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

Hao Dinh
Delft University of Technology
c.h.dinh@student.tudelft.nl

ABSTRACT
Crisis situations require critical decision making under high uncertainty and time pressure. 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 consideration and offer a safe environment to practice decision making in. This paper presents the outcomes of a design process for this purpose. The proposed game immerses participants into a new world, in which a cyber crisis has occurred. The design is perceived as useful by participants but also provides three key findings for future design. The simulation game offers opportunity for extension, including for testing models and theories or as a foundation for similar game design.

Keywords
Cyber crisis, Simulation Game, Decision-making, Uncertainty, Situational Awareness

INTRODUCTION
This paper presents outcomes from a project on the development of a simulation game which provides a training methodology for senior-managers to practice decision-making during cyber crisis situations. With the increase of dependency on information from our application and services, many information systems have been linked together forming complex networks. In the last couple of years, data breaches and other information security incidents seem to be recurring headliners of major newspapers (Campbell et al., 2003).

During crisis, many overwhelming events need attention from crisis managers. Everything screams for attention at the same time. The need for adaptability and flexibility in crisis 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 well as adding flexibility increases effectiveness (Mendonca et al, 2006; Lindstrom & Pettersson, 2007).

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. Examples are, emergency planning (Chrinchton, 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 is done upfront. They help enable rapid coordination of actions (Rankin et al., 2013). However, one important notion 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, deal with uncertainty.

Even though there is a 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. Given this, preparing for crisis blindly trusting only on static documents is unwise and should be added with training methods which prepares crisis managers to deviate effectively from planning when deemed necessary.
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 incident within a single 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 crises through the use of simulation games.

Crisis simulations are designed to take rare and uncertain situations into account. Gestwicki and Strumbaugh (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. Borodzicz & 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. These are typically performed in a simulated environment, which received much effort from the academic community in developing these environments and assessing the effects (Bergstrom et al., 2012). Specifically, simulation games 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 crisis, 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 situations while being immersed in a (safe) simulated environment.

**Related work**

A couple of crisis simulation papers exist which focus around a cyber security 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. Examples are to improve communication and collaboration (Pherson and Bishop, 2014) and the exploration of how individual users respond to cyber-based financial fraud and identity theft (Rosoff et al., 2014). This type of research is focused on behavioral aspects, but do not address training on cyber concepts or focus on decision-making aspects.

Secondly, a large group of cyber security simulations focus strongly on education and awareness for children and teenagers. Examples are the use of joy and efficiency to increase awareness (Giannakes et al., 2015) and teaching high-school kids cyber security concepts (Salazar et al., 2013).

One cyber simulation game which focuses on decision-making aspects and their consequences is CyberCIEGE (Bishop and Frincke, 2005). This game focuses on increasing the awareness of the impact of poor security choices and the concrete steps that students can take which improves security in the game. 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 game does focus on players’ decision-making, however not on senior-management level.

Gestwicki and Stumabugh (2015) analyzed 21 games, focused on teenagers, which designed to teach cybersecurity concepts. They conclude with the concern on the existing literature that very little researches explain, contextualize or justify their designs.

A review on the crisis and cyber security simulation 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 and teenagers. These types of games are mostly focused on prevention. Finally, Cybersecurity simulation game literature lack explanation of design choices, contextualization or justification.

**Objective and Research question**

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.
The objective of the research is designed 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 environment for participants to practice decision making under crisis characteristics like time-pressure and uncertainty.*

This research objective involves three important aspects. First, the research requires a research design approach, in which 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 game is required.

By following a research design methodology, the following main question is answered: *How to support senior-managers in preparing for Cyber Crisis decision-making by means of crisis simulation games?*

The following sections will guide the reader through the different elements that the simulation game beholds and how each step in the process has influenced the design. Finally, the main research question is answered and the outcomes of this paper are discussed.

**METHODOLOGY**

The simulation game design effort is guided by a research design approach. Hevner’s *three cycle view of Design Science Research* (2007) is 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 construction of the artifact focuses more on the research goal, instead of the urge to optimize organizational fit. 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. 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 Caluwé 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.

As depicted in figure 1, the process starts with the *need for a Cyber Crisis Simulation game*, already discussed in the introduction. From here, the process during the research is not as linearly as depicted in figure 2. In other words, the process is more iterative and jumping between application domain and knowledge base. The theoretical framework follows first, as it provides the outset of the simulation game design, regardless of requirements and important application domain concepts. It provides a blueprint simulation game which fit the outlined research goal. Following are sections from the application domain in which the practitioners view is elaborated. Eight semi-structured interviews are conducted with six cybersecurity experts, one crisis management expert and one business leader which experienced a cyber crisis and consequences in the past. The practitioners view provides both the relevant concepts and models from the Crisis literature and the requirements. From there the simulation game design initiates. After two test sessions of the prototype, the simulation game is evaluated for its perceived usefulness.
Figure 1: Steps of the Cyber Crisis Simulation Game Design

DESIGN: Simulation Game Development for decision-making under Uncertainty

Requirements and Design Choices
Prior to the development of the simulation game several requirements are defined, based on the experience and knowledge of experts. First, the simulation game offers participants to test and assess the effectiveness of the team and preparation plans defined, during times of cyber crisis. Second, participants are introduced to the complexities linked to cyber crisis and its decision-making. Third, 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. Fourth, the simulation game involves group dynamics and emotions. Fifth, the simulation game is grounded in reality and provides practice for future situations. Finally, participants learn from each other during debriefing. Specifically, focusing on why and how they made decisions during the situation and their consequences.

For these reasons, the game focuses on interactions from both internal and external stakeholders, simulating a close-to-real experience of decision making in a cyber crisis. Each simulation run has a similar beginning and an end, but is flexible in the center, in which facilitators have the freedom to lengthen and shorten the game based on evaluation of the game during play. This happens by introducing less or more events during the crisis situation.

Given the above mentioned requirements as well as the conducted interviews with experts the following design choices were made:

The level of reality. One of the requirements is that the game is grounded in reality. There are two aspects that can be made realistic in this case 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. To find a common ground to both aspects in reality the following is chosen: the game revolves around a fictive organization, in which the scenario and situation is as real as possible. This enables the possibility to keep the game generalizable, when participants from different organizations are involved, but can be easily tailored to an organization when a group from a single organization participates.

Target Participants. The game can host participants from different organizations. Different test sessions showed that the game was enjoyable and challenging irrespectively of the experience, organization or function.

Balance between patronizing and explaining background information. An 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 individuals. Therefore, it is important to balance patronizing and giving them background information.
**Duration of the Simulation Game.** The target participant is a senior-manager within an organization. In this sense, one can assume that blocking such a person’s agenda is challenging and can be costly for the organization. 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. Therefore, the game will take four hours in total.

**Number of facilitators.** From the organizing 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. Initially the game will have three facilitators.

**Location independent.** The game needs to be portable. In other words, the number of physical elements, that do not necessarily have to do with any contextual factors.

**When did the participants do well?** As this game evolves around building a narrative, which is reflected in the debriefing, the participant’s effectiveness has to be evaluated by themselves in the reflection and evaluation rounds.

**Own role or different?** 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 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 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.

**Cooperation or Competition?** Finally, 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, but also have their personal goals. In the end they reflect on their actions, team work and emotions.

**Proposed Simulation Game Design**

The proposed game immerses 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.

The game is played with five players plus three facilitators, in two separate rooms. The game starts with a general briefing. After which participants choose their role. When the CEO is briefed separately the game commences. And here is where the chaos starts. Two main phases are simulated in the game: Discovery and First Response and managing the Media. In these phases there is a special role for a facilitator which simulate the media. In a hectic two hours, the facilitators ask the participants to prepare for the final press conference, after which the debriefing starts. The game revolves around a narrative, but also about building a narrative by playing the game.

A fictitious scenario is used in the simulation and has five roles: CEO, CISO, Business Leader, Communication / PR representative and CFO and numerous non-playable characters simulated by facilitators. The facilitators put the participants through events and forces them to make decisions, based on information acquired. The informative system makes gathering of information, the decisions and communications even increasingly interactive.

There is one key design variable that was particularly 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. 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 for example means a loss of control of the use of the information or a loss of control over the speed of the game. Based on the requirements the choice is made towards realism. The following section describes how the proposed game design is perceived by the participants.
Game Evaluation
This section discusses 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:

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.

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.

In conclusion, the simulation game is perceived as useful by participants. Particularly, participants enjoy the challenge in the game created by the interactivity, disruption and flexibility. One of the key elements that increased the realism of the simulation game is the information system. Therefore, the next section focuses on describing this key element.

TECHNOLOGY: The Information System

An absolutely crucial element in the game is the web application provided to the participants. The tool adds complexity, interactivity as well as flexibility to the simulation game which is praised by participants. This application represents several important aspects. The first aspect it represents is a communication tool, similarly to email. Participants use the application to communicate their actions to the facilitators. The second function the information system has is to receive information in the form of messages and news articles, provided by the two facilitators through the tool. As it is a web application, the tool can be accessed from anywhere with any computer, mobile phone or tablet (assuming there is internet).

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.

The game control consists mainly of three sources information, that guide and direct the crisis team to next phases. The first is the media articles, which are stored in a database. The facilitator which plays the media decides when to publish which article. The second is the events and tasks described above, these require participants to make a decision. The facilitator responses with consequences. These responses are included in the event description, provided to facilitators. However, facilitators need to be flexible and creative in providing suitable and realistic responses to actions. The third is information requested by participants, to gain situation awareness as well. These responses are mostly included in the scenarios, that need to be uncovered.

![Figure 2: Information System Views](image)
CONCLUSION and DISCUSSION

In this paper, the outcomes of a design study for a simulation game to prepare senior-managers for cyber crisis are discussed. It answers the question: how to support senior-managers in preparing for cyber crisis decision making by means of crisis simulation games?

The proposed game immerses 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.

There is one key design variable that was particularly 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. 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 for example means a loss of control of the use of the information or a loss of control over the speed of the game. Based on the requirements the choice is made towards realism.

The simulation game is perceived as useful by participants. Particularly, participants enjoy the challenge in the game created by the interactivity, disruption and flexibility. One of the key elements that increased the realism of the simulation game is the information system. The tool adds complexity, interactivity as well as flexibility to the simulation game which is praised by participants.

Based on the evaluation, the following lessons are learned from designing the simulation game:

**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.

**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.

**LIMITATIONS and FUTURE RESEARCH**

This game design is still in development and requires some more testing before finalizing. Three limitations of this research are important to mention:

1. **The effectiveness of the game is untested with the target group.** This game is designed for senior-managers. However, both test sessions did not include members of this group, except for one. Therefore, the usefulness as well as the adjustments of the game elements based on these game elements might be premature and are still up for change.

2. **The Simulation Game is perceived useful, but that’s all known.** It is unknown which concepts from cyber crisis are internalized by the participants during the simulation and due to which game elements or mechanisms as well as there are no models or theories tested or evaluated, nor have their prescriptive models added to explain which approach can be taken. Participants have to trust on their own experience in decision-making, which is chosen as a design. However, the game does have the potential to include different prescriptive models.

3. **The Simulation Game is complex and intense, also for facilitators.** The game is complex due to its interactivity, flexibility and large range of solutions to deal with during crisis. It is its strength, but also its weakness. This requires a lot from the facilitators, requiring both knowledge and creativity to respond to participants in a way that makes sense and does not stall the game by constantly referencing to documents. However, documenting all from the start is nearly impossible. But as the number of game sessions increase, the knowledge increases, which makes it easier for the facilitators to adapt to new situations.

The conceptual framework upon which the game has been build provides interesting opportunities for both future use and research. The designed simulation game can be extended with either different, or more models from reality. Additional game elements as well as scenarios are easily implemented in this framework. By capturing the actions and responses, the database will increase which can be used for either research or used in re-play. The designed game also provides a simulation game which can serve as an experimental tool, in which theories and models are tested, from any type of research field. Finally, the findings as presented in the conclusion, can be used for simulation game designs that resemble cyber crisis situations.

**REFERENCES**


