems that you make quite a bit of money on them, we want you to quit your collaboration. Call them now, to cancel your contract.. otherwise we will continue the terror.

<table>
<thead>
<tr>
<th>Action</th>
<th>Response</th>
<th>Time Delay</th>
</tr>
</thead>
<tbody>
<tr>
<td>Wait</td>
<td>Nothing</td>
<td>None</td>
</tr>
<tr>
<td>Call Nucleo</td>
<td>Nucleo gets mad and walks to the media</td>
<td>10 minutes</td>
</tr>
<tr>
<td>Request Information</td>
<td>Provide them with the relationship with Nucleo. They are clearly not the best relationship you have. But you make over 10 million euros yearly only on this account.</td>
<td>5 minutes</td>
</tr>
<tr>
<td>Communicate</td>
<td>Depends on the situation</td>
<td>Depending on the situation</td>
</tr>
<tr>
<td>Other</td>
<td>Depends on the situation</td>
<td>Depending on the situation</td>
</tr>
</tbody>
</table>

Note:
- Prepare for the Press Release
We cannot wait any longer. Press is on our tail and we really need to provide some answers to the general public.

Everybody has to write up a press release! They all need to be ready for the questions. Media prepares 5 questions each.

<table>
<thead>
<tr>
<th>Action</th>
<th>Response</th>
<th>Time Delay</th>
</tr>
</thead>
<tbody>
<tr>
<td>They have to prepare</td>
<td>We decide randomly who has to give the press release</td>
<td>15 minutes</td>
</tr>
</tbody>
</table>

**Note:**

- Regulators knock doors

**Provide to:** Crisis Team (CEO)

**Message:**

Shouldn’t you notify us?????? If this turns out to be huge, you will hear from us soon. You have 10 minutes.

<table>
<thead>
<tr>
<th>Action</th>
<th>Response</th>
<th>Time Delay</th>
</tr>
</thead>
<tbody>
<tr>
<td>Wait</td>
<td>Nothing</td>
<td>Fine! 10% of their coins</td>
</tr>
<tr>
<td>Inform</td>
<td>Provide which information</td>
<td>5 minutes</td>
</tr>
<tr>
<td>Other</td>
<td>Depending on the situation</td>
<td>Depending on the situation</td>
</tr>
</tbody>
</table>

**Note:** This is something they should do!

- Media Demands answers

**Provide to:** Crisis Team – Communications / PR

**Message:**

What’s going on!? We know this is happening, but they haven’t informed anybody about ANYTHING.. we suspect that something deeper is going on. Please elaborate. (Phone call)

<table>
<thead>
<tr>
<th>Action</th>
<th>Response</th>
<th>Time Delay</th>
</tr>
</thead>
<tbody>
<tr>
<td>Wait</td>
<td>Media is free to speculate</td>
<td>Depends on MT</td>
</tr>
<tr>
<td>Inform</td>
<td>Good – Media can take that into account</td>
<td>Depends on MT</td>
</tr>
<tr>
<td>Other</td>
<td>Depending on the situation</td>
<td>Depending on the situation</td>
</tr>
</tbody>
</table>

**Note:**
D.7 Leaked information
Screenshots of the “leaked information”. Generated automatically.
<table>
<thead>
<tr>
<th>A</th>
<th>B</th>
<th>C</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>BSN</td>
<td>Account</td>
</tr>
<tr>
<td>Mark Hempstead</td>
<td>410342204</td>
<td>348753150</td>
</tr>
<tr>
<td>Esther Hoover</td>
<td>540220511</td>
<td>639716456</td>
</tr>
<tr>
<td>Amy Recher</td>
<td>847810985</td>
<td>513484648</td>
</tr>
<tr>
<td>Melvin Tester</td>
<td>761499169</td>
<td>44564449</td>
</tr>
<tr>
<td>Steven Theiss</td>
<td>234848990</td>
<td>382011592</td>
</tr>
<tr>
<td>Ivy Blackwell</td>
<td>745126919</td>
<td>480246891</td>
</tr>
<tr>
<td>James Turner</td>
<td>384039983</td>
<td>855231204</td>
</tr>
<tr>
<td>Jacob Betance</td>
<td>456560547</td>
<td>26246138</td>
</tr>
<tr>
<td>Joseph Zack</td>
<td>645570002</td>
<td>58990842</td>
</tr>
<tr>
<td>Delia Whitley</td>
<td>934876810</td>
<td>932526154</td>
</tr>
<tr>
<td>Leia Fernandez</td>
<td>893922361</td>
<td>13460178</td>
</tr>
<tr>
<td>Elizabeth Kitchen</td>
<td>126372003</td>
<td>853723754</td>
</tr>
<tr>
<td>Johnathan Page</td>
<td>525861247</td>
<td>352113542</td>
</tr>
<tr>
<td>Malcolm Flaim</td>
<td>205540067</td>
<td>431435848</td>
</tr>
<tr>
<td>Jessica Nelson</td>
<td>286290222</td>
<td>678262019</td>
</tr>
<tr>
<td>Virgie Stergios</td>
<td>369622902</td>
<td>835571008</td>
</tr>
<tr>
<td>Lillian Davis</td>
<td>852718334</td>
<td>942256282</td>
</tr>
<tr>
<td>Dean Dillard</td>
<td>358799433</td>
<td>498882781</td>
</tr>
<tr>
<td>David Seabron</td>
<td>279216458</td>
<td>565882284</td>
</tr>
<tr>
<td>Clifford Fraley</td>
<td>640338026</td>
<td>493568074</td>
</tr>
<tr>
<td>Billie Laschinger</td>
<td>132551808</td>
<td>145260268</td>
</tr>
<tr>
<td>Richard Knight</td>
<td>568873107</td>
<td>764200606</td>
</tr>
</tbody>
</table>

206
<table>
<thead>
<tr>
<th></th>
<th>First</th>
<th>Last</th>
<th>email</th>
<th>phone</th>
<th>BSN</th>
<th>wage</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Bonnie</td>
<td>Tellez</td>
<td>B.Tellez@Fin</td>
<td>3149913516</td>
<td>235353257</td>
<td>49,531.00</td>
</tr>
<tr>
<td>2</td>
<td>Nathan</td>
<td>Bouknight</td>
<td>N.Bouknight@Fin</td>
<td>3141584788</td>
<td>363378897</td>
<td>756,371.00</td>
</tr>
<tr>
<td>3</td>
<td>Carl</td>
<td>Mitchell</td>
<td>C.Mitchell@Fin</td>
<td>3171388997</td>
<td>739656479</td>
<td>713,447.00</td>
</tr>
<tr>
<td>4</td>
<td>Maria</td>
<td>Perdue</td>
<td>M.Perdue@Fin</td>
<td>3159263545</td>
<td>888474161</td>
<td>163,628.00</td>
</tr>
<tr>
<td>5</td>
<td>Nora</td>
<td>Tolin</td>
<td>N.Tolin@Fin</td>
<td>3117429290</td>
<td>338186778</td>
<td>454,127.00</td>
</tr>
<tr>
<td>6</td>
<td>Mike</td>
<td>Kennedy</td>
<td>M.Kennedy@Fin</td>
<td>3165230770</td>
<td>871481920</td>
<td>689,147.00</td>
</tr>
<tr>
<td>7</td>
<td>George</td>
<td>Adkins</td>
<td>G.Adkins@Fin</td>
<td>313118250</td>
<td>542514399</td>
<td>544,560.00</td>
</tr>
<tr>
<td>8</td>
<td>James</td>
<td>Davis</td>
<td>J.Davis@Fin</td>
<td>3196805993</td>
<td>743351133</td>
<td>640,673.00</td>
</tr>
<tr>
<td>9</td>
<td>Antonia</td>
<td>Nowlin</td>
<td>A.Nowlin@Fin</td>
<td>3187334809</td>
<td>118035150</td>
<td>129,920.00</td>
</tr>
<tr>
<td>10</td>
<td>Arthur</td>
<td>Colbert</td>
<td>A.Colbert@Fin</td>
<td>3199069410</td>
<td>886580509</td>
<td>461,764.00</td>
</tr>
<tr>
<td>11</td>
<td>Robert</td>
<td>Hayes</td>
<td>R.Hayes@Fin</td>
<td>3181433036</td>
<td>945522073</td>
<td>492,799.00</td>
</tr>
<tr>
<td>12</td>
<td>Carolyn</td>
<td>Lockhart</td>
<td>C.Lockhart@Fin</td>
<td>3132290102</td>
<td>349528656</td>
<td>251,582.00</td>
</tr>
<tr>
<td>13</td>
<td>Paul</td>
<td>Bullock</td>
<td>P.Bullock@Fin</td>
<td>3115419315</td>
<td>293665657</td>
<td>683,506.00</td>
</tr>
<tr>
<td>14</td>
<td>Christina</td>
<td>Davis</td>
<td>C.Davis@Fin</td>
<td>3190518222</td>
<td>791699681</td>
<td>166,268.00</td>
</tr>
<tr>
<td>15</td>
<td>Charles</td>
<td>Turner</td>
<td>C.Turner@Fin</td>
<td>3194740027</td>
<td>219974312</td>
<td>283,120.00</td>
</tr>
<tr>
<td>16</td>
<td>Carl</td>
<td>Lanigan</td>
<td>C.Lanigan@Fin</td>
<td>313644325</td>
<td>815145109</td>
<td>472,408.00</td>
</tr>
<tr>
<td>17</td>
<td>Henrietta</td>
<td>Durall</td>
<td>H.Durall@Fin</td>
<td>3161727170</td>
<td>578458529</td>
<td>125,171.00</td>
</tr>
<tr>
<td>18</td>
<td>Jon</td>
<td>Andersen</td>
<td>J.Andersen@Fin</td>
<td>3190637399</td>
<td>289555170</td>
<td>395,674.00</td>
</tr>
<tr>
<td>19</td>
<td>Gonzalo</td>
<td>Fields</td>
<td>G.Fields@Fin</td>
<td>3139618069</td>
<td>436182767</td>
<td>608,754.00</td>
</tr>
<tr>
<td>20</td>
<td>Elizabeth</td>
<td>Tarango</td>
<td>E.Tarango@Fin</td>
<td>3153839615</td>
<td>279564782</td>
<td>192,376.00</td>
</tr>
<tr>
<td>21</td>
<td>Kayleigh</td>
<td>Neveu</td>
<td>K.Neveu@Fin</td>
<td>3170374317</td>
<td>110552496</td>
<td>356,158.00</td>
</tr>
<tr>
<td>22</td>
<td>Teresa</td>
<td>Winters</td>
<td>T.Winters@Fin</td>
<td>3178113791</td>
<td>780998215</td>
<td>484,012.00</td>
</tr>
<tr>
<td>23</td>
<td>Michael</td>
<td>Foley</td>
<td>M.Foley@Fin</td>
<td>3186832842</td>
<td>733354447</td>
<td>487,366.00</td>
</tr>
<tr>
<td>24</td>
<td>Peter</td>
<td>Escalante</td>
<td>P.Escalante@Fin</td>
<td>3187899468</td>
<td>226277360</td>
<td>550,269.00</td>
</tr>
<tr>
<td>25</td>
<td>Tony</td>
<td>Stutzman</td>
<td>T.Stutzman@Fin</td>
<td>3126258324</td>
<td>969752716</td>
<td>353,446.00</td>
</tr>
<tr>
<td>26</td>
<td>James</td>
<td>Russell</td>
<td>J.Russell@Fin</td>
<td>3157773577</td>
<td>802475190</td>
<td>745,438.00</td>
</tr>
<tr>
<td>27</td>
<td>Una</td>
<td>Mattera</td>
<td>U.Mattera@Fin</td>
<td>3174081857</td>
<td>259943373</td>
<td>527,254.00</td>
</tr>
</tbody>
</table>
-----BEGIN CERTIFICATE-----
KmgFjqOEPnRkkQmbZtMUuqjSMnPnXKQrTBtctcMwpGuTbpfyyoppBLRZssywagsFaVnUpgRWJabpEbHLWdAbAWgfb
fpZBuzq2GANrBooFNS5EsibSkEpSkpDlDx5LiixxxvPfpgOuuj3pZhyuCNQJxjuywuzetJyLFLnPnGyCyU
DmKcOQaWCDvSNQfSnlWhbuuqBGjtGHCMSmqgHPbCgZsMPUC1HEXXqOpxSjyCxEJMcEdnVLvQpxLFK
yan0jKQqBxfmKCDMePqZCuwcK8UHgBnChzEzBHdrDEPErXyfzHzOMvqShvQ0kQpWypnKyaavNZ1YkFfEBkLrmG
PPbCWsTMurxOnDHaSbInhuaKlgLRKHFNBEKyeEQvVYhbbweYgCyHOCwqofeJqjJBySyboPtUewHAqKxeZsrgf
b

-----END CERTIFICATE-----
<table>
<thead>
<tr>
<th>Service</th>
<th>Server</th>
<th>Response</th>
<th>IP</th>
<th>function</th>
</tr>
</thead>
<tbody>
<tr>
<td>STEP</td>
<td>Apache</td>
<td>200</td>
<td>123.16.864.850</td>
<td>client-facing</td>
</tr>
<tr>
<td>RAWE</td>
<td>Apache</td>
<td>200</td>
<td>123.16.295.326</td>
<td>internal use</td>
</tr>
<tr>
<td>ZAPP</td>
<td>Apache</td>
<td>200</td>
<td>123.16.382.970</td>
<td>partner portal</td>
</tr>
<tr>
<td>BACK</td>
<td>Apache</td>
<td>200</td>
<td>123.16.221.545</td>
<td>administration</td>
</tr>
<tr>
<td>STUM</td>
<td>Apache</td>
<td>200</td>
<td>123.16.230.381</td>
<td>partner portal</td>
</tr>
<tr>
<td>LEE</td>
<td>Apache</td>
<td>200</td>
<td>123.16.256.396</td>
<td>partner portal</td>
</tr>
<tr>
<td>DRIS</td>
<td>Apache</td>
<td>200</td>
<td>123.16.901.774</td>
<td>internal use</td>
</tr>
<tr>
<td>FAY</td>
<td>Apache</td>
<td>200</td>
<td>123.16.443.533</td>
<td>partner portal</td>
</tr>
<tr>
<td>OWEN</td>
<td>Apache</td>
<td>200</td>
<td>123.16.392.796</td>
<td>partner portal</td>
</tr>
<tr>
<td>CATH</td>
<td>Apache</td>
<td>200</td>
<td>123.16.117.507</td>
<td>client-facing</td>
</tr>
<tr>
<td>MAXW</td>
<td>Apache</td>
<td>200</td>
<td>123.16.659.684</td>
<td>partner portal</td>
</tr>
<tr>
<td>COBE</td>
<td>Apache</td>
<td>200</td>
<td>123.16.925.967</td>
<td>internal use</td>
</tr>
<tr>
<td>GORM</td>
<td>Apache</td>
<td>200</td>
<td>123.16.879.868</td>
<td>client-facing</td>
</tr>
<tr>
<td>DOWN</td>
<td>Apache</td>
<td>200</td>
<td>123.16.885.815</td>
<td>partner portal</td>
</tr>
<tr>
<td>CARD</td>
<td>Apache</td>
<td>200</td>
<td>123.16.602.817</td>
<td>client-facing</td>
</tr>
<tr>
<td>INMA</td>
<td>Apache</td>
<td>200</td>
<td>123.16.628.93</td>
<td>client-facing</td>
</tr>
<tr>
<td>BAKE</td>
<td>Apache</td>
<td>200</td>
<td>123.16.48.47</td>
<td>internal use</td>
</tr>
<tr>
<td>COOK</td>
<td>Apache</td>
<td>200</td>
<td>123.16.249.315</td>
<td>client-facing</td>
</tr>
<tr>
<td>STEW</td>
<td>Apache</td>
<td>200</td>
<td>123.16.278.840</td>
<td>internal use</td>
</tr>
<tr>
<td>LOTH</td>
<td>Apache</td>
<td>200</td>
<td>123.16.331.150</td>
<td>internal use</td>
</tr>
<tr>
<td>DYE</td>
<td>Apache</td>
<td>200</td>
<td>123.16.110.883</td>
<td>client-facing</td>
</tr>
<tr>
<td>WHIT</td>
<td>Apache</td>
<td>200</td>
<td>123.16.905.902</td>
<td>partner portal</td>
</tr>
<tr>
<td>JUST</td>
<td>Apache</td>
<td>200</td>
<td>123.16.212.161</td>
<td>internal use</td>
</tr>
<tr>
<td>HUMP</td>
<td>Apache</td>
<td>200</td>
<td>123.16.446.485</td>
<td>partner portal</td>
</tr>
<tr>
<td>LEE</td>
<td>Apache</td>
<td>200</td>
<td>123.16.567.872</td>
<td>partner portal</td>
</tr>
<tr>
<td>MILL</td>
<td>Apache</td>
<td>200</td>
<td>123.16.602.380</td>
<td>internal use</td>
</tr>
<tr>
<td>DREW</td>
<td>Apache</td>
<td>200</td>
<td>123.16.137.528</td>
<td>partner portal</td>
</tr>
<tr>
<td>AKIN</td>
<td>Apache</td>
<td>200</td>
<td>123.16.755.674</td>
<td>client-facing</td>
</tr>
<tr>
<td>GREY</td>
<td>Apache</td>
<td>200</td>
<td>123.16.90.826</td>
<td>partner portal</td>
</tr>
<tr>
<td>LOPE</td>
<td>Apache</td>
<td>200</td>
<td>123.16.103.453</td>
<td>internal use</td>
</tr>
<tr>
<td>SEAR</td>
<td>Apache</td>
<td>200</td>
<td>123.16.223.358</td>
<td>partner portal</td>
</tr>
<tr>
<td>LINE</td>
<td>Apache</td>
<td>200</td>
<td>123.16.0.419</td>
<td>client-facing</td>
</tr>
<tr>
<td>SHOU</td>
<td>Apache</td>
<td>200</td>
<td>123.16.884.786</td>
<td>internal use</td>
</tr>
</tbody>
</table>
ia$symbols = symbols
ia$symbol.names = symbol.names
ia$n = len(symbols)
ia$hist.returns = hist.returns

# convert to annual, year = 12 months
annual.factor = 12
ia$expected.return = annual.factor * ia$expected.return
ia$risk = sqrt(annual.factor) * ia$risk

# compute covariance matrix
ia$risk = iif(ia$risk == 0, 0.000001, ia$risk)
ia$cov = ia$cor * (ia$risk %% t(ia$risk))

### Create Efficient Frontier

ia = aa.test.create.ia()
n = ia$n

# 0 <= x.i <= 0.8
constraints = new.constraints(n, lb = 0, ub = 0.8)

# SUM x.i = 1
constraints = add.constraints(rep(1, n), 1, type = '=' , constraints)
### The Bank's 2015 Plan

<table>
<thead>
<tr>
<th></th>
<th>2016 budget</th>
<th>2015 actual</th>
</tr>
</thead>
<tbody>
<tr>
<td>Operating expenses</td>
<td>363.0</td>
<td>348.0</td>
</tr>
<tr>
<td>Bank note production</td>
<td>37.0</td>
<td>96.0</td>
</tr>
<tr>
<td>Non-current deferred employee benefits</td>
<td>14.0</td>
<td>(3.0)</td>
</tr>
<tr>
<td>MTP programs, including Head Office Renewal</td>
<td>19.0</td>
<td>37.0</td>
</tr>
<tr>
<td><strong>Total expenses</strong></td>
<td><strong>469.0</strong></td>
<td><strong>478.0</strong></td>
</tr>
</tbody>
</table>

#### 2016 Outlook

The Bank's forecasts for its operations do not include projections of net income and financial position. Such projections would require assumption about interest rates, which could be interpreted as a signal of future monetary policy.

Total operating expenses in 2016 are budgeted to decrease by Eur 9 million from 2015 levels.

Expenses related to bank note production are budgeted to be lower than in 2015 as a result of lower production volumes.

Operating costs associated with the Head Office Renewal Program are also budgeted to decrease in 2016, since the majority of costs associated with the project will be capital in nature.

In 2016, the Bank also budgeted to incur $208 million in capital expenditures, of which the majority relates to the Head Office Renewal Program.

At the end of the third quarter, the Bank was on track to deliver on its full-year Financial Plan.

#### Financial Discussion

##### Financial Position

The Bank's **Total assets** and **Total liabilities and equity** have increased by Eur 3,607.7 million since 31 December 2015 as a result of seasonal fluctuations in bank notes in circulation.

The Bank invests proceeds from the issuance of notes into Government securities. **Investments** have increased by Eur 6,110.9 million (7 percent).

Government of the Netherlands treasury bills increased by Eur 2,555.9 million and Government of Dutch bonds increased by Eur 3,510.7 million. The balance of the change in investments resulted from an increase of $44.3 million in the fair value of the Bank's investment shares of the Bank for International Settlements (BIS).
We showed the IT security is bad.. but now some proof that some might know this fact..

An email string showed up in the data in which a senior IT officer knew that his security protocols were not good enough. Conversing with IT auditors from a big4 company, it shows that even though the IT auditor has mentioned that several security protocols and implementations were far below par, James Jackson, threatened and the auditor to not write up the findings as a Sarbanes-Oxley violation.

He even mentioned to his colleagues that these auditors cannot tell him anything. I guess this message has never reached your Chief Information Security officer, did it?

Maybe it’s time to let this fella go..

- Anarchy Angels
Security Operating Center. There is an internal SOC deployed in India. In general, the SOC can detect simple external attacks but it stops there. When there is a hunch for a bigger attack, they always deploy a 3rd party expert to explore what happened. The SOC is capable to look back about 1 Month internally. There is data from previous Months, however this cannot be actively accessed by employees from the SOC.

Applications. Applications are developed within the Services Oriented Architecture (SOA), connected by APIs. There are about 1024 services available. Around 50 of those are critical for the company, some client-facing, some internal. The full list of applications is available as well as the list of the critical applications.
E. Screenshots of the Information System

Crisis Team

Overview of Crisis Communications

FinCorp Hack timeline

Messages to Crisis Team

Send a new Message:

To:
Isolate Systems Partially

Subject:

Message:

Urgency:
Very High

<table>
<thead>
<tr>
<th>Subject</th>
<th>To</th>
<th>Message</th>
</tr>
</thead>
<tbody>
<tr>
<td>E-mail to A-list clients</td>
<td>Other</td>
<td>E-mail towards our A-list clients responding to the situation with a crisis number that can be reached. We will be updating these clients during the process.</td>
</tr>
<tr>
<td>Investigation IT</td>
<td>Private email</td>
<td>Administrator Network - Please Start Scanning internal scanning on malware and potential leak in the outbound connection with third parties and suspicious country.</td>
</tr>
</tbody>
</table>
### Crisis Team Messages

**Danger: RE: Communication Strategy**
This call cost £0. Note that due to the complexity of the situation we will not be able to provide a strategy to you before 20:30.

2016-06-14 12:11

**Danger: How long are systems still down?**
- ...this already has been taking way too long...

2016-06-14 12:20

**Danger: Press Conference**
Please be advised that a press conference will take place at 20:30. All of you will have to be prepared to deliver the final statement to the press, and one representative will be randomly selected to present. Note that the press will also have a chance to ask you questions.

2016-06-14 12:35 - Deadline: 15 minutes

**Danger: you did not respond...**
How do you like your Q2 report? - AnonyAngels

2016-06-14 12:35

**Danger: CISO check your email**
This might be interesting??

2016-06-14 12:42
Overview of published articles

FinCorp Hack timeline

Messages to Media Team

Add a new Article:
Title:

Reporter Name:

Post:

Timeline Summary:
ECONOMY & INTERNET

Major data breach at renowned financial institution

Daniel
2016-06-09 14:42

Breaking news: Finance Daily have received a significant amount of confidential data from an anonymous source, who states that this data belongs to a large financial institution. This data is of such a confidential nature, that the impact could be disastrous to the organisation, should it truly relate back to them.
ECONOMY & INTERNET

FinCorp. Hack Timeline

2016-06-14 18:02

Financial Report leaked by data breach - (Jeroen)

Finance Daily has just received confidential financial data including the draft version of FinCorp’s financial statements for this year. This has major impact on their financial shareholders. Looking from a social perspective, we urge FinCorp to take action as soon as possible! Read more...

2016-06-14 17:57

FinCorp does not respond on major data breach - (Jeroen)

We have called FinCorp to get an interview about their major data breach. Communications is not willing to give an interview. From different customers we heard that a number of systems are shut down. FinCorp does not know how to handle this situation and what actions they should take. We hope this will not have a large impact on the customers. Read more...

2016-06-14 17:25

FinCorp confirms to be involved in data breach crisis - (Jeroen)

Finance Daily have been in contact with FinCrop, who have confirmed that it is their system that has been breached. At the moment they aren’t fully aware of the magnitude of the data breach. However, they have assured us that they have started an investigation and will do everything possible to keep the damage to a minimum for their affected customers and employees. A lot of clients have responded and are contemplating to switch from FinCorp to another organisation. Read more...
Facilitator controlling information

Received Messages from Crisis Team

<table>
<thead>
<tr>
<th>Message</th>
<th>Date</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Hire 3rd party advisors: advise on our security protocols</strong></td>
<td>2018-06-14 16:18</td>
</tr>
<tr>
<td>external consultant to fix sec protocols or design new ones.</td>
<td></td>
</tr>
<tr>
<td><strong>Hire 3rd party advisors: Advice on our PR</strong></td>
<td>2018-06-14 16:10</td>
</tr>
<tr>
<td>Consultancy on our communications strategy.</td>
<td></td>
</tr>
<tr>
<td><strong>Release Press Release on own website: Press release on website.</strong></td>
<td>2018-06-14 17:06</td>
</tr>
<tr>
<td>we have shut down some of the systems, awaiting our internal analysts to work out what the potential impact is. We will inform all involved parties as soon as information becomes available.</td>
<td></td>
</tr>
<tr>
<td><strong>other: Internal communication</strong></td>
<td>2018-06-14 17:47</td>
</tr>
<tr>
<td>E-mail to all employees, with an update on what is going on and how we are working to solve the problem. If there are questions, they can contact the following number (...)</td>
<td></td>
</tr>
</tbody>
</table>

**Send a Message to the Teams**

- FinCorp Hack timeline
- Messages to Crisis Team
- Messages to Media Team

**Send a new Message:**

**Team:**
- Crisis Team

**Header:**

**Message:**

**Type:**
- Danger / Penalty

**Timer:**
- None

Send
<table>
<thead>
<tr>
<th>Title</th>
<th>Message</th>
<th>Date</th>
</tr>
</thead>
<tbody>
<tr>
<td>RE: Communication Strategy</td>
<td>This will cost 20. Note that due to the complexity of the situation we will not be able to provide a...</td>
<td>2016-06-14 18:11</td>
</tr>
<tr>
<td>How long are systems still down?</td>
<td>... this already has been taking way too long.. I...</td>
<td>2016-06-14 18:09</td>
</tr>
<tr>
<td>Press Conference</td>
<td>Please be advised that a press conference will take place at 20:20. All of you will have to be prepa...</td>
<td>2016-06-14 18:03</td>
</tr>
<tr>
<td>you did not respond</td>
<td>how do you like your Q2 report? - Anarchy Angels...</td>
<td>2016-06-14 18:00</td>
</tr>
<tr>
<td>CiSO check your email</td>
<td>this might be interesting??...</td>
<td>2016-06-14 17:57</td>
</tr>
<tr>
<td>ANARCHYYYY</td>
<td>We have shown you what we have.. you might be wondering WHY?? Well you have money, we want it. Simpl...</td>
<td>2016-06-14 17:42</td>
</tr>
<tr>
<td>Regulators</td>
<td>As told on the telephone, you need to inform the regulators.. please what happened.. 5 minutes to go...</td>
<td>2016-06-14 17:39</td>
</tr>
<tr>
<td>CiSO received email</td>
<td>Ton, check your email. There are samples of the data....</td>
<td>2016-06-14 17:22</td>
</tr>
<tr>
<td>RE: Investigation IT</td>
<td>This is quite an extensive operation.. we have 1024 services running.. do you want to scan everythin...</td>
<td>2016-06-14 17:09</td>
</tr>
<tr>
<td>RE: e-mail to A-list clients</td>
<td>received thank you...</td>
<td>2016-06-14 17:07</td>
</tr>
<tr>
<td>CHECK THE TIMELINE</td>
<td>THERE IS A MESSAGE ON FDI...</td>
<td>2016-06-14 16:53</td>
</tr>
<tr>
<td>Warning</td>
<td>FinCorp we have your data. You will hear from us again soon, and we have demands. Prepare yourself. ...</td>
<td>2016-06-14 16:43</td>
</tr>
</tbody>
</table>