SECURITY FROM A SYSTEMS THINKING PERSPECTIVE - APPLYING SOFT SYSTEMS METHODOLOGY TO THE ANALYSIS OF AN INFORMATION SECURITY INCIDENT

Bilal AlSabbagh
Stockholm University
Stockholm, Sweden
bilal@dsv.su.se

Stewart Kowalski
Stockholm University
Stockholm, Sweden
stewart@fc.dsv.su.se

ABSTRACT

Applying systems theory to information security enables security analysts to consider the socio-technical role of the security system instead of only focusing on the technical part. Systems theory can also equip security analysts with the skills required to have a holistic and an abstract level of understanding of the security problem in their organisations and to proactively define and evaluate existing risks. The Soft Systems Methodology (SSM) developed by Peter Checkland was created in order to deal with unstructured situations where human beings are part of the socio-technical system. In this paper, SSM is applied as a framework to diagnose a real case security incident in an organisation. The purpose of this application is to demonstrate how the methodology can be considered a beneficial tool for security analysts during security incident management and risk analysis. Literature review and experience indicate an existing lack of customisable incident response tools that facilitate communication and elaboration within organizations during incident management. In addition to the fact that these tools are mainly technical and don't take the human factor into consideration. Using SSM as such, we define the security attack as a human activity transformation system that transforms a security event triggered by an attacker into a security breach that cause damage to the victim organisation. The attack system is then modelled to include a number of dependent activity sub-systems that interact with each other and their environment including the security control activity systems. By having such systemic perception of a security attack, security analysts, we suggest, can have a holistic perception under what conditions a security attack has succeeded and what elements of the socio-technical system and its environment should have been considered in order to mitigate and reduce the risk exposure.

Keywords: SSM, Socio-Technical Approach, Information Security, Security Approach, Security Incident

INTRODUCTION

Information security is a complicated problem and security breaches continue to manifest their complexities. According to the 2013 data breach and investigation report (Verizon, 2013): "*Security breaches are multifaceted problem and any one-dimensional attempt to describe them fails to adequately describe their complexity*". Based on the findings and analysis of more than 47,000 reported security incidents and 620 confirmed data breaches the report combines the expertise of 19 global organisations from around the world with a mix of incident response and forensic agencies, research institutes, law enforcement agencies and incident handling and reporting entities.

One of the interesting figures brought by the report is that social threat action, i.e. the threat where attackers have used social skills in order to cause or contribute to the breach, was ranked third and constituted 29% of total breaches after malware and hacking. The list also includes misuse, physical, error and environmental threat actions. Phishing was reported to be the primary tactic used in social threats while email was the dominant attack vector used in about 80% of the phishing attacks. According to the U.S. Computer Emergency Readiness Team (US-CERT), phishing is a malicious attempt by an individual or a group in order to steal personal information from unsuspecting users using social engineering skills (McDowell, 2013). This information usually enables attackers to steal victim's credentials or account information, which later expose them or their companies to further compromises. In its negative context, social engineering is defined as the act of influencing a person to do something not in her or his interest (Social Engineer, n.d.). Having said about the complexity of current security breaches and the need for a multi-dimensional approach to describe their complexities shows the importance why we, as a problem solvers, need to seriously start considering a holistic approach for managing and controlling information security incidents. An approach that uses systems thinking that perceives security breaches as an outcome of a certain security system state. A system of interrelated parts or subsystems that interact with each other and with their surrounding environment.

Holistic property of information security has been recognised through the ongoing research on the socio-technical nature of information security. For instance, the socio-technical theory developed by Kowalski has used a holistic approach to model the dynamics of social and technical changes of the system where IT security problem is perceived as an emergent property of an open socio-technical system that is dependent on its environment including social and technical changes (Kowalski, 1994). The system has two subsystems, social and technical. These subsystems are further divided respectively into culture and structure, methods and machines. To reach the secure or controlled state of IT security, the overall system should maintain equilibrium i.e. balance between its social and technical components. Cultural aspect of information security is concerned with human cognition of information security, which accordingly creates distinct attitudes toward understanding existing security risks and how to manage information security. Security culture was defined by (AlSabbagh & Kowalski, 2012) as "*the way our minds are programmed that will create different patterns of thinking, feeling and actions for providing the security process*". One of the metrics being proposed for modelling security culture is "Security Value Chain". The metric was originally developed by Kowalski as a framework that models the mental spending models of organisations based on how they distribute their allocated security budgets on the implementation of the five main security access control categories: Deter, Protect, Detect, Correct and Recover (Kowalski & Edwards, 2004). The framework was then developed as a social metric for modelling the security culture of IT workers individuals at personal, organisation and national levels (AlSabbagh & Kowalski, 2012).

In this paper, we aim at demonstrating the application of Checkland Soft Systems Methodology (SSM) as a managerial tool to diagnose a real case security incident. Because the methodology was created in order to deal with unstructured situations where human beings are part of the socio-technical system, then we suggest it can be a beneficial tool to understand under what conditions a security attack has succeeded and what elements of the system should be taken into account in order to mitigate or reduce the risk exposure.

RESEARCH PROBLEM

There are several reasons motivating us to operationalize SSM as an incident management tool and which constitute the research problem addressed by this paper. The increasing complexity of current security breaches requires more than ever a holistic systemic approach for diagnosing security incidents. An approach that takes into account both the social and technical aspects of the security system including the environment the incident occurs within. Literature survey shows that security incident management and response is still in its infancy (Killcrece et al., 2005). (Spafford, 2003) discussed the 1988 Internet worm that led to the establishment of the first CERT (Computer Emergency Response Team) incident response model. After several years of its establishment, Spafford questioned the CERT model and claimed that current incident response is poorly coordinated and of minimal effect. A similar statement was made by (Schultz, 2004) about CSIRT (Computer Security Incident Response Team) model since they always provide the same generic level of information without thoroughly examining the security incident. According to ENISA (European Union Agency for Network and Information Security), CSIRT and CERT are alternative names for the same incident response model. Moreover, in a recent case study by (Werlinger et al., 2010), 16 semi-structured interviews with IT security practitioners from 7 organisations were conducted to examine the security incident response practices. Their findings showed that organisations are facing challenges when diagnosing security incidents, at least because of the "insufficient" tools support, and that security incident response process required active collaboration between the security incident diagnosis participants and other stakeholders in organisations. The analysis showed that these tools regardless how sophisticated in supporting incident diagnosis they can't be customized to fit those organisations needs.

Current security incident management standards and guidelines, while they attempt to tackle the human factor of the security system by focusing on security awareness and knowledge sharing, still lack the required attention to the socio-technical nature of security systems. (Mitropoulos et al., 2006) proposed a detailed management framework and structured methodology for an appropriate incident management. The framework is based on number of security incident management standards like ISO/IEC 27035, NIST Computer Security Incident Handling Guide, etc. and existing research. Mitropoulos found that current incident response practices are closely related to IT systems and networks and as the intelligence of attacks is increasing by targeting the human factor, security incident response practices should now shift toward the human factor and address security incidents not only reactively but also proactively (i.e. systemically).

Another application of SSM is to facilitate communication and collaboration between incident diagnosis participants and stakeholders in organisations. Empirical research by (Casey, 2005), (Gibson, 2001), (Riden, 2006), (Hove & Tårnes, 2013) and (Ahmad et al., 2012) confirmed challenges associated with insufficient communication and information dissemination during incident management practices and their negative impact on the overall process. SSM can then be used here to integrate the viewpoints and perceptions of stakeholders who are participating in the incident management and to minimise the gap between the awareness and responsibilities of different parties.

We have seen some studies that used SSM methodology for solving issues related to information security as in (Staker, 1999), (Patel, 1995), (Biggam & Hogarth, 2001), etc. However, and to the authors best knowledge, this paper is among the first studies that applied the SSM methodology for diagnosing a real case security incident.

SSM OVERVIEW AND APPLICATION METHODOLOGY

SSM as a methodology has originated during the 1960's by Gwilym Jenkins and his team at Lancaster University. However, It was during the 70's and 80's when SSM became well established and recognised by the work of Peter Checkland (Veltman, 2006). The methodology has emerged as the result from attempts to solve problems related to organisational management using existing systems engineering approach i.e. hard systems thinking methods. At that time it was found that such approach is mainly appropriate for solving well-defined technical problems where the system objectives are already known. For situations where the problem is ill-structured or ill-defined and involves considerations related to human beings e.g. culture, a more appropriate approach was needed which resulted in the development of SSM. While the hard system thinking approach perceives the world as systemic, SSM systemic perception lays on the process of inquiring and exploring an observed complexity i.e. deal with unstructured problem and then have it moved to a structured one (Checkland, 1999).

During its development SSM has undergone substantial evolution since its inception. However, the original "seven-stage" version depicted in Figure 1 and published by Checkland in his book "*Systems Thinking, Systems Practice*" is "rich enough", "resilient" and still widely used and taught. In this version the seven stages are categorised under two kinds of activities: real world and system thinking. Real world activities (comprised of stages 1, 2, 5, 6 and 7) use non-systems thinking language and involve collecting and presenting information about the problem in hand. The problem solver i.e. system thinker then moves to systems thinking activities (comprised of stages 3 and 4) in order to perform analysis and unravel then understand the existing complexity which after moves back to real world activities to verify the findings and requirements.

In this study we aim at exploiting SSM features to check how the methodology can be operationalized as a support tool for diagnosing a real case security incident. Literature survey shows the importance and need for more collaboration between stakeholders in organisations during an incident response in addition to an existing lack in incident diagnostic tools. For the context of this paper, the most interesting feature of SSM, in addition to its ability to deal with unstructured human related situations and subjectivity associated with every human activity system, is the one described by (Khisty, 1995) about having two “streams” of analysis: “Logic-driven” and “Culture-driven”. In culture-driven analysis, both the social and political contexts of the problem situation are examined. Both streams interact with and inform each others during the problem analysis. For us this is an interesting feature given the scope of the problem is to identify the socio-technical issues associated with the security incident and to improve collaboration between stakeholders.

We are going to test the application of SSM in its seven-stages model to diagnose a real-case security incident that hit an organisation and incurred confidential information disclosure associated with confusion among stakeholders regarding responsibilities and awareness. More information about the security incident is provided while applying the methodology. Our expectations from applying the methodology to the problematic situation is to respond to the security incident management challenges we presented in the introduction and research problem sections by meeting the following criteria:

- An incident management tool that can facilitate collaboration and communication between stakeholders by developing dialogues to minimise existing gaps in security awareness and responsibilities.
- An incident management tool that provide a holistic and systemic perception to the security incident situation that in turns enable us to:
    - Identify the required and missing technical security controls that should be implemented in order to deal with every activity of the security attack system.
    - Identify the security vulnerabilities triggered by the organisation culture and individuals norms.

We start our experiment by collecting information from the stakeholders about the problematic situation including the nature and impact of the security incident. This information will be used to compose the rich picture about the current problem situation. We then work toward creating a root definition of the security attack activity system followed by a generic low-resolution conceptual model. A High-resolution version of the conceptual model is then created in order to reflect how the system activities are taking place and interacting with the surrounding environmental elements. The conceptual model will then be compared to the identified problematic situation to identify the required socio-technical improvements. At the end we list what are the taken improvement actions and existing limitations, if any. In the next sections we provide a short account of every stage of the SSM methodology while demonstrating its application to the security incident.

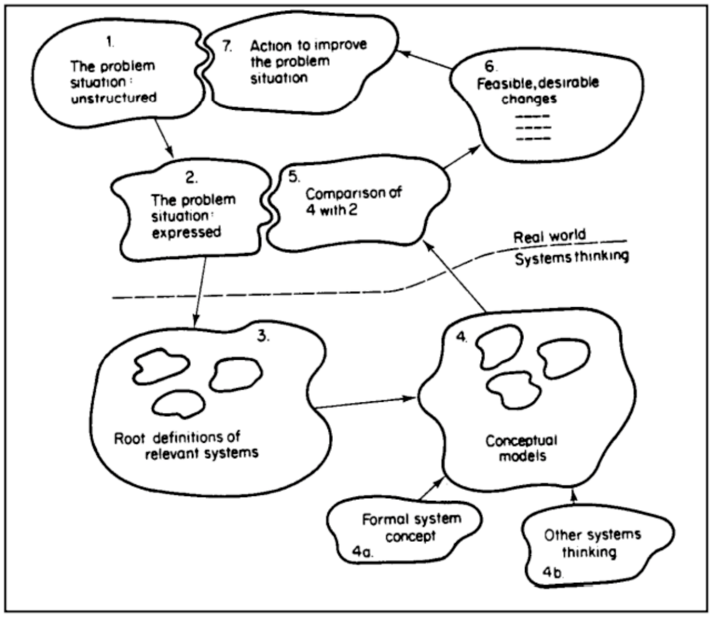
1.
The problem situation: unstructured
7. Action to improve the problem situation
6. Feasible, desirable changes
2. The problem situation: expressed
5. Comparison of 4 with 2
Real world
Systems thinking
3.
Root definitions of relevant systems
4.
Conceptual models
Formal system concept
4a.
Other systems thinking
4b

Figure 1. Checkland Seven-Stage SSM Methodology

UNDERSTANDING THE PROBLEM SITUATION: STAGES 1 AND 2

During the first two stages of the methodology the problem situation is understood then expressed. In stage one there is no clear definition of the problem situation, instead understanding of the problem is collected from the involved stakeholders. In stage 2 the problem situation is expressed, preferably using a “rich picture” where the system thinker develops a detailed description of the problem. The rich picture usually captures the relationships between the problem elements and their structure.

To understand the problem situation we have conducted a number of unstructured interviews with stakeholders from different departments in the organisation including the security operations department, IT department, general management and number of regular staff. The interviews discussion has focused on a recent security attack that hit the organisation email service and on the stakeholders’ role to the security process and their responsibility about the success of the security incident. What happened is that an attacker has targeted the organisation email service and compromised users’ emails credentials by sending them a malicious email from the compromised organisation director email address. The email included a malicious link to a phishing website similar to the organisation email portal requesting them to login again. Those users who have responded to the email and attempted to login through the phishing site have basically provided their credentials to the attacker. Figure 2 below provides the rich picture of the situation after collecting different perceptions about the problem.

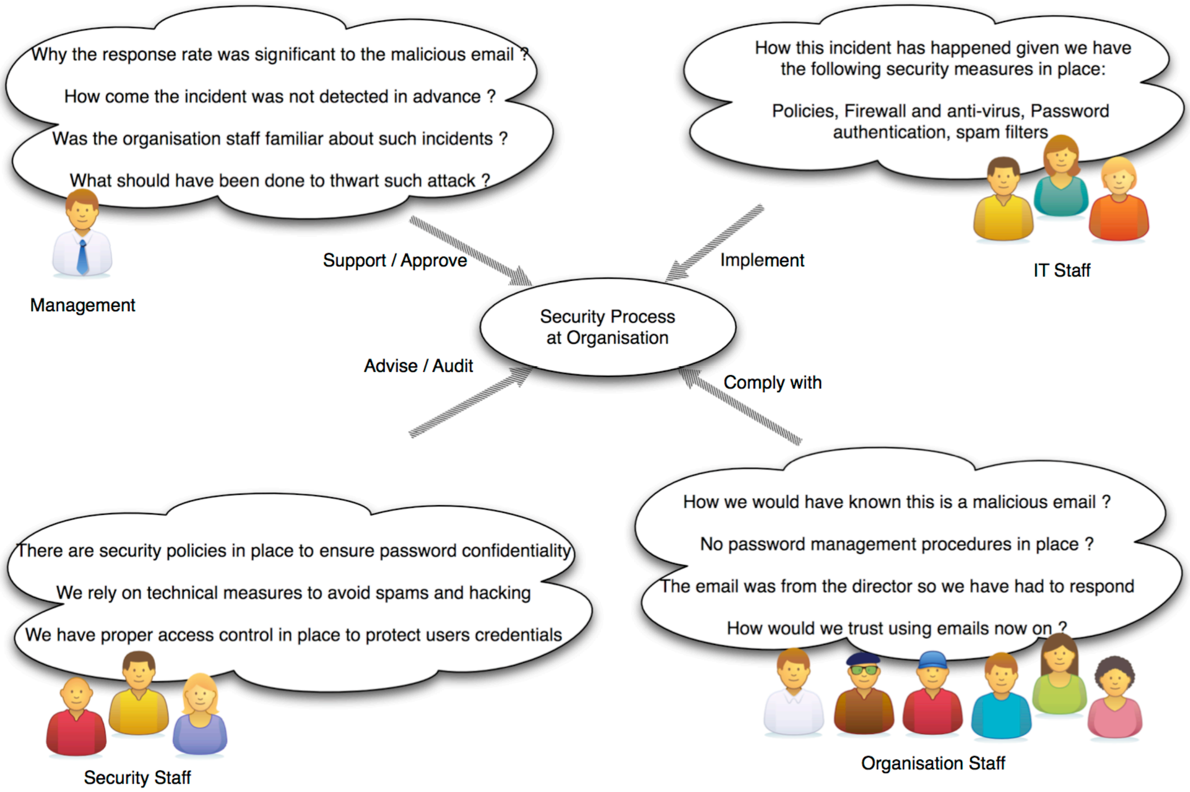
Why the response rate was significant to the malicious email ?
How come the incident was not detected in advance ?
Was the organisation staff familiar about such incidents ?
What should have been done to thwart such attack ?
Management
How this incident has happened given we have the following security measures in place:
Policies, Firewall and anti-virus, Password authentication, spam filters
IT Staff
Support / Approve
Implement
Security Process at Organisation
Advise / Audit
Comply with
There are security policies in place to ensure password confidentiality
We rely on technical measures to avoid spams and hacking
We have proper access control in place to protect users credentials
Security Staff
How we would have known this is a malicious email ?
No password management procedures in place ?
The email was from the director so we have had to respond
How would we trust using emails now on ?
Organisation Staff

Figure 2. The Rich Picture of the Problem Situation

THE ROOT DEFINITION: STAGE 3

Developing the root definition is a fundamental activity in the SSM methodology where a human activity system relevant to the complex problem situation is identified and defined. The root definition should include a structured description of the elements captured in the defined system with a clear statement of the activities it should perform. According to (Checkland, 1999) and (Smyth & Checkland, 1976), an adequate root definition should contain six explicit elements known by the mnemonic “CATWOE” derived from Customers, Actors, Transformation process, Weltanschauung, Owners and Environment. The omission of any of these elements should be conscious and only for a good reason.

Given the subject matter of this paper is to diagnose a real case security incident using SSM methodology, it was found that considering a “security attack” as an activity system for the root definition will provide the required rich picture needed in order to reduce the problem complexity and identify the issues of concerns. According to Checkland, there are two types of systems that can be described: primary task and issue based systems. The system described in the root definition falls under the issue based system. This root definition was constructed considering the point of view of the security analyst.

A root definition of the security attack as an activity system is:

“A malicious activity committed by an individual‘ to exploit existing social or technical vulnerability, to compromise organization security controls, to make unauthorized use of organization assets, to cease or damage the organization business.”

The “CATWOE” elements of the root definition are illustrated along a brief description of each of the mnemonic elements as follows:

C: Customers of the system are those who are either beneficiaries or victims of the system activities. From the point of view of a security analyst the victim of a security attack is the organization while the main beneficiary is the attacker or adversary.

A: Actors of the system are those who actually carry out the main activities of the system and transform its inputs into outputs. A security attacker is considered the main actor of the defined system.

T: The transformation process carried out by the system. What does the system do in order to transform its inputs into outputs. A security attack as an activity system transforms a security event triggered by an attacker into a harmful action i.e. damage against a target organization. The harm can be against a particular service or against the organization business and reputation.

W: The Weltanschauung or viewpoint that makes the root definition meaningful. In this study the Weltanschauung that makes this root definition meaningful is the need for diagnosing the security incident in order to determine the related issues and contributing factors.

O: The system owner is the one who has the ultimate power over the system and can stop it. In the context of a security attack the system owner is the security attacker who plans and commits the attack activity. However there could be cases where the system ownership is lost or transferred based on the nature of the security attack and its progress. For example, an attacker who has sent an infected email attachment might not be able to control the consequences or stop the progress of the attack. Having that said, it is doable to consider the security operations team as a secondary system owner because ideally the team should be capable of stopping security attacks targeting the organization.

E: The environmental constraints the system will operate within. In the case of a security attack the environmental constraints are determined by the existing security risks at the organization, access control implementations, staff security awareness, existing security culture and security mental models. The conceptual model in the next section will include more elaboration about the environmental constraints the security attack will operate within.

THE CONCEPTUAL MODEL: STAGE 4

The conceptual model is an abstract representation of the suggested human activity system described in the root definition. According to Checkland, the conceptual model should include "what" activities happen in the system. A higher resolution version of the conceptual model can later include "How" these activities are actually happening. The verbs used in the conceptual model activities should be limited and preferably not to exceed more than six verbs (Checkland, 1999). These verbs should be sufficient to make the conceptual model the one described in the root definition. The logical dependencies between the system activities in the conceptual model are represented using connecting arrows. In Figure 3 we depict the basic low-resolution conceptual model we have developed to describe the security attack as an activity system. The conceptual model also includes five security-control systems that comprise the surrounding environment, which the attack system operates within and interacts with. These control systems represent the different types of security measures implemented in the organization and which, based on how effective they are, can either hinder the attack or control it. The effectiveness of these security controls depends on how well the organization manages existing risks, both social and technical.

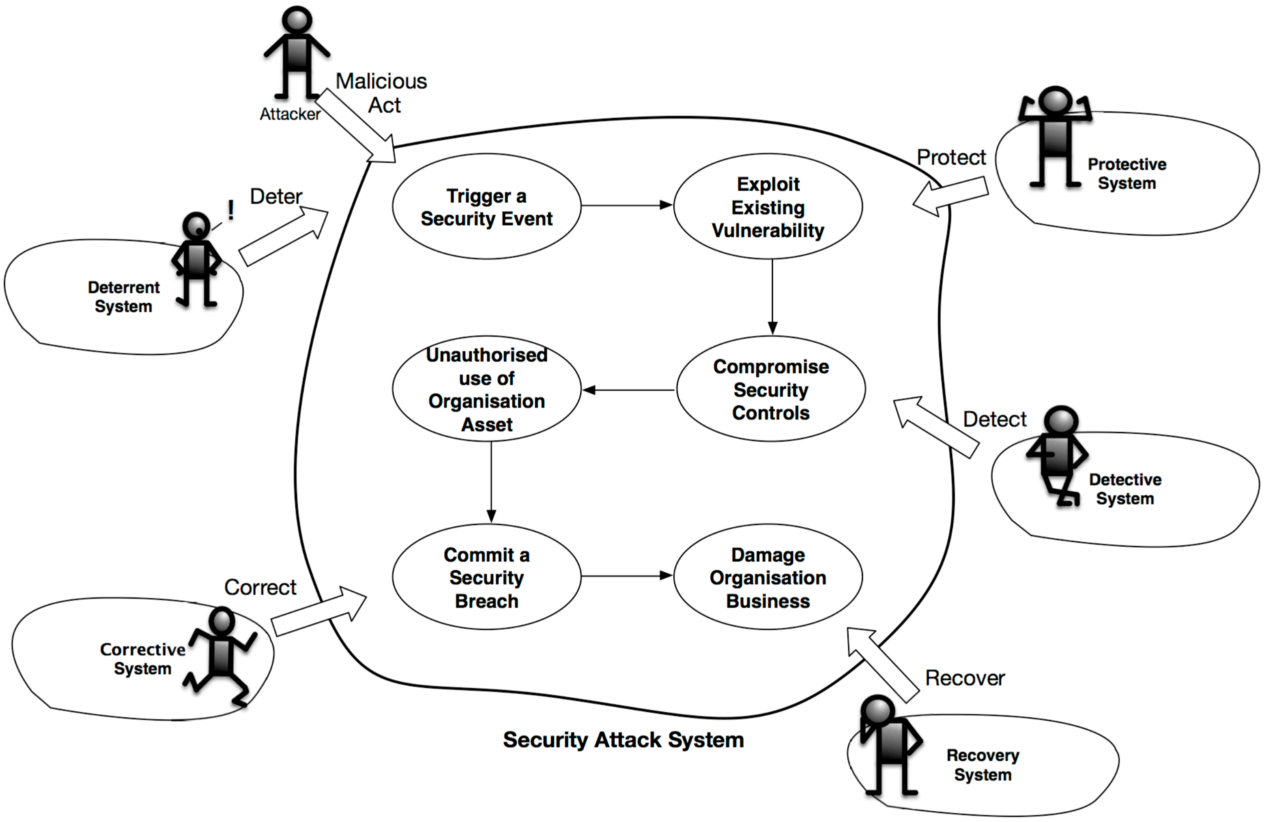

Figure 3. The Conceptual Model of the Security Attack System

After planning and setting up the attack objectives the initial action taken by an attacker to commence his attack will trigger a security event that, based on the attack type, can take various forms. Security events have two categories: social and technical. For instance, a false telephone call impersonating helpdesk or support staff member in order to steal employee credentials or other sensitive information is considered a social security event. A malicious request against the organisation computing resources e.g. SQL injection, Cross Site Scripting, brute forcing is an example of a technical security event. A malicious email including a harmful attachment or phishing contents sent to an individual or group of employees in order to trick them to perform a desired malicious action is an example of both social and technical security event. The next activity of a security attack is to have the security event successfully enable the attacker to exploit an existing social or technical vulnerability or even both. Social vulnerabilities are results of human attitudes and lack of security awareness. Research has shown interesting findings about how individuals from different cultures can have different cognition of what constitutes a security risk and what approaches are perceived required to mitigate those risks (Oltedal et al., 2004) (Douglas & Wildavsky, 1982). Other researches show how different cultural norms cast individual attitudes that itself can be a threat to security or constitute a security vulnerability (Glaster, 2009). Technical vulnerabilities are caused by platforms misconfiguration, lack of or improperly configured access control, not patched operating systems and application or even a completely new unknown vulnerability as in Zero day attacks (Symantec, n.d.). Whether social or technical, once an existing vulnerability is successfully exploited it will enable the attacker after then to compromise existing security controls in an attempt to illegitimately access and make use of an organization asset.

Committing a security breach starts by the time the attacker has successfully managed to bypass the security controls and illegitimately accessed an organization asset. At this stage the attacker leverages the acquired asset to commit his attack and meet the planned attack objectives. For instance the acquired asset might includes the confidential information the attacker wanted to obtain or the asset can be further used as an offset to launch a more sophisticated attack against internal or external networks. The last stage of a security attack is to trigger damage against the victim organization and have it suffering from the attack consequences. Such damage usually harms the organization business and its reputation e.g. stealing business secrets.

In the next figure 4 a high-resolution version of the security attack conceptual model is demonstrated to include together the “Whats” and “Hows” activities of the attack system and its surrounding environmental control systems. The details included in the conceptual model correspond to a real case security attack that has hit a client organisation the author works for. The author acts here as a system analyst who is using the SSM methodology to diagnose the situation and identify the problematic areas and suggested improvements.

The security incident has involved an attacker who has designed and implemented a phishing webmail portal, with the exact look and feel as the webmail portal of the organization, to illegitimately collect the login credentials of the organization staff. The attacker has then crafted a malicious email message to the organization director. The message included a URL to, which appeared to be, an interesting online article but in fact it was just a link to the phishing webmail portal. It was at this point when the director got confused and just thought that he has to login again to his organization email account. Now, and due to the director insufficient security awareness about such kind of attacks e.g. not looking at the address bar of the fake webmail, the attacker was able to steal the director credentials and take control over his email to further continue with his attack. Such an attack should have not succeeded if there was a multi-factor authentication mechanism implemented at the organization. In multi-factor authentication it is not just enough for a user to supply a username and password in order to login, instead the user should supply more information during the login related to something he own such a one-time password security token or a digital certificate. In this case even if the username and password were compromised, they are not sufficient for the attacker to accomplish a successful login. The existing vulnerabilities related to the missing password management standard, insecure authentication practices and lack of security awareness have enabled the attacker to compromise the company access controls and have a direct access to the director email looking at potential confidential internal communication and business activities.

Taking control over the director email has allowed the attacker to leverage this asset i.e. the director email account and commit a major security breach against the organization. This time the attacker has used the director email to influence the response rate upon sending a malicious message targeting the internal staff and requesting them to visit a particular URL which include a malicious link to the phishing webmail portal. It was at this point when the security breach had a significant effect where the attacker has started collecting victims credentials and take control over the organization email communication. During discussions with some victims we have noticed that one important factor behind the significant response rate to the director impersonated email message is a cultural factor related to what Hofstede has called “Power Distance” (Hofstede & Hofstede, 2005). Power distance is defined as theextend to which an organization employees accept that power is unequally distributed among its staff members. High levels of power distance imply higher unquestioned adherence to the orders and instructions of managers. According to Hofstede, in organizations with high levels of power distance subordinates expect to be told what to do. On a scale of 74 countries, the organization country where this case study was conducted was on the top twelfth of large power distance. This social norm has constituted a social vulnerability that has been indirectly exploited during the attack to trigger higher response rate. The damage incurred by the attack is the exposure of the confidential information included in the email communications. There was no certainty for what purpose the information will be used and at what time. The incident has also rendered the email service unreliable within the organization, at least at the beginning after disclosing the attack because the email users have stopped trusting this service.

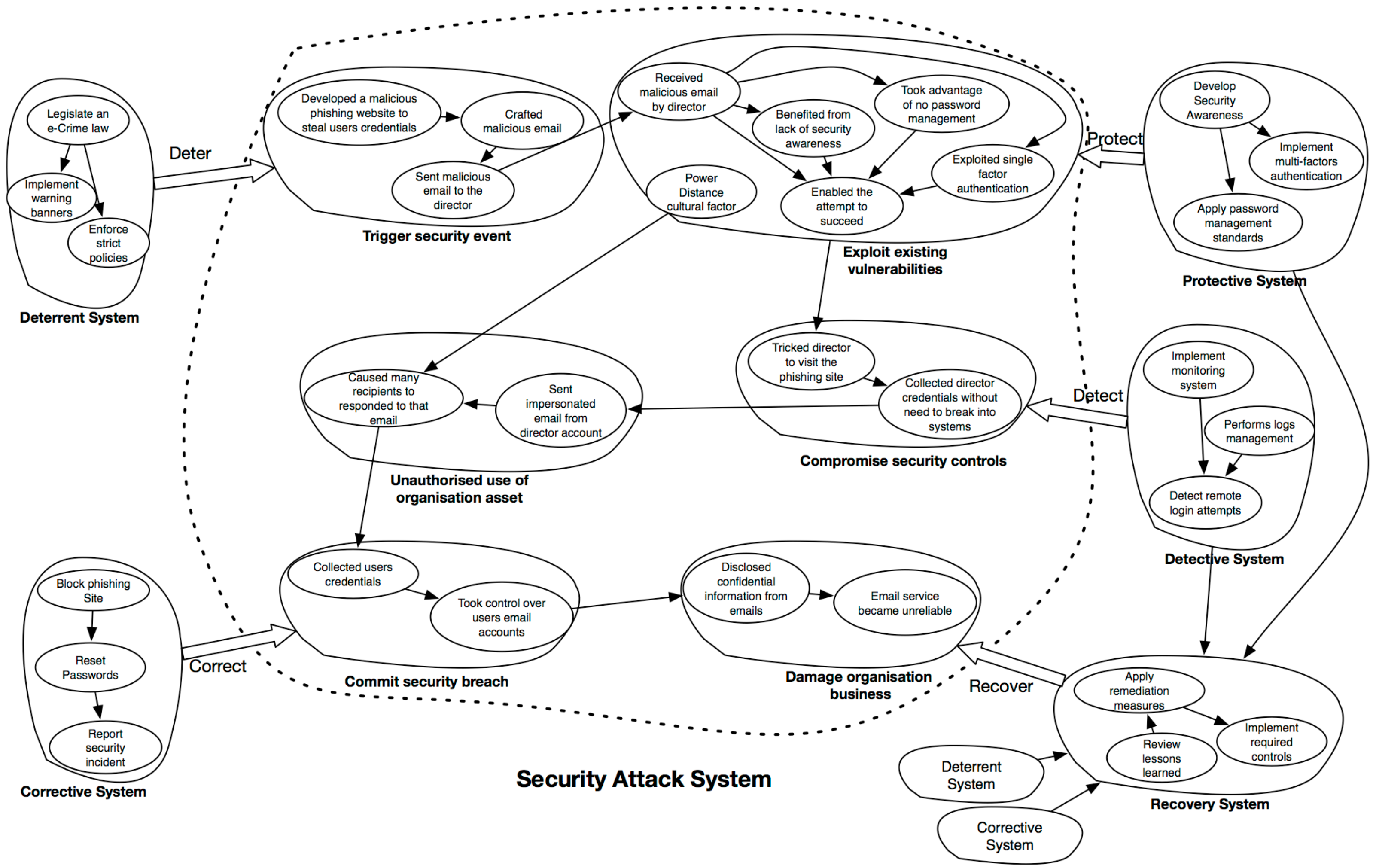
Legislate an e-Crime law
Implement warning banners
Enforce strict policies
Deterrent System
Deter
Developed a malicious phishing website to steal users credentials
Crafted malicious email
Sent malicious email to the director
Trigger security event
Received malicious email by director
Benefited from lack of security awareness
Took advantage of no password management
Exploited single factor authentication
Power Distance cultural factor
Enabled the attempt to succeed
Exploit existing vulnerabilities
Protect
Develop Security Awareness
Implement multi-factors authentication
Apply password management standards
Protective System
Caused many recipients to responded to that email
Sent impersonated email from director account
Unauthorised use of organisation asset
Tricked director to visit the phishing site
Collected director credentials without need to break into systems
Compromise security controls
Detect
Implement monitoring system
Performs logs management
Detect remote login attempts
Detective System
Block phishing Site
Reset Passwords
Report security incident
Corrective System
Correct
Collected users credentials
Took control over users email accounts
Commit security breach
Disclosed confidential information from emails
Email service became unreliable
Damage organisation business
Recover
Security Attack System
Apply remediation measures
Review lessons learned
Implement required controls
Recovery System
Deterrent System
Corrective System

Figure 4. The High Resolution Conceptual Model of the Case Study Incident

COMPARING THE CONCEPTUAL MODEL TO THE EXPRESSED PROBLEM FOR IMPROVING THE PROBLEM SITUATION: STAGES 5 AND 6

During this stage the developed conceptual model from the root definition is compared against the problematic situation in order to define the required improvement areas or changes. According to Checkland and based on practical experience there are four ways to carry on this kind of comparison:

- Use the conceptual model as a source of questions for raising a debate about what changes are needed to solve the existing problem.
- Compare the conceptual model with a sequence of historical activities which have triggered the existing problem and see what would have happened and maybe improved if the developed conceptual model was applied.
- Compare the conceptual model features to the current practices and raise challenging questions about the current activities if they are anymore required.
- Create a conceptual model for the current situation and perform a “direct overlay” with the conceptual model developed from the root definition in order to reveal areas of mismatch and determine the required changes.

In this study we have used a hybrid comparison approach by combining the first and third methods from the previous list. The root definition of the security attack and its developed conceptual models have enabled us to create a breakdown of the security attack activities and elaborate on how every activity was carried out in reality. We were also able to conceptualise the security controls as external activity systems that interact with the defined activities of the security attack as an activity system. This systemic approach to analysing the security attack has enabled us to identify the existing socio-technical vulnerabilities that were exploited, and those missing security controls. Based on these findings a number of questions were developed to administer a dialogue with the IT and security operations department about the problematic situation and how improvements can be applied taking into account our findings. The problem situation captured in the rich picture and which represents the different stakeholders perception of the security incident has made the dialogue more effective as it helped us to learn more about the organization security culture and existing awareness. These findings were also considered in the suggested improvement actions.

The table below lists the identified vulnerabilities and related missing controls, then followed by the questions used during the dialogue:

Table 1. List of identified social and technical vulnerabilities

Identified vulnerabilities			
Social			
	Lack of security awareness about phishing techniques and how to verify a website authenticity	High levels of power distance cultural factor have resulted in a significant response rate to the director impersonated email.	Lack of deterrent security controls due to believing they are inappropriate and they instead stimulate attacks.
Technical			
	Password only based authentication (single-factor authentication)	Immature detective measures for monitoring external login attempts to email system during working hours	Missing practices related to password management standards and procedures

Developed dialogue questions:

1. Do you agree that implementing a warning message on the organisation webmail portal against phishing attempts could have demotivated the attacker from continuing his attack?

2. The attacker has successfully taken over the director email and later other employees' emails after collecting their credentials. This was technically possible because the attacker only requires a username and password to login. How about improving the situation and start introducing a two-factor authentication to make such attack impossible to commit next time?

3. Did we have the means to monitor and detect external login attempts to the email system during the working hours? i.e. a monitoring system that notifies IT administrators about such attempts. Such measure could have helped our administrators to interrupt the attack earlier.

4. The significant response rate to the impersonated director email, we believe, has to do with the high levels of power distance cultural factor. What controls should be implemented to refrain exploiting such attitude?

5. Our employees were obviously not aware enough about phishing techniques. Are there any plans for running security awareness campaigns in the organization?

THE SITUATION IMPROVED: STAGE 7

The following actions were taken as a result of the study:

- Agreement to conduct an internal security awareness program for the organisation staff followed by an assessment to measure the effectiveness of the awareness process.
- Decision to implement two-factor authentication for accessing the organization email service. A certificate based authentication for accessing the email system internally from within the organisation network and a security token (one time password) for accessing the webmail portal.
- Leverage the monitoring system to accommodate a feature related to detecting external login attempts to the organisation email system during working hours.
- Potential consensus on implementing deterrent measures including security warning banners on all organisation web services.

DISCUSSION AND FURTHER RESEARCH

In this paper we have demonstrated the use of Checkland Soft Systems Methodology (SSM) as a diagnostic tool to analyse a real case security incident. Current literature survey and empirical research about incident response practices at organizations reveal issues related to communication and collaboration between stakeholders for a successful incident management. Latest reports about security breaches confirm the increasing social vector of security incidents and that security response practices should take this fact into consideration. By applying SSM to analyse a real case security incident we would like to present the tool as a strong candidate that can optimise the communication and elaboration between stakeholders. Applying the methodology has enabled us to capture the different attitudes and conception of stakeholders about the security incident and develop a dialogue that has facilitated key decisions related to security controls implementations. Another strength of the tool is that it enabled us to capture and identify vulnerabilities related to some stakeholders' attitudes. For instance the high power distance inherited from the local culture where the organization is located was a key factor for the high response rate to the malicious email. The rich picture of the problem situation has also revealed issues related to security awareness and misconception of security controls application.

However, it is important to mention that applying SSM for security incident management seems to have limitations and constraints as well. For instance, the system thinker, if to use the methodology by her or his own, should have a strong account in information security management and how attack techniques work. This is required in order to be able to create the high-resolution conceptual model for the corresponding incident. Also the tool should not be considered a technical one. The ideal application of the tool, we suggest, is to be considered as a managerial one that is used to provide holistic perceptions of the security in an organization and in turns provide insights on the required proactive and reactive security controls measures.

As a future research, we would be interested to have this experiment replicated in other organizations to validate the gained benefits and possible weaknesses in using SSM as an information security incident management tool.

REFERENCES

AlSabbagh, B. and Kowalski, S. (2012). Developing Social Metrics for Security – Modeling the Security Culture of IT Workers Individuals (Case Study), in proceedings of the 5th International Conference on Communications, Computers and Applications (MIC-CCA 2012).

Ahmad, A., Hadgkiss, J. and Ruighaver, A.B. (2012). Incident response teams– Challenges in supporting the organisational security function, *Computers & Security.* 31(5):643-652.

Biggam, J. and Hogarth, A. (2001). Using Soft Systems Methodology to Facilitate the Development of A Computer Security Teaching Module. Proceedings of the IFIP TC11 WG11.1/WG11.2 Eigth Annual Working Conference on Advances in Information Security Management & Small Systems Security, Pages 113-126.

Casey, E. (2005), Case study: network intrusion investigation – lessons in forensic preparation, *Digital Investigation*. 2(4):254-260.

Checkland, P. (1999). *Systems Thinking, Systems Practice: Includes a 30-Year Retrospective.*, Wiley, England.

Douglas, M. and Wildavsky, A. (1982). *Risk and Culture.*, University of California Press, Los Angeles; London.

Gibson, S. (2001), The strange tale of the denial of service attacks on GRC.com, available at: http://whitepapers.zdnet.co.uk/,.

Glaser, T. D. (2009). Culture and Information Security: Outsourcing IT Services in China. Berlin Institute of Technology.

Hofstede G. and Hofstede, G. J. (2005). *Cultures and Organizations, Software of the Mind.* Second Edition., McGraw-Hill, United States of America.

Hove C and Tårnes M. (2013). Information Security Incident Management : An Empirical Study of Current Practice. Norges teknisk-naturvitenskapelige universitet Institutt for telematikk.

Killcrece, G., Kossakowski, K., Ruefle, R. and Zajicek, M. (2005). Incident management. A technical report US Department of Homeland Security, Washington, DC.

Khisty, C. J. (1995). Soft systems methodology as learning and management tool, *Journal of Urban Planning and Development.*, 121(3):91–107.

Kowalski, S. 1994. IT insecurity: a multi-discipline inquiry. Department of Computer and System Sciences, University of Stockholm and Royal Institute of Technology, Sweden.

Kowalski, S. and Edwards, N. (2004). A security and trust framework for a wireless world: A cross issue approach. Wireless World Research Forum no. 12, Toronto, Canada.

McDowell, M. (2013). Avoiding Social Engineering and Phishing Attacks. United States Computer Emergency Readiness Team. Available at: http://www.us-cert.gov/ncas/tips/ST04-014. Accessed: May 30th, 2014.

Mitropoulos, S., Patsos, D., Douligeris, C. (2006). On incident handling and response: a state of the art approach, *Computers and Security.*, 25(5):351-370.

Oltedal, S., Moen, B., Klempe, H. and Rundmo, T. (2004). Explaining Risk Perception. An evaluation of cultural theory. Norwegian University of Science and Technology.

Patel, N. (1995). Application of soft systems methodology to the real world process of teaching and learning, *The International Journal for Educational Management.*, 9:13-23.

Riden, J. (2006). Responding to security incidents on a large academic network. Available at: www.infosecwriters.com/text_resources/ pdf/case_study_JRiden.pdf.

Schultz, E. (2004). Incident response teams need to change, *Computers and Security Journal.*, 23:87–88.

Social Engineer (n.d.). What is Social Engineering. Available at: http://www.social-engineer.org. Date of Access April 20th, 2014.

Smyth, D. S. and Checkland, P. B. (1976). Using a systems approach: the structure of root definitions, *Journal of Applied Systems Analysis.*,5(1):75-83.

Spafford, E.H. (2003). A failure to learn from the past. Annual Computer Security Applications Conference (ACSAC), Las Vegas, NV, December 8-12, pp.217-33.

Staker, R. J. (1999). An Application of Checkland's Soft Systems Methodology to the Development of a Military Information Operations Capability for the Australian Defence Force. Salisbury, South Australia: Electronics and Surveillance Research Laboratory.

Symantec (n.d.). Vulnerability Trends. Available at: http://www.symantec.com/threatreport/topic.jsp?id=vulnerability_trends&aid=zero_day_vulnerabilities. Date of Access: April 30th, 2014.

Veltman, K. (2006): Understanding New Media: Augmented Knowledge and Culture. University of Calgary Press.

Verizon Risk Team (2013). 2013 Data Breach Investigations report. Available at: http://www.verizonenterprise.com/DBIR/2013/. Date of access: March 2nd, 2014.