An interdisciplinary approach and framework for dealing with security breaches and organizational recovery

Trim, P.R.J., Lee, Yang-im and Weston, D.

This is a copy of a chapter published in: Trim, P.R.J. and H.Y. Youm (ed.) Korea-UK Collaboration in Cyber Security: From Issues and Challenges to Sustainable Partnership Republic of Korea British Embassy Seoul, pp. 34-43.

Paper 7: An interdisciplinary approach and framework for dealing with security breaches and organizational recovery.

Peter R.J. Trim, Yang-Im Lee and David Weston.

Introduction

This paper takes into account the work undertaken by Winsberg (2003), Yao et al., (2005), van der Aalst and Stahl (2011), and Thomas et al., (2013). It represents an attempt at studying the effect of an information breach, how an organization recovers from an attack and also, how management can estimate the cost of an attack in terms of resources, lost income and future investments in recovery related expenditures. We concur with the view of Thomas et al., (2013, p.2) and accept that more needs to be done with respect to developing methods and frameworks that assist the closure of the gap between academic research and professional practice. The objective of this paper is therefore, to explain how managers in an organization can estimate the cost of a potential security breach and make a case to senior management for additional resources that assist the repair and recovery stage. We assume, therefore, that a breach will occur and that by investing resources in the recovery stage, the organization will be able to continue functioning. We assume that managers within the organization will, by referencing the incident in the organization's risk register, be transparent about a potential impact and its consequences, and will share information with other organizations in the industry and elsewhere. It is our ultimate intention to produce a virtual cyber security emergency planning simulation that can train cyber security professionals and those undertaking a training and/or educational programme in the area of cyber security.

Scenario exercises

It is our intention to add to the academic literature highlighting the importance of scenario planning, for example, Yao et al., (2005, p.1645) are right to suggest that: "Through scenarios we can prioritize the opportunities or threats and put our scarce and valuable resources to producing the greatest return". This statement has implications for management and we intend to make clear the fact that by adopting a pro-active approach to cyber security problems, management can think less about the "what if" factors and more about the contingencies that need to be in place to stop an impact having a detrimental effect on a company. Another point to take into account when engaging in modelling of any kind, is that a business intelligence system (van der Aalst and Stahl, 2011, p.11): "provides tools to analyze the performance-that is, the efficiency and effectiveness-of running business processes". It is envisaged that the research referred to in this paper will add to the body of knowledge relating to how modelling is used to facilitate decision-making in complex situations. As regards the benefits associated with simulations, Winsberg (2003, p.116) has suggested that "Simulation is a technique that begins with well-established theoretical principles, and through a carefully crafted process, creates new descriptions of the systems governed by those principles. It is a technique that, when properly used, will provide information about systems for which previous experimental Data is scare.……..Furthermore, simulations often yield sanctioned and reliable new knowledge of systems……"

Yao et al., (2005, p.1644) acknowledge that: "Simulation is probably the most widely used and the most effective method to train emergency management workers. Its fidelity can create

tensions and stimulate emotions similar to real emergency/disasters". There are two types of simulation. The real world version such as "Operation Waking Shark 2" (where UK banks were subject to a simulated attack) and the type of simulation we shall do using, the petri-nets where we attempt to model certain aspects of the information security process. A virtual simulation has a number of advantages associated with it, for example, according to Yao et al., (2005, pp.1644-1645) it can be considered (i) flexible (various emergency/disaster situations can be incorporated); (ii) easy to deliver (those involved can be based anywhere and only need a personal computer, to be connected to the Internet, and a groupware server package); (iii) promote collaborative learning, as the on-line learning environment can facilitate, through interaction, deep thinking, as well as critical and creative thinking.

Theoretical framework and conceptual approach

The focus of attention is how managers in an organization establish that a potential cyber attack launched on an organization will cause harm and how resources for the recovery period can be committed so that the organization is able to carry out a full repair and continue in business. We assume that the impact on the organization is insufficient to put it out of business for a long period of time and assume that the organization will be fully operational within 24 hours. Should the breach be more harmful than expected, it is envisaged that the company will be unable to operate for 48 hours; and if it is considered a really devastating attack, the company will be unable to trade for 36 hours or longer. From a financial point of view, we estimate that the cost of not operating for 24 hours (wages, insurance, lost business for example) is referred to as LB (loss in business) and denoted as LB-1, and for subsequent days is LB-2, LB-3 etc. If the cost of a data breach is £100 per record, then if 1,000 records are effected, the cost would be 1,000 x £100 = £100,000 times 2 days represents £200,000 and three days would represent £300,000. This cost is not we consider unreasonable although we accept that it is higher than other estimates reported (House of Commons, 2012, p.6).

We accept that research related to recovery and restoration underpins resilience planning (Thomas et al., 2013, p.9) and it is our intention to provide an interactive framework so that managers within an organization communicate with each other in order to rectify a problem as soon as possible. For example, we have used the following weighting factor: c (communication) is excellent and rated C1. When communication is poor, we assume that there is a 24 hour delay in a message being transmitted so therefore, C+24, is represented by C+0.24 (weighting factor) and for a 48 hours delay we use C+0.48 and for three days we use C+0.60 for example. If we accept that cyber attacks are increasing in intensity and sophistication, it is possible to include in the equation an extra element, namely the cost of buying in expertise and assistance. For example, a 'light' impact which causes limited disruption means that the organization's cyber security defences are reasonably robust, however, a devastating impact allows us to assume that the organization's cyber security defence system is ineffective in which case the in-house cyber security knowledge and capability is deemed to be poor and the company has to buy in knowledge and expertise from specialist providers. We denote this in the following way: CSP (cyber security provision) can be rated as poor, adequate or satisfactory. This can be interpreted at levels, for example, CSP 3(poor) and a high need represents a weighting factor of 0.3; CSP 2 (adequate) represents a weighting of 0.2; and CSP 1 (satisfactory) represents a weighting of 0.1. It is possible to quantify these weightings in terms of cost: poor represents an immediate investment in cyber

security services of £75,000; adequate represents an immediate investment in cyber security services of £50,000; and satisfactory represents an immediate investment in cyber security services of £25,000.

With reference to the case example outlined below, we can assume the reputational damage to the company was 15% of its share value. Therefore, we need to include in the above equation a weighting factor of 0.15 loss in company value which can be interpreted as a multiplier of 0.15. Should this be the case, it is possible that shareholders will divest their shares in the company because they consider that the company's shares will deteriorate further. Hence we assume that one shareholder will sell their shares in the company and as a result, the share price will fall by another 5 per cent. We include this in the calculation as an additional multiplier of 0.05. So reputational damage is estimated at 20% of the share value of the company or 0.20.

As regards quantifying the share value, it can be noted that the day before the incident the share price of the company stood at £20; therefore, on day 1 of the incident, the share value represented £17 and day 2 witnessed a decrease of an additional 5%, so the actual value of the shares would be £16.15 each representing a decrease of £3.85 or 19.25% from the day before the incident.

Owing to the fact that companies do not operate in isolation and have a number of interdependent relationships with other companies, and are part of a network of organizations, it can be assumed that there is a risk that the company that has sustained a cyber attack will lose future business as customer organizations consider that the staff in the company are untrustworthy if they do not communicate the depth of the problem at the earliest opportunity. For example, if on day one management within the company attacked keep quiet (do not inform customer organizations, financiers (banks) and suppliers for example), the risk associated with these stakeholder organizations terminating business links with the company is considered to be low (e.g., a weighing of 0.10 is assigned). However, once rumours spread or matters become public the risk that the stakeholder organizations will terminate business with the affected company increases from low to medium risk (e.g., 2 to 3 days and a weighting of 0.2 to 0.3). By day 4 a high risk is recorded. From day four onwards a weighting of 0.4 is recorded because it is assumed that after day 4 the risk will become constant because it is not in the interest of anybody to terminate the business relationship by then.

Case example. The branching or cascading effect.

The IT Manager, had discovered that the company's marketing data base had been penetrated by a competitor and that staff in the competitor organization had been stealing data from the company. This was not unusual because a report in a national newspaper had indicated several cases of hacking in association with customer client lists. In some cases, it was the result of insider action. For example, in one case, two employees working for the same company had taken a manager's password and entered and downloaded sensitive company data from one of the subsidiary organizations working in the area of government contracts and the same company had been subject to several hacking attacks from a private company that was known to be stealing sensitive data for resale.

A competitor had also been attacked at some stage or been associated with one or several

attacks, and had started a rumour about the market leader resulting in the company's market share value falling by 15% in a single day. Following an internal inquiry, it was clear that the data that was hacked related to:

1. data regarding suppliers (e.g., types of contract awarded, penalty clauses and prices paid for example);
2. information about the company's new product development process (e.g., a specific 3D printing technology and intellectual property); and
3. information about the online customer-finance department payment system.

It seemed that large blocks of data relating to existing customers had been obtained (so the competitor could offer better price deals) and establish what type of risk was involved (e.g., this would result in improved risk assessment and risk analysis). In addition, the data obtained relating to the company's new product development process would allow the competitor to circumvent the company's main patent and/or identify the next generation of the technology/application. An internal investigation had also unearthed the fact that some staff had been actively involved in exchanging information with unknown individuals on social websites and as a result two junior members of staff in the organization's design department had been enticed into giving away sensitive data.

The inquiry undertaken by senior managers and the corporate security team within the organization, revealed that the company's website had been infected with malware and those downloading a company brochure had had their details sent secretly to the competitor so potential customers could be easily targeted. This was most disturbing and it was necessary for the legal team to be consulted vis-à-vis possible legal action against the company. Three months prior to this set of events, the IT manager had been asked to undertake a security review of the company's computer systems and networks and an internal report, sent to the company's board had indicated that:

> "The IT manager had been asked to undertake an audit of the company's computer system and network but was reluctant to talk with staff in other departments (especially marketing and finance) because they could not understand the technical aspects of the proposed work. Several influential and knowledgeable people had been excluded from the work because they were either disliked by the IT manager or were thought to have limited intellectual capability and were thought not to be able to understand what was going on. This being the case, it was thought that some staff would not be able to contribute to the study.
>
> On one occasion, the marketing research manager was required to purchase data from an outside market research agency but refused to inform the IT manager about where the data was stored as they were not on speaking terms. It is believed the data was stored with a cloud provider but no record existed of what data or indeed other company data was stored in the cloud".

Additional evidence of mismanagement was also outlined in the report:

> "The Marketing Manager informed his boss, the Marketing Director, that one of the company's suppliers, had informed him, via their Managing Director, that they had heard that they were offering their top suppliers (those with 20% of their business (category A supplier)) a financial incentive to lower costs and gain more

business. This was a surprise to the Marketing Manager because this had only been discussed internally by several senior managers, the Marketing Director and the Finance Director. It seems that either one of the category A suppliers had leaked the information or the teleconferencing facility had been hacked into and rumours circulated for a deliberate reason".

The report continued:

> "This sensitive information or the ability of other suppliers to influence negotiations, was crucial as there was a shakeout in the industry and price cutting had taken hold. The effect would possibly be that lower prices would have to be set; profit margins would be lower, and more emphasis would be placed on promotion and advertising to gain more customers to offset the reduced profitability".

The minutes of a meeting held to discuss the findings of the report suggested that:

> "The consequences for the marketing department were:
> confidential and sensitive data had already been leaked;
> once prices fell it would be difficult to increase them again;
> the public relations department would have to work harder and faster, and would have to embrace digital marketing campaigns to get the appropriate message out to customers and end users faster.
>
> The implications for security were:
> either somebody within the company or somebody within a supplier organization was leaking information;
> the company's marketing data base had been penetrated;
> company passwords had been intercepted;
> a contractor may have stolen and sold sensitive data;
> company representatives or supplier representatives had attended a venue that was electronically bugged;
> a third party (bank) may have released information or a wholesaler or retailer may have done so; and
> a competitor may have deliberately started a rumour to gain insights and information about the company and its relationships with it suppliers".

In addition, those attending the meeting that had discussed the issues and challenges resulting were convinced that:

> "A new information security policy and strategy was needed.
> A risk manager needed to be appointed.
> A risk mitigation strategy was needed.
> The company needed to establish a risk register.
> A new model of risk management was needed.
> The marketing supplier data base needed to be patched".

The report made known the following:

> "It became clear from a board meeting held earlier in the month that the initial report had raised concerns among senior management with respect to how the

> scenario would unfold, and also, how mechanisms could be put in place to produce a receptive and sympathetic organizational culture that resulted in cyber security management processes being implemented that would change the organizational culture for the better. The following question had been posed: How would the scenario play out?"

The head of corporate security had stated at the time:

> "Some of the actions outlined will in actual fact have a very negative impact on the company. What worries me more than anything, is how can we square the marketing situation and ensure that the security consequences do not snowball out of control".

A background company report had been produced one year earlier and had made interesting reading:

> "A small company with 50 employees and 5 directors. Managing Director, Marketing Director, Finance Director, Human Resource Management Director and Technology Director. There was a marketing manager, a marketing research manager, a marketing data base manager, a finance manager, an IT manager, a personnel manager, a technology manager and a research and development manager. The main workforce was employed in marketing and sales work. Immediate problems facing the company were:
>
> *Known threats*
>
> Two non-information security threats were: competitor companies were increasing their market share by (1) introducing new products (4 in the last 12 months) and (2) price cutting (which was attracting price sensitive customers).
>
> *Unknown threats*
>
> A criminal group had attempted to hack directly into the company's bank account to steal money from the company. A son of one of the mangers was downloading games from the Internet on his father's laptop computer which the manager used to take to work and download files and then take them home to work on at the weekend.
>
> A new cleaning company had been hired and one of the cleaners had been paid by a competitor to try and steal a data stick from the company and other information (eg., financial data reports and design work) that was left openly available and unguarded by staff after they finished work for the day.
>
> As well as this, the company was facing a law suit over non-payment of an account, because they said they had not received delivery of a component. When looked into, it was discovered that the component had been signed for by somebody within the company, but the signature did not match a current employee. It was possibly a casual worker employed by the company during a temporary period of high demand and the person(s) no longer worked at the

company. News of this had got out and some existing customers had not renewed their business contracts (e.g., reputational damage).

The marketing director and the finance director had been in discussions with a potential collaborator and had mistakenly provided them (via an email) with the blue print of a new technology the company was developing. The company concerned said that they had deleted the material as a matter of policy but this could not be verified.

It was known that one of the company's suppliers was regularly being subject to power shortages and the electricity supply to the company was disrupted two to three times per month. On one occasion the product produced and shipped to the company was faulty and this had raised concerns that the supplier was not carrying out quality checks. But the company in question had not invested in sufficient quality control (both internally (products made or assembled in-house) and externally (those bought in from external suppliers).

Owing to the fact that the company's sales were declining and the profit margins were being squeezed, rumours had started to surface that the company would go bust and because of this two experienced staff members had left the company and taken up work with other companies. They had taken knowledge about the company and its management procedures with them.

The company's information security system was dated and the manuals relating to the system had been misplaced.

The finance director and his staff undertook risk management but did not talk with staff in other departments. The risk analysis model was statistical in nature and was not that well understand by some managers.

Company staff had not adhered to any industry standard and managed as they considered relevant. There was an ad hoc approach to problem solving and the common message was: "If it is okay leave it. If it is broken fix it. Do not fix it until it is broken".

The IT manager had read about the cloud and said that the company should outsource to a cloud provider the human resource management capability of the company. It was reported that the personal records of staff may be at risk and then staff and the organization would be vulnerable. The IT manager said it should be okay because the cloud provider could take responsibility for managing the situation and they must be responsible for everybody's data".

Recommendation: Research needs to be undertaken to explain how a virtual cyber security emergency planning simulation can be used to train cyber security professionals and those undertaking a training and/or educational programme in the area of cyber security.

A framework for information security modelling

A Petri net is a mathematical modelling tool that has a simple graphical representation. Within the context of security Petri nets have been used in diverse number of ways, ranging

from modelling of cyber-physical attacks on smart grids (Chen et al., 2011), to formal verification of security policies (Huang and Kirchner (2011). We propose to build an information security framework using Petri nets and we provide herewith a brief description of Petri nets before we introduce our framework.

A brief introduction to Petri nets

A Petri net can be conveniently described using its graphical representation (van der Aalst and Stahl (2011). Consider the simple Petri net is shown in Figure 1. The circles denote *places*, inside some of the places there are dots, these are denoted *tokens*. Taken together, the places and the tokens represent the *state* of the Petri net. The rectangles denote *transitions*; it is through the actions of these transitions that the Petri net state can evolve.

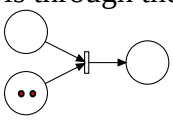


Figure 1 A simple Petri net

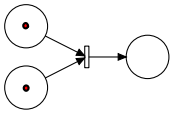
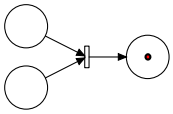


Figure 2 (a) An active transition



(b) Petri net state after the transition has fired

The arcs in the net are directed (they have arrows showing their direction) and these arcs only join a place to a transition (and vice versa). For each transition, we distinguish between places that are connected to it with arcs that are entering the transition (input places) and places connected with arcs exiting the transition (output places). A transition that has at least one token in each of its input places may then *fire*. Firing a transition simply means subtracting one token from each of its input places and adding one token to each of its output places (Figure 2).

From this simple local update rule sophisticated models may be built, which can model processes that involve concurrency and synchronization. However, there are limitations and a variety of extensions to the basic Petri net have been proposed. For our purpose, we propose to build the framework using a *timed* and *coloured* Petri net. This type of net extends the concept of tokens such that they can contain information themselves. Timing allows us to model temporal processes. Indeed it is this type of Petri net that has been demonstrated to be useful for modelling business processes (van der Aalst and Stahl, 2011).

The Petri net framework

Figure 3 shows a representation of the proposed Petri net. Before describing the network in detail, there are two issues we wish to clarify. First the boxes “A” through “E” are not transitions but entire petri nets, henceforth *subnets*. These subnets are plugged into the framework and must conform to certain constraints described below. Second, for technical reasons we would wish to have bi-directional arcs, this allows a subnet the flexibility to remove or replace tokens from input places. However, for ease of exposition we have used dashed arrows to represent these bi-directional arcs. The direction of each arrow allows the

reader to clearly see which places are considered inputs and which are considered outputs from each subnet.

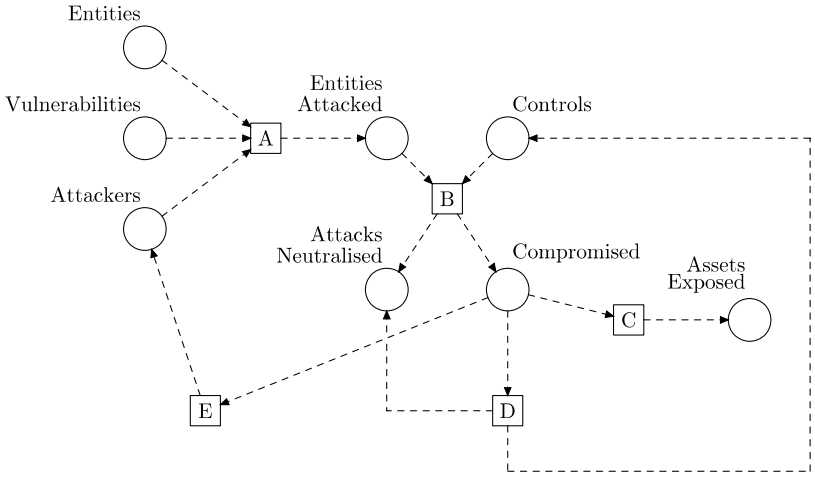


Figure 3 The Petri net Information Security Framework

The subnet denoted "A" (near the top left of the network shown in Figure 3) has three input places:

"Entities" contains (coloured) tokens representing all the possible targets (particular organisations, individuals, etc). Each token has at least a unique identifier, but will typically also contain a record of relevant information regarding the particular entity.

Similarly the place denoted "Vulnerabilities" contains tokens relating to all forms of vulnerability, each token will have at least a unique identifier.

Finally the place denoted "Attackers" contains tokens representing different possible attackers, each with a unique identifier. Maintaining the identity of an attacker throughout the framework is useful for modelling composite (attack tree) style attacks and for being able to introduce into the model the idea that different attackers will have different goals once they have compromised an asset.

Subnet "A" produces new tokens, denoted **attack** tokens, which are a join of the **Entity, Vulnerability** and **Attacker** tokens, (for clarity we use a bold font to identify token types). It is important to note that due to the Petri net's ability to model concurrency; the output of subnet "A" can result in multiple tokens. Hence we can model multiple attacks on multiple entities that are all occurring simultaneously. The output tokens from subnet "A" enter the "Entities Attacked" place. This place represents all the currently active attacks.

Moving on to subnet "B", the input places are "Entities Attacked" and "Controls". The "Controls" place contains tokens representing each control that each entity currently has in place. Each **control** token will have a list of vulnerabilities it covers and a list of vulnerabilities it exposes, along with an identifier for the particular entity. It is the job of subnet "B" to determine if a **control** token exists that has an entity/covered vulnerability component that matches the entity/vulnerability component of the **Attack** token. If an **attack** token is covered by a **control** token, then the **attack** token is moved into the "Attacks Neutralised" place. This particular place allows us to record all successfully defended attacks. If an **attack** token is not successfully covered by a **control** token, this means that the entity has been successfully compromised. The **attack** token is moved to the "Compromised" place.

The “Compromised” place is an input to the last three remaining subnets. We shall describe each of these subnets in turn.

Subnet “E” returns information back to the attacker. At a minimum this can be the fact that the attack was successful, which is useful for modelling the ordering within attack trees. That is to say the attacker can initiate a further attack based on the success of the original attack(s). Subnet “C” is used to determine which assets are exposed given the set of successful **attack** tokens. The output is an **Asset Exposed** token which contains an asset identifier and the relevant attack tokens. (The details regarding assets and the attacks required to expose them is part of the information recorded about an entity.)

Finally subnet “D” models the ability to find and exploit and potentially deal with it, first by neutralising the attack and then by building new controls. It is worth noting that this process of security hardening need not be modelled independently for each entity. Information is typically shared between entities in order to speed up this process.

By probing the state of the framework we can reason about variety of attack scenarios and responses. Cost models can be built on top of this framework by introducing additional information relating to costs such as the cost of exposure of each asset and the cost of maintaining a particular control.

References

Chen, T. M., Sanchez-Aarnoutse, J. C., and Buford, J. (2011). Petri net modeling of cyber-physical attacks on smart grid. *Smart Grid, IEEE Transactions on*, *2*(4), pp.741-749.

House of Commons. (2012). *Malware and Cyber Crime: Twelfth Report of Session 2010-12.HC 1537*. London: The Stationery Office Limited.

Huang, H., and Kirchner, H. (2011). Formal specification and verification of modular security policy based on colored petri nets. *Dependable and Secure Computing, IEEE Transactions on*, *8*(6), pp.852-865.

Thomas, R.C., Antkiewicz, M., Widup, S., and M. Woodyard. (2013). “How bad is it? A branching activity model to estimate the impact of information security breaches”. 12th Annual Workshop on the Economics of Information Security. Washington DC.,: Georgetown University 11th to 12th June), pp.1 to 34.

van der Aalst, W., and Stahl, C. (2011). *Modelling Business Processes: A Petri Net-Oriented Approach.* Cambridge, Massachusetts: The MIT Press.

Winsberg, E. (2003). Simulated experiments: Methodology for a virtual world. *Philosophy of Science*, 70 (January), pp.105-125.

Yao, X., Konopka, J.A., Hendela, A.H., Chumer, M., and Murray, T. (2005). Unleash physical limitations: Virtual emergency preparedness planning simulation training, methodology and a case study. Proceedings of the Eleventh Americas Conference on Information Systems, Omaha, NE (11th to 14th August), pp.1643 to 1652.