The Incident Prevention Team
A proactive approach to Information Security

Nishan Marc Pereira
Master's Student
Faculty of Technology, Policy and Management
Delft University of Technology
Email: n.m.pereira@student.tudelft.nl

Jan van den Berg, Wolter Pieters
and Dina Hadziosmanovic
Faculty of Technology, Policy and Management
Delft University of Technology
Email: (J.vandenBerg, W.Pieters, D.Hadziosmanovic)@tudelft.nl

***Abstract*—Information Security Risk Management is gathering significant attention in organisations today. Incident response teams are set up to handle cyber incidents. However, an analysis of the literature and the increasing trends in incidents reported, indicate that these measures are failing to fully achieve their goals. Despite the efforts in Information Security Risk Management, organisations are unable to proactively implement information security control measures based on dynamic information. To address this problem, this research describes the development of an Incident Prevention Team. The team actively scans for information about threats and vulnerabilities affecting external organisations and then using this information to proactively address its risk. The implementation of this Incident Prevention Team will enable organisations to transform their incident response process from being reactive to also proactive.**

***Index Terms*—Information Security, Risk Assessment, Incident Response, Incident Prevention.**

I. Introduction

There is an increasing trend of cyber incidents [1], [2]; and cyber attacks are more frequent, varied and mobile [3]. This is attributed to the diversity of security threats and dynamic changes to information security environment [4]. However, practice shows that not all incidents can be clearly characterised with the two features of diversity of security threats and dynamic changes to information security environment. For example, data breaches at two large-scale retailers (Target and Home Depot) had an estimated impact of loss of more than 100 Million Credit card details and 70 million customer personal information [5]. The incidents themselves occurred months apart and affected the same point-of-sale system in these companies. Despite the information of the previous incident at Target, Home Deport failed to adequately protect itself. Therefore, the example highlights the question if the scale of the attack could have been decreased if Home Deport had processed the information on recent incidents with more urgency. A quick scan of recent cyber incidents, also reveals similarities in types of threats impacting other organisations [6].

The NIST risk management guide for information technology systems [7] and NIST computer security incident handling guide [8] describes the process how organisations manage risks and incidents. Organisations manage incidents, but in a reactive way [9]. The computer security incident response team (CSIRT) performs the function of preparation for, identification, containment, eradication and recovery from incidents. We argue that the current views on incident response in organisations are not sufficient because the information on threats and vulnerabilities was available before the incident itself. This raises the question, why the organisation was not able to proactively address Information Security risk based on information already available. We argue that there is a need to also focus on incident prevention along with incident response practiced today.

For the preceding reasons this paper explores the design of a proactive approach to incident response that affects the overall organisational security function. The main goal of this paper is to introduce the design of an Incident Prevention Team that provides clear guidance for organisations in developing a proactive cyber incident prevention process. We structure the research using the design science cycle as described by Kuechler & Vaishnavi [10]. This methodology allows for research through design and is the art of learning through the act of building. To do so, in section II, the gaps in the current state in risk assessment and incident response is identified that influences the way organisations focus on incident management. The analysis is done by using TIP design perspectives [11]. In section III, precursors are identified as a key ingredient of incident information. In addition, the characteristic elements of incident information is identified, in order to create a process to interpret incident information. In section IV, we combine these elements to design an incident prevention team and the incident prevention process, which is finally evaluated in section V. Conclusions are drawn in section VI.

II. State-of-the-art

The theoretical basis of this research evolved as a result of both the understanding gained through the practical inputs from security experts and from studying the Information Security literature and looking for an appropriate theory. An approach to analyse and design a solution in socio-technical systems is by using TIP design [11]. TIP design describes three perspectives of Technical, Institutional and decision Process aspects. Technical and institutional artifacts enable the management of Information Security to be carried out by different processes, and is described in detail in this section.

A. Technical Perspective

The technical artifacts are the various risk assessment tools available [12]. These tools are developed based on the Information Security Risk Management (ISRM) process [7]. The main steps are identifying risk, assessing risk and taking steps to reduce risk to an acceptable level. Organisations need to make trade-offs from the perspective of financial, resource utilisation, compatibility, etc. to implement these tools [13], therefore the benefits of the process is not fully achieved.

The incident response team also uses a variety of incident response tools to carry out the activities during the incident response lifecycle. In the preparation phase the technical artifacts are incident handler enabling technologies and tools to detect and prevent known threats. In the detection and analysis phase, there is a variety of sophisticated Network Intrusion Detection Systems, anti-spam and anti-malware software, security information and event management tools, etc. [8]. Each tool performs a specific sub-function in the process of incident response after the detection of the incident.

The incident response team (IRT) retrieves information shared about incidents but, even after this, IRTs fail to react to information [14]. This is because the focus of IRTs is on incident response and its contribution to incident prevention is to provide advice [8]. It provides recommendations on practices for securing networks, systems, and applications; risk assessments; and user awareness and training. However, the access, retrieval and interpretation of information are important aspects of incident response.

Indicators and precursors are used as a sign to detect incidents [8], [15]. Precursors are relatively rare, while indicators are easier to detect [8]. The partial or lack of complete information is a major hurdle that the incident response team faces. Sophisticated incident detection and assessment tools are available in the market to interpret the information. Nevertheless, threats and vulnerabilities continue to be undetected in many cases because only indicators are used as the source of information in the detection and analysis phase; thereby creating the requirement of "the use of precursors as information sources" to strengthen the process of incident response.

Furthermore, information that does not necessarily affect the organisation directly, still needs to be investigated and monitored for potential risk. Cyber incident information is shared using Cyber Security Reporting System [16]. The final phase of the incident response lifecycle focuses on reporting of information and is part of the continuous feedback loop in organisations. This acts both as a retrospective measure internally and as a predictive measure to other organisations if the information is shared externally. Therefore, "using the information from external organisations" can strengthen the process of incident prevention.

B. Institutional Perspective

In order to assess the current institutional setting of the Risk Management and Incident Response Process, the four layer institutional model by Williamson (1998) is selected [17]. The model gives an overview of social and institutional arrangement in an integrated fashion. This framework allows for liberty in the analysis of separate layers. Each level operates at its own pace, protected from above by slower, larger levels but invigorated from below by faster, smaller cycles. Thus a multi-layer system can be described that shows both bottom-up and top-down causation [18].

Level 1, describes the actors and their interactions in socio-technological setting [18]. There are various actors directly and indirectly involved in risk assessment and incident response [19], [20], [21]. The actors interact with complex information systems in cyberspace[1]. IRT's carry out the function of ensuring information security by following the various steps as described in the incident response guide; while the management is responsible for ensuring that risk management activities of assessment and control is carried out appropriately [7]. The interactions of these actors is guided by these processes since incidents create an uncertain environment in which decisions have to be taken.

Level 2, describes the formal and informal institutional arrangements of these socio-technological systems. This includes covenants and contracts, but also informal rules, codes and norms [18]. The National Institute of Standards and Technology (NIST) published the Computer Security Incident Handling Guide [8], describing the process followed by Incident Response Teams while the Risk Management Guide for Information Technology Systems [7], describes the risk management process. Each step of the Risk Management and Incident Response process helps the organisation to achieve compliance to standards described in Level 3. Therefore the compliance helps to promote customers trust by verifying the fulfillment of well-known and accepted international standard [23]. Furthermore, industry specific security checklists, for example, Checklist security of ICS/SCADA systems [24], also is used. The technical artifacts described in Section II-A are implemented by 3rd party security vendors based on the service level agreement and contract agreed by both stakeholders.

Level 3, describes the formal institutional environment; the formal rules, laws and regulations [18]. The ISO/IEC 27000, 27001 and 27002 are information security standards for the protection of the information and information systems [25]. ISO 27005:2011 standard is an information security risk management standard [26], while ISO 27035:2011 standard is an Information security incident management standard widely adopted in organisations [27]. The standards specify a security baseline that the organisation should achieve and offers guidelines in achieving it. Furthermore, strategies like *National Cyber Security Strategy 2* of the Netherlands [28], Articles

[1] *Cyberspace is defined as "the complex environment resulting from the interaction of people, software and services on the Internet by means of technology devices and networks connected to it, which does not exist in any physical form"* [22]

30, 31 and 32 of the Data Protection regulation from the European Union [29], etc. show that cyber security is gaining prominence internationally in both public and private sector. Therefore, this indicates that at an institutional level these formal rules, laws and regulations contributes to the awareness of information security in organisations today.

Level 4, describes the informal institutional environment, these are the norms, values, orientation and codes [18]. Information security is not yet at the forefront of priorities in organisations. It lacks the full support of top management [25], [30]. The organisational culture has a large part to play here [31]; thereby the norm of organisation wide proactive information security awareness has to still develop. This can be compared with the culture of safety in organisations, which has significantly "more support from the top management" [32]. Furthermore, the management focuses on the importance of an incident recovery plan in the event of a security breach [33]. If a high-impact security breach affects the organisation, the seriousness of its security control measures is brought to the forefront of organisational priorities.

The four layer institutional model by Williamson (1998) also explains the relationships between the various layers [18]. Even though, Incident Response teams described in Level 1 uses the various Information Security tools described in Level 2, which are implement to be complaint to Information Security standards described in Level 3, it is selected based on trade-offs between constraints and requirements of the organisation. Organisations are limited by labour, financial, expertise, and other resources necessary to implement such comprehensive tools based on these standards [13], [34]. The decision is influenced by the norm that Information Security risk is not likely to affect them and hence not a priority described in Level 4. Therefore, the culture of "proactive Information Security awareness" has to be fostered through the process in order to notice changes across all institutional levels.

C. Process Perspective

The function of achieving information security is effectively accomplished, when the Risk Management team performs the Risk Management process [7] and the Incident Response team makes use of the process described in the Incident Response lifecycle [8]. Therefore, the technical and institutional artifacts described earlier are structures when implemented together with a context, produce the process that performs the intended function of the artifacts [11].

The output of the risk assessment and incident response process is to reduce risk in the organisation. The risk level determines the extent to which organisations are willing to absorb risk; thereby determining risk control measures [7]. However, we see that the control measures adopted are backward-looking; because of the focus towards incident response. Often, these controls measures fail because of the following two aspects.

Lack of implementation: Information security controls are not implemented because the perceived benefit of information security does not justify the high cost of implementation [35]. The investment in right controls is not for the information sets with the highest vulnerability but for information sets with midrange vulnerabilities [36]. With trade offs being made, organisations run the risk of not having invested in the right security controls.

At times, implementation of controls measures is postponed until it is too late [25]. This indicates that information security is not a top priority, because it lacks the full support of top management [25]. However, we see that both private and public organisations, and even individuals are equally susceptible to cyber incidents, therefore, the requirement of "top management support" is further advocated.

Failure in implementation: The complexity in information systems means that controls have to be implemented correctly or else failure leads to a less secure system, thereby increasing risk to frequent and damaging security breaches [37]. This is a process failure and has to be addressed by the management.

Even in the presence of controls, information systems are not fully protected because of inherent control weaknesses [38]. Therefore, the incident response process is crucial to ensuring that organisations manage these risk. Organisations respond to incidents by tightening security controls [39]. The tightening of security controls does not indicate greater security, because, once a resource is successfully attacked, there is a high probability of a similar resource being attacked again [8]. Therefore we can conclude that if this information is available to organisations, they can proactively use the information to update its security controls and change its risk posture. However even with various information sharing mechanism in place [14], the control measures are not adapted to the risk. There is lack of appropriate implementation strategies [40], which is creating the need for "a forward-looking process".

To achieve the overall function of risk assessment and incident response, there are many sub-processes each contributing to achieving the function of each activity in the process. However, achieving the objectives of each function is not easy, because even with the adoption of the risk management perspective it does not drive the level of security risk to zero [41]. Residual risk still exists, regardless of the action taken [42], thereby, creating an opportunity for attackers to target the organisation. Therefore, organisations have to be vigilant to any information regarding its information security status. However, the risk assessment process consumes time and resources in the organisation where it is implemented [43]. Therefore, there should be "flexibility in the process" designed to ensure that the risk assessment is performed only on the information systems that are affected.

The incident response life cycle offers a structured process for IRT to respond to incidents. This means that Incident Response is initiated only after an incident is detected. The prevention process in the preparation phase of lifecycle fails to prevent incidents even with prior information available. Both the technical and institutional artifacts only prepare the organisation for maintaining a minimum level of security.

However, there is no process to proactively prevent incidents. Therefore, with "the design of a proactive incident prevention process" we can change the perspective of how organisations view information, thereby improving its information security awareness.

D. Stakeholders

A stakeholder analysis is a crucial step in the design of any process. Cyber incidents involve various internal and external stakeholders. These actors and their interactions create a challenging environment that has to be considered because each stakeholder interacts in their own unique way with the information systems. Organisations manage incidents with the help Incident Response Teams, which perform specific functions [44]. Based on the structure, size, geographical distribution, complexity of IT operations and connection with the location of the organisation key information systems can play a role in the selection of the team [19]. Killcrece, et al, (2003) describes 5 models of IRTs [19], which shows that the requirements for IRTs are diverse.

This analysis of requirements identifies that the skills and expertise of the members of the IRT are crucial to the team's success. Furthermore, there is a high demand for very detailed knowledge about the IT security domain and the actual company environment [45]. Ahmad, et al (2012) describes the various actors involved in incident response [9]. The IRTs consist of internal stakeholders who include team leaders, technical experts and process experts. Other internal stakeholders include legal experts, communication advisors, end-users, etc External stakeholders include both technical and process experts from outside the organisation. Furthermore, the media, customers, supply chain vendors, etc. are external stakeholders. The attacker also is considered as an external stakeholder [46].

We see that the design and set up of IRTs are comprehensive and detailed, because it is the first line of defence when an incident occurs [47]. Therefore even with limited resources and capabilities, there is still a response mechanism in place in organisations. The more advanced computer security IRTs tend to adopt a proactive role, seeking out vulnerabilities before they become incidents [20]. They provide advice and educate employees on information security matters [19]. Therefore, in this research, "critical stakeholders should be identified from IRTs" in order to engage them to collaborate for the prevention of incidents.

III. Design Ingredients

To improve the current state of information security described in Section II, this research focuses on information not detected in the organisation but is still available in the form of precursors. This helps to bridge the gap in incident prevention. The challenge of this research is to differentiate incident information, i.e., precursors and indicators, and is described in this section. This is followed by introducing the elements of incident information (*Trigger, Template & Twitch*) from Vigilant Information Systems [48], to create a shared understanding of information for information security teams decision-making process. In this research, we further extend the elements, by introducing the concept of *Tweak*, to describe the action taken on interpreting the information.

A. Precursors

The NIST publication, Computer Security Incident Handling Guide, classifies incidents based on the time the incident is detected in the organisation [8]. Indicators are a sign that an incident may have occurred or may be occurring now and precursor is a sign that an incident may occur in the future. In this research, we make the distinction in the classification of incident information by depicting the warning phase of the incident lifecycle [49] as illustrated in Figure 1. The generic incident notification timeline using this lifecycle, also start once the security incident or "indicator" is confirmed and recorded in the system [46]. This is the time between the detection of the incident and the start of the risk assessment process. Therefore, the time between receiving information and detecting the incident is used to define information as a "precursor".

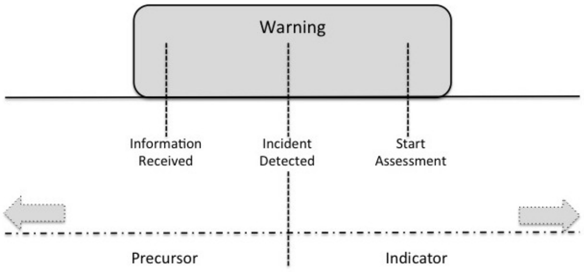

Fig. 1. Classification of information, derived from [46]

In this research, we focus on precursors. It is the security state of the system before the occurrence of the incident [50]. Precursors can include a variety of information. However, we focus on information about threats and vulnerabilities that have a negative impact on an external organisation with similar information systems.

Attackers Perspective: Precursors viewed from the attackers' perspective are described as threats. Organisations struggle to assess threats accurately, because the motivation of the attacker is unknown. Organisations are ill equipped to protect itself from a highly motivated attacker. With a wide range of combinations of attack possible, the motivation of attackers is beyond the scope of the organisation's information security management practise. However, using the information already available, it offers a field-tested analysis of threat that affected an organisation, thereby, value is derived from this information.

Targets Perspective: Precursors from the target organisations point of view are vulnerabilities in their IT environment. Vulnerabilities inherently exist in every organisation [38]. However, information on vulnerabilities in information systems is readily available both internally though alerts, intrusion detection systems, etc, and externally from information sharing networks.

Therefore, using this information organisations can preempt an incident from occurring by altering their information systems security control measures according to risk assessment. To achieve this, an active scanning of the environment is required as part of the process to prevent incidents.

B. Triggers

Trigger is defined as the stimuli that when interacting with the template may cause a shift in the template [48], [51]. By definition, any event influencing the security baseline is termed as a trigger. These events are both positive and negative. In this research, we focus on precursors as triggers since it works as an early warning system to the organisation. El Sawy, et al., (1988) describes the characteristics of trigger [51], however, these characteristics are not restricted to those specified and can be modified based on inputs from industry experts.

Source: The trigger source is from where the information comes. Precursors are obtained by active scanning of the environment. This environmental scanning can help supplement and guide the decision-making process. However not all information are considered as trust worthy precursors. Attackers are known to use social engineering to spread false information and gain access to organisations. Therefore, the trustworthiness of the data source is crucial since it helps the organisation to prioritise the information received from this source.

Information: The trigger information is a narrative description of the information that the trigger conveys. Every organisation has different information systems depending on its business requirements. Therefore, the relevant information related to organisation's information systems are important characteristics of the information to be assessed in triggers. This is because confidence in decision-making increases with the availability of relevant information. Moreover, the completeness and accuracy of information is crucial towards sound decision making. Another important factor is the consistency of the information across the various sources.

Latency: The latency is defined as the time from the notification of incident to the organisation reacting to it. The time allowed for the threat to affect the organisation is a lost opportunity in incident prevention. This information can define a critical factor in determining the effectiveness of the Incident Prevention Team's proactive approach to incident scanning.

C. Template

The template is the frame of reference through which organisational processes are described [48], [51]. In this research, we use the template to describe the security baseline from risk maturity levels of the organisation. It also maps out information system architecture details and the interaction of various elements in the information system environment. These help to identify what organisations consider as key information systems. There are various characteristics of the information captured in the template. El Sawy, et al., (1988) describes the characteristics of information captured in the template [51]. We use this as a starting point to describe the template, however, these characteristics are not restricted to those specified and can be modified based on inputs from industry experts. The characteristics of theme, construct and framework best describe the template.

Theme: This describes the overarching goals and objectives of organisations. This is high-level goal describing the unifying idea describing the processes in organisations.

Construct: Constructs help to determine the relative positioning of the security maturity levels of the current state of the system as well as the future state. This is measured on a qualitative scale enabling ease of decision-making.

Framework: The organisation has a variety of information systems interconnected in cyber space. These information systems are used to achieve the business goals. Therefore, the framework describes the process, the interconnections and various control mechanisms that exist.

D. Twitch

The twitch is defined as the result of the trigger influencing the template by causing a change in the template [48], [51]. This change in the template adversely affects information security environment in the organisation. The identification of the twitch is an important element, because it identifies the root cause of the problem in the organisation. El Sawy, et al., (1988) describes the characteristics of twitches having both causes and effects [51] and is therefore more informative than the template itself. We use this as a starting point to describe the twitch, however, these characteristics are not restricted to those specified and can be modified based on inputs from industry experts.

Descriptor: Twitch descriptors are used to describe the nature of the twitch. This is the effect it has on the template. There are both direct and indirect affects of the twitch in the information system.

Magnitude: The twitch magnitude is a quantitative measure describing the effect of the twitch. It is defined as the relative aggregate modification in a template due to a cumulative trigger effect in a chosen period of elapsed time.

Driver: The twitch drivers are causes that can influence the template to twitch. We see that the most significant driver is the root cause of the problem. Moreover, organisations have to generate a detailed assessment of risk to identify the underlying root cause to be controlled. Threats are external influences but these, in combination with internal vulnerabilities, create risk to the organisation.

E. Tweak

We will now extend the concept of Vigilant Information Systems with Tweak. We use Tweak to describe the action taken after interpreting the information because this information about incidents is incomplete without referring to the action taken during cyber incidents. There are various means to negate the effect of the twitch. Organisations can either remove the cause of the twitch or modify the template to reflect the twitch to maintain a stable risk posture. In an uncertain threat environment organisations need to make decisions. With the limited influence, that organisations have on the threat, the modification of template is recommended. Using precursors, the tweak is a proactive control mechanism. The nature of action are outcomes to counter the twitch in templates, therefore the framework for In-context Information System research by Braa & Vidgen (1999) is used [52].

Change: Change is described as an intervention action to the template. These are short term or long-term actions depending on the strategy adopted. This measure usually includes a change in controls to compensate for vulnerabilities or a correction in the vulnerabilities to maintain the risk level.

Prediction: Prediction is described as a positivist approach. This is a reduction mechanism to prepare for a potential risk in the organisation, thereby, adapting the controls.

Understanding: Understanding is described as an interpreter approach. This helps in promoting a shared understanding of knowledge. Here, the lessons learned from risk analysis and control identification is used to improve the overall information security awareness.

IV. Development of Incident Prevention Team

The ingredients described in Section III are essential components that contribute towards establishing an Incident Prevention Team (IPT) in organisations. A high-level incident prevention process, shown in Figure 2, is used to illustrate the incident prevention process.

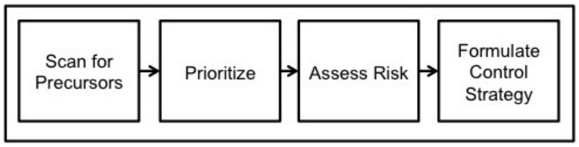

Fig. 2. High Level Incident Prevention Process

This section describes each step of the process, by giving the input, activities performed in each step and output of the process. Questions that can be used by the IPT to perform its function is also described in each step of the process. For easier reference, every questions is assigned a Roman Numeral, starting with (I) and ending with a (XI).

Step 1: Scan for Precursors

The Figure 3, *Scan for Precursors*, represents the first step in the incident prevention process. In this step, the IPT actively scans the environment for precursors.

The input for this activity is the knowledge of the information system and information security environment in the organisation. This knowledge is to help the IPT have a baseline understanding of the organisation's information systems. The activities that the IPT performs in this step include the scanning for threats and vulnerabilities and the monitoring of incidents affecting other organisations. This activity is a key characteristic feature of the incident prevention process because it is forward looking. The IPT should attempt to retrieve complete, accurate and reliable information.

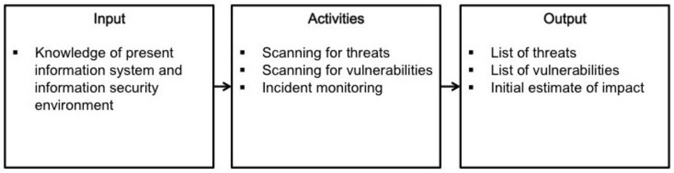
Input
▪ Knowledge of present information system and information security environment
Activities
▪ Scanning for threats
▪ Scanning for vulnerabilities
▪ Incident monitoring
Output
▪ List of threats
▪ List of vulnerabilities
▪ Initial estimate of impact

Fig. 3. Step 1, Scan for Precursors

The IPT can effectively and efficiently gather precursors from trustworthy information sources. The IPT defines trustworthy information sources as those sources from which there is value derived from the information available. Here, the IPTs understanding of the organisation's information system and its experience as incident handlers, will strengthen the identification and interpretation of precursors. The outcome of this process is a preliminary list of threats and vulnerabilities considered as precursors. The IPT also makes an initial estimate of impact of the incident.

The information retrieved is now categorised as triggers. The source, information itself and latency are the characteristic elements of triggers, used to operationalise this incident prevention process. These characteristic elements are used because precursors by itself are raw data. The shared understanding of the information in context with information security requirements will add value to the information, triggering the next step of the process.

The following generic questions are asked by the IPT when scanning for precursors. These questions serve as stimuli towards generating triggers to assess the current information security environment in the organisation.

I Does the information come from a trustworthy data source?

II Is the information complete, accurate and reliable?

III Is the information relevant to the present organisations system, process or people?

IV Is the information consistent?

V How long has the information been available?

Step 2: Prioritise

The Figure 4, *Prioritise*, represents the next step in the incident prevention process. The list of triggers identified is prioritised in this step by the IPT.

The input to this step is derived from the output of the previous step, i.e. list of triggers. Furthermore, information

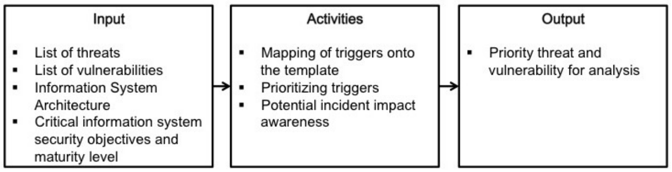
Input
▪ List of threats
▪ List of vulnerabilities
▪ Information System Architecture
▪ Critical information system security objectives and maturity level
Activities
▪ Mapping of triggers onto the template
▪ Prioritizing triggers
▪ Potential incident impact awareness
Output
▪ Priority threat and vulnerability for analysis

Fig. 4. Step 2, Prioritise

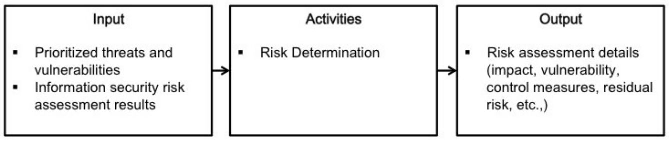
Input
▪ Prioritized threats and vulnerabilities
▪ Information security risk assessment results
Activities
▪ Risk Determination
Output
▪ Risk assessment details (impact, vulnerability, control measures, residual risk, etc.,)

Fig. 5. Step 3, Assess Risk

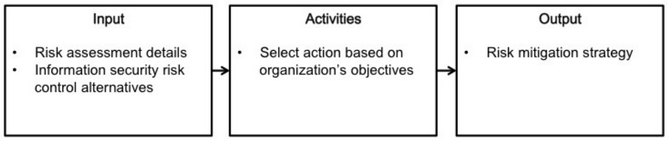
Input
• Risk assessment details
• Information security risk control alternatives
Activities
• Select action based on organization's objectives
Output
• Risk mitigation strategy

Fig. 6. Step 4, Formulate Control Strategies

about the information system, described using a template is also used as input. Input to the template is obtained from the most recent risk assessment activity as well as lessons captured from post incident phase of the incident response lifecycle. These inputs are used because it comprehensively describes the security baseline of the organisation.

The activities performed by the IPT in this step of the process are as follows. The IPT maps the trigger onto the template. For example, vulnerability in the list of triggers is mapped onto the organisation's information system to assess the potential impact a threat might have on that information system. The trigger with the highest impact is prioritised by the IPT. Here, the IPT needs consensus on the impact of triggers on the business objectives of the organisation. By having consensus it establishes the priorities for risk assessment in the next step. Therefore, the outcome is a list of priority triggers made up of information on threats and vulnerabilities, agreed by the IPT.

In this step, the IPT focuses on comparing the information from triggers and templates. This step is useful since it is a high level prioritisation performed by the IPT. It is high-level process because there are large volumes of information that the IPT has to process and a risk assessment of all triggers is not feasible. There has to be a filter to segregate information. Therefore, in this step the team identifies triggers that it considers a priority. The operational questions to determine this priority are enumerated below.

VI Does the Incident Prevention Team have consensus on the priority?

VII Can the Incident Prevention Team justify why the other triggers are not considered as a priority?

Step 3: Assess Risk

The Figure 5, *Assess Risk*, represents the next step in the incident prevention process. The IPT determines the risk in this step of the incident prevention process.

The input to this activity is the prioritised list of threats and vulnerabilities determined in the previous step. Additionally information security risk assessment results from earlier risk assessments are used to compare the change to information security status.

In this step, the IPT carries out a risk assessment. In the risk assessment process, the vulnerable information systems are evaluated on the information security principles of confidentiality, integrity and availability. This step is a reiteration of the Information Security Risk Management (ISRM) process within the organisation.

The IPT determines the level of abstraction required for this risk analysis because it is not feasible to perform a complete risk assessment. The IPT focuses on assessing information security risk of only the information system likely to be affected. It does not require all the resources used in traditional ISRM processes. Therefore, it is an agile incident prevention process.

Therefore, the output is a detailed risk assessment of the information system affected. These details include the vulnerabilities in the information system identified, the control measures associated, the potential impact of the risk, residual risk from the threat, etc.

In this step, the IPT focuses on the twitch in template caused by triggers. The assessment of the risk posture identifies the magnitude (impact) and drivers (vulnerabilities) of the twitch. These details are useful towards understanding the complexity in information systems and the risk associated with them. Therefore, organisations move from compliance based risk assessment to awareness based risk assessment. The operational questions that the IPT can ask in this step of the process are enumerated below.

VIII Is there a likelihood of threat?

IX Is there a vulnerability in the information system?

X What is the potential impact of risk in the organisation?

Step 4: Formulate Control Strategy

The final step of the incident prevention process is depicted in Figure 6, *Formulate Control Strategies*. The IPT formulates control strategies in this step of the process.

The input to this activity is the detailed risk assessment information from the previous step and a list of Information Security control measures. If the trigger indicated a twitch in status quo of the template, remedial action should be taken to return the template to a stable risk posture. The IPT along with the management can determine the appropriate control strategies based on the organisation's risk appetite. Therefore, the output of this step is a risk mitigation strategy to address the risk in the organisation.

The failures in information security are due to ineffective implementation of controls measures, resulting in significant risk to the organisation. Therefore, this activity is needed to integrate the lessons learned from the risk assessment process with the implementation of information security controls in the organisation by formulating effective control strategies. This step is crucial to incident prevention, because, it determines the organisation's ability to react to information security risk. An agile process will transform the organisation, enabling it to adapt to changing security conditions, thereby making it more adaptive. The operational questions asked by the IPT are enumerated below.

XI Is there a mechanism to implement the control strategy determined? If not, how can the IPT help implement the control strategy?

It is important to note that the IPT is not responsible for implementing information security controls. There are mechanisms in place that address this in the organisation. However the IPT can assist in the implementation of control strategies should the need arise.

V. Evaluation

The proposed incident prevention team has been been validated, firstly by defining two cyber security incident scenarios followed by the evaluation with a security expert. Due to space limitations in describing the entire evaluation process here, we only sketch some highlights related to this. The aim of the scenarios, was to check the feasibility of the proposed design in a real world setting and understand in detail how the process of incident prevention works. The discussed incident scenarios made clear how the incident prevention team addresses information retrieved about threats and vulnerabilities in external organisations and uses it to proactively adapt its own security posture. The analysis reveals that, scanning for precursors and its prioritising depends on the knowledge and experience of the people in the incident prevention team. However, the process enables the organisation to look at information that was previously not considered, thereby, creating an awareness of the Information Security environment beyond its information system boundaries. For more details on this validation step, we refer to [53].

The next validation was done by an interview with a security expert. This helped us understand what advantages and difficulties can be associated with the implementation of an incident prevention team in the company. The major concern, presented was the interpretation of information by the IPT, because the questions asked related to cyber intelligence which is a very big challenge faced by organisations today. This again, depends on the skills and experience of the incident prevention team. However, the team can be easily adopted, because of its flexibility, and reuse of information security elements in the organisation. Furthermore, the value of the incident prevention team, was described both as an operational team in an organisation proactively addressing information security risk as well as a third party service offering by security companies to other companies. For more details on this validation step, we refer to [53].

VI. Conclusion

In this paper, we started by identifying the gaps in risk assessment and incident response using the Technical, Institutional and decision Process perspectives. This was further combined with the design ingredients of precursors as a means to differentiate incident information, with trigger, template, twitch and tweak used to interpret the information. Based on these ingredients, we designed an Incident Prevention Team. This was presented in Section IV.

The Incident Prevention Team in a nutshell is a proactive approach to manage Information Security by using precursors (information on threats and vulnerabilities already available) affecting external organisations with similar information systems, and evaluating the potential risk to the organisation, thereby determining the risk control strategies. By providing a clear step-by-step process with the questions to be asked by the IPT, the proposed process encourages the company to change its perspective of incident response from a backward-looking approach to a more forward looking approach.

The proposed incident prevention team addresses a different perspective of Information Security not presented in the current information security research. The majority of studies focuses on establishing teams that react after the incident occurs. Using the incident prevention process, the IPT will be able to adapt the security controls in the organisation proactively. Even the preventive measures based on risk assessment, is not proactively used; therefore the process followed by the IPT combines technical and organisational processes to address security requirements at an organisational level. Moreover, the use of the concepts of trigger, template, twitch and tweak to interpret information will help to create a shared understanding of information, and thus benefiting the society as a whole.

The limitations (and hence opportunity for further research) is the lack of empirical testing of the proposed Incident Prevention Team. Furthermore, this research was not designed with a specific organisation's business requirements. Input from information security experts in the field was used, but this means that some amount of bias does exists in the research findings. The design of the proposed team and its process was generalised to allow for the designs adoption in any organisation. However, this research, introduces a different perspective in information security through incident prevention. With limited IS literature addressing this aspect of information security, this research offers scope for further research into Incident Prevention Teams.

Acknowledgment

We would like to acknowledge the following people for their contributions to this research. Marcel Hoeke (from Atos Consulting) and Jacques Tuin (Politie, Landelijke Eenheid) for their advice and critical input on the subject, which added a practical aspect to this research. Dr. M. E. Warnier (from Faculty of Technology, Policy and Management, Delft University of Technology) for his feedback during the research.

References

[1] L. Marinos, "Threat landscape 2013, overview of current and emerging cyber-threats," tech. rep., ENISA, 2013.

[2] P. Wood, "Internet security," Tech. Rep. 19, Symantec Corporation, 2014.

[3] S. Caponi, "Cybersecurity trends for 2014." [Online], Retrieved on 1st October, 2014, Available: http://www.corporatecomplianceinsights.com/cybersecurity-trends-for-2014/, 2014.

[4] J. Ma, C. Wang, and Z. Ma, “Adaptive security policy,” in *Security Access in Wireless Local Area Networks*, pp. 295–329, Springer, 2009.

[5] N. Bose, “Home depot confirms security breach following target data theft.” [Online], Retrieved on 10th Sep, 2014, Available: http://www.reuters.com/article/2014/09/09/us-usa-home-depot-databreach-idUSKBN0H327E20140909., 2014.

[6] Verizon, “2014 data breach investigations report,” tech. rep., Verizon Enterprise, 2014.

[7] G. Stoneburner, A. Goguen, and A. Feringa, “Risk management guide for information technology systems,” *NIST Special Publication*, vol. 800, no. 30, pp. 800–30, 2002.

[8] P. Cichonski, T. Millar, T. Grance, and K. Scarfone, “Computer security incident handling guide,” *NIST Special Publication*, vol. 800, p. 61, 2012.

[9] A. Ahmad, J. Hadgkiss, and A. B. Ruighaver, “Incident response teams - challenges in supporting the organisational security function,” *Computers & Security*, vol. 31, no. 5, pp. 643–652, 2012.

[10] B. Kuechler and V. Vaishnavi, “On theory development in design science research: anatomy of a research project,” *European Journal of Information Systems*, vol. 17, no. 5, pp. 489–504, 2008.

[11] P. W. Bots and C. E. van Daalen, “Designing socio-technical systems: Structures and processes,” in *proceedings of Third International Engineering Systems Symposium*, 2012.

[12] D. Ionita, “Current established risk assessment methodologies and tools,” Master’s thesis, Universiteit Twente, 2013.

[13] W. Al-Ahmad and B. Mohammad, “Addressing information security risks by adopting standards,” *International Journal of Information Security Science*, vol. 2, no. 2, pp. 28–43, 2013.

[14] G. B. White and D. J. DiCenso, “Information sharing needs for national security,” in *in proceedings of 38th Annual Hawaii International Conference on System Sciences, HICSS’05.*, pp. 125c–125c, IEEE, 2005.

[15] B. R. Pandey, “Indicators for ict security incident management,” Master’s thesis, Norwegian University of Science and Technology, 2013.

[16] J. J. Gonzalez, “Towards a cyber security reporting system–a quality improvement process,” in *Computer Safety, Reliability, and Security*, pp. 368–380, Springer, 2005.

[17] O. E. Williamson, “Transaction cost economics: how it works; where it is headed,” *De economist*, vol. 146, no. 1, pp. 23–58, 1998.

[18] J. Koppenjan and J. Groenewegen, “Institutional design for complex technological systems,” *International Journal of Technology, Policy and Management*, vol. 5, no. 3, pp. 240–257, 2005.

[19] G. Killcrece, K.-P. Kossakowski, R. Ruefle, and M. Zajicek, “Organizational models for computer security incident response teams (csirts),” tech. rep., DTIC Document, 2003.

[20] D. Smith, “Forming an incident response team,” in *Proceedings of the FIRST Annual Conference*, 1994.

[21] E. E. Schultz Jr, D. S. Brown, and T. A. Longstaff, “Responding to computer security incidents: Guidelines for incident handling,” tech. rep., Lawrence Livermore National Lab., CA (USA), 1990.

[22] ISO/IEC27032:2012, “Information technology - security techniques - guidelines for cybersecurity,” Geneva, Switzerland, 2012.

[23] G. Disterer, “Iso/iec 27000, 27001 and 27002 for information security management,” *Journal of Information Security*, vol. 4, p. 92, 2013.

[24] N. C. S. Centre, “Checklist security of ics/scada systems,” 2012.

[25] E. Humphreys, “Information security management standards: Compliance, governance and risk management,” *information security*, vol. 13, no. 4, pp. 247–255, 2008.

[26] ISO/IEC27005:2011, “Information technology - security techniques - information security risk management,” Geneva, Switzerland, 2011.

[27] ISO/IEC27035:2011, “Information technology - security techniques - information security incident management,” Geneva, Switzerland, 2011.

[28] N. C. for Security and Counterterrorism, “National cyber security strategy 2, from awareness to capability,” 2013.

[29] Y. Poullet, “Eu data protection policy. the directive 95/46/ec: Ten years after,” *Computer Law &amp; Security Review*, vol. 22, no. 3, pp. 206–217, 2006.

[30] S. Posthumus and R. Von Solms, “A framework for the governance of information security,” *Computers &amp; Security*, vol. 23, no. 8, pp. 638–646, 2004.

[31] D. Ashenden, “Information security management: A human challenge?,” *Information Security Technical Report*, vol. 13, no. 4, pp. 195–201, 2008.

[32] A. Hopkins, “Studying organisational cultures and their effects on safety,” *Safety Science*, vol. 44, no. 10, pp. 875–889, 2006.

[33] S. Mitropoulos, D. Patsos, and C. Douligeris, “On incident handling and response: A state-of-the-art approach,” *Computers & Security*, vol. 25, no. 5, pp. 351–370, 2006.

[34] S. L. Barton and P. J. Gordon, “Corporate strategy and capital structure,” *Strategic management journal*, vol. 9, no. 6, pp. 623–632, 1988.

[35] C. D. Ittner and D. F. Larcker, “Coming up short on nonfinancial performance measurement,” *Harvard business review*, vol. 81, no. 11, pp. 88–95, 2003.

[36] L. A. Gordon and M. P. Loeb, “The economics of information security investment,” *ACM Transactions on Information and System Security (TISSEC)*, vol. 5, no. 4, pp. 438–457, 2002.

[37] J. Eloff and M. Eloff, “Information security architecture,” *Computer Fraud &amp; Security*, vol. 2005, no. 11, pp. 10–16, 2005.

[38] N. Feng and M. Li, “An information systems security risk assessment model under uncertain environment,” *Applied Soft Computing*, vol. 11, no. 7, pp. 4332–4340, 2011.

[39] G. V. Post and A. Kagan, “Evaluating information security tradeoffs: Restricting access can interfere with user tasks,” *Computers & Security*, vol. 26, no. 3, pp. 229–237, 2007.

[40] W. H. Baker and L. Wallace, “Is information security under control?: Investigating quality in information security management,” *Security &amp; Privacy, IEEE*, vol. 5, no. 1, pp. 36–44, 2007.

[41] A. G. Kotulic and J. G. Clark, “Why there aren’t more information security research studies,” *Information & Management*, vol. 41, no. 5, pp. 597–607, 2004.

[42] D. B. Parker, “Risks of risk-based security,” *Communications of the ACM*, vol. 50, no. 3, p. 120, 2007.

[43] C. Pak and J. Cannady, “Asset priority risk assessment using hidden markov models,” in *Proceedings of the 10th ACM conference on SIG-information technology education*, pp. 65–73, ACM, 2009.

[44] K. P. Kossakowski, J. Allen, C. Alberts, C. Cohen, and G. Ford, “Responding to intrusions,” tech. rep., DTIC Document, 1999.

[45] A. Ekelhart, S. Fenz, and T. Neubauer, “Ontology-based decision support for information security risk management,” in *proceedings of Fourth International Conf. on Systems*, pp. 80–85, IEEE, 2009.

[46] O. Kulikova, R. Heil, J. van den Berg, and W. Pieters, “Cyber crisis management: A decision-support framework for disclosing security incident information,” in *proceedings of 2012 International Conference on Cyber Security*, pp. 103–112, IEEE, 2012.

[47] B. Horne, “On computer security incident response teams,” *Security & Privacy, IEEE*, vol. 12, no. 5, pp. 13–15, 2014.

[48] J. G. Walls, G. R. Widmeyer, and O. A. El Sawy, “Building an information system design theory for vigilant eis,” *Information systems research*, vol. 3, no. 1, pp. 36–59, 1992.

[49] R. C. Chandler, “Message mapping: How to communicate during the six stages of a crisis,” tech. rep., Everbridge, 2009.

[50] W. Jansen, *Directions in security metrics research*. DIANE Publishing, 2010.

[51] O. A. El Sawy and T. C. Pauchant, “Triggers, templates and twitches in the tracking of emerging strategic issues,” *Strategic Management Journal*, vol. 9, no. 5, pp. 455–473, 1988.

[52] K. Braa and R. Vidgen, “Interpretation, intervention, and reduction in the organizational laboratory: a framework for in-context information system research,” *Accounting, Management and Information Technologies*, vol. 9, no. 1, pp. 25–47, 1999.

[53] N. M. Pereira, J. v. d. Berg, W. Pieters, D. Hadziosmanovic, M. Warnier, M. Hoeke, and J. Tuin, “The incident prevention team a proactive apporach to information security,” Master’s thesis, Delft University of Technology, January 2015.