Incident Handling: Where the need for planning is often not recognised.

Conference Paper · January 2003

Source: DBLP

CITATIONS
26

READS
174

3 authors, including:

Anthonie Bastiaan Ruighaver

56 PUBLICATIONS **572** CITATIONS

SEE PROFILE

Atif Ahmad

University of Melbourne

81 PUBLICATIONS **909** CITATIONS

SEE PROFILE

Incident Handling: Where the need for planning is often not recognised

Terence Tan
Tobias Ruighaver
Atif Ahmad

Department of Information Systems,
University of Melbourne,
Parkville, Victoria.
cctt@studentmail.dis.unimelb.edu.au
e-mail: anthonie@unimelb.edu.au
e-mail: atif@unimelb.edu.au

Abstract

While vulnerabilities to intrusions in organisations are on the increase, it becomes vital that organizations are able to handle security incidents and undertake security/forensic investigation. These investigations are necessary to identify potential weaknesses in the security and prevent future incidents or to deter future attackers. We performed several case studies to explore what factors have influenced managers in organizations in their decisions not to perform security/forensic investigations. The study identified that not having prior planning for any incident handling and being unaware of the importance to do so are major inhibitors to an organization's ability in reacting to security incidents.

Keywords

Forensic investigations, planning, decision making, management of incident handling

INDTRODUCTION

Current studies in the area of information security and computer crime clearly indicate an increase in the number of attacks on organizations. Research studies performed by the Computer Security Institute (CSI), the Federal Bureau of Investigations (CSI/FBI Survey, 2002) and Auscert (AusCert et al, 2002) have indicated that the level of security incidents (including internal and external attacks) in organizations have risen over the last couple of years compared to earlier studies (KPMG Canada, 1997; KPMG Canada, 1998; The Association of Certified Fraud Examiners, 1996). This increase in attacks coincides with the explosive growth of the Internet and the availability and connect-ability (reach) that it provides (Hafner & Lyon, 1996; Levy, 1984; Bloombecker, 1990).

The likelihood that an organization's information systems are insufficiently secluded and protected against certain kinds of damage or loss, is known as "systems risk" (Straub & Welke, 1998). An underlying problem with systems risk, in the 90's and more so today, is that managers and security personnel are generally unaware of the full range of actions that they can take to reduce risk and to manage incidents. Due to this lack of knowledge in risk management and incident handling, subsequent actions to plan for and cope with systems risk are far less effective than they need to be.

Fortunately, there are a number of well-established behavioural theories and other conceptual models that offer insight into what influences managers in making decisions when dealing with systems risk and incident handling. This is one viable explanation as to why studies by the CSI and the FBI (CSI/FBI Survey, 2002) have shown evidence of a change in the way organizations are choosing to handle security incidents. Organizations are now beginning to realize the importance of having to handle attacks/incidents appropriately and effectively. Likewise, they are beginning to carry out security and/or forensics investigations in order to identify weaknesses in their security, improve overall security, prevent future occurrences, and to prosecute offenders (Braid, 2001; Haugen and Selin, 1999; Theunissen, 2001; Pasikowski, 2001).

However, even with this emphasis on incident handling and security/forensics investigations, the majority of organizations nevertheless continue to react unfavourably to security incidents. That is, they often do not perform any investigations, but simply focus on business continuity (resuming production) (see AusCert et al, 2002: 23; D'Amico, 2002; Braid, 2001). This is not surprising as most firms would rather ignore or take care of security breaches themselves, than report them and risk negative publicity. Further, in certain industries, organizations even fear that the information provided to authorities may be used against them.

This then leaves us with a puzzling picture. On the one hand, attacks on organizations are increasing and hence the emphasis placed on incident handling and investigations are higher. Although we see a higher awareness in

organizations on information security issues, the reality seems to be that many organizations are merely 'paying lip service' and perhaps are not very serious about its execution. Many organizations are ill-prepared for incident handling and/or choose to react to security incidents by focusing not on collecting evidence (forensics or otherwise) or identifying what went wrong but on resuming production as their first and perhaps only priority. So the question then posed is why? What makes these organizations or incident handlers, react in such a contradictory manner to what literature imparts as 'best practice'?

In order to understand these phenomena better, a number of case studies were performed. The primary aim of those studies was to explore the reasons why managers in organizations are not deciding to perform security and/or forensic investigations. In order to understand why these decisions are being made, it was necessary to investigate the managerial decision-making process. A literature search revealed a framework for security risk planning proposed by Straub and Welke (1998) from a decision-making model published by Simon (1960), which we adapted along with Straub and Welke's model for managerial perceptions of security risk. The resulting Incident Handling Management model will be discussed in a later section.

This paper presents the findings and revelations of one of those studies performed – in a company we have called S&B. We decided that S&B is the most appropriate case to illustrating the findings of this study as S&B functions in an environment that conveys high security but yet dissuades "best practice" in handling security incidents.

Our study has been motivated by the actions or lack thereof that organizations are employing in reacting to security incidents. These reactions are mostly unfavourable although the number of attacks on organizations (both internal and external) is on the increase.

Beyond the motivation, the need for this study is justifiable from a few perspectives. Firstly, there is a dearth of literature exploring why organizations do not perform computer forensics investigations. Whilst it can be appreciated that the subject is relatively new in the computer world, the notion of forensics investigations itself is not a new field. There are as yet no strong advocates of this type of investigation, so a research towards this end can contribute significantly to bridging this gap in literature and establishing a realistic need for it.

Secondly, this study is a response to the inability and lack of awareness or understanding that organizations have, with regard to computer forensics investigation procedures and suitable incident handling planning. Organizations need to have sound incident handling plans, guidelines and procedures in place before an incident (see Spruit, 1998; Pham, 2001; Theunissen, 2001). In so doing, organizations would in effect assist incident handlers in applying the appropriate techniques and correct methods in dealing with incidents, and when collecting evidence.

RESEARCH APPROACH

The aim of this study is to explore reasons why organizations are not investigating security incidents. This study further aims at exploring and understanding the influences that different factors have in inhibiting decisions to perform security or forensics investigations in organizations.

To empirically study these propositions and with this exploratory nature in mind, several interpretive qualitative study were conducted, of which we have chosen an organization in the financial services industry to use as an example in this paper. Because security is an extremely sensitive subject for many organizations, firm identity has been disguised. From the standpoint of research design, Stocks & Bonds (S&B) was an ideal organization for this type of study to be performed in. S&B is a reasonably prominent organization in the Australian financial services market and its business involves processing data and marketing this value-added product to customers. Furthermore, S&B has been in the business for many years, has a reasonably stable annual revenue, and information security had been staffed within the IS department for many years. We will discuss S&B in more detail in the following section.

The researchers are aware that although case studies can be used to study decision-making using the 'Incident Handling Management' model as a lens, the results may in fact be difficult to generalize to other companies. To minimize this drawback, multiple cases were performed in the initial study, to allow for theoretical generalisations to be carried out from results of similar cases. As such, the evidence found can be considered more compelling, thus making the overall study more robust (Yin, 1994: 46-48).

The data for this case study was collected between the months of August and September 2002 via semi-structured onsite interviews with open-ended questions. It was supplemented with field notes taken during the visits to the organization. Each interview plan consisted of a substantial mix between open and closed ended questions with the open and creative questions asked in order to take advantage of serendipity, those unexpected factors that have larger implications (Neuman, 2000: 21).

Once data collection was completed, data was organized and structured into a matrix displaying the link between the three constructs and the key incident handling decisions that could be made by the participants:-

(a) ***Reacting to a security incident*** – Emphasis is placed on understanding how the organization's industry and hence the participants distinguish anomalies from security incidents. How are decisions to classify an incident made? What influences these decisions?

(b) ***Performing a security investigation*** – The consideration here is to understand what inhibits incident handlers from conducting a thorough security investigation? What is the primary aim of incident handlers in performing a security investigation and how does this limit their ability or decision to thoroughly investigate?

(c) ***Prosecuting an offender (forensics investigation)*** – Is the organization interested in prosecuting offenders? What inhibits the incident handler's ability to collect forensics evidence? What are the incident handler's objectives in prosecuting an offender?

With all the data now organized, categorized, reduced and tabularized, reflective analysis was then used to gather the real meaning behind the information. In relation to this study, meanings were drawn allowing the researcher to build a logical chain of evidence (Darke et al, 1998: 12) from both participants, as this would assist in corroborating information provided by participants. This approach used primarily intuition and judgement to portray and/or evaluate the phenomenon.

S&B ORGANISATION DETAILS

Stocks & Bonds Limited (S&B) is a financial services organization with a number of offices in Australia and with overseas associates in Europe and Asia. S&B provides investment advice and transaction execution for securities listed on the Australian Stock Exchange (ASX) and on securities listed on approved overseas stock exchanges. S&B markets itself through its unique team of experienced advisors and in-house research members who is both experienced and qualified with an in-depth knowledge and understanding of the markets, industries and companies under their portfolio.

S&B is one of the largest independently owned small to medium enterprise (SME) financial services organizations in Australia with roughly over a hundred personnel. Unlike those SMEs that have IT departments but who outsource their server hosting and various other IT functions, S&B's IT functions are completely operated in-house. At S&B, they have their own networks, servers, communications, back-up equipment, access control systems, monitoring software and so on.

Being in the financial industry a number of conditions and requirements are laid out for S&B. In particular is the security requirement mandated by Federal law for organizations involved in financial services.

"We operate under an Act of Parliament which is monitored by the Australian Securities and Investment Commission; the level of legal requirements is the highest… for operating in the financial area" (Michael, General Manager)

The main participants from S&B who were involved in this study were Michael the General Manager (GM) and Robert the IT Manager (ITM). Michael's responsibility as the GM lies in overseeing the organization's overall operations. He is responsible for ensuring that the organization function smoothly, continues to be profitable and competitive and operates in accordance with the rules and regulations set forth by the Australian Securities and Investment Commission (ASIC).

From an operational perspective, these include matters like following correct procedures in selling and buying shares, right down to the security aspects, including the types of software that can be used and the minimum level of physical and information security that need to be in place. As such, Michael feels that the organization and the industry, is already secure and has the highest security standards.

"…the systems are of such a nature… they are the most secure systems we have in Australia… the security system is of the highest possible level."

Robert, as the IT Manager is solely responsible for the organization's internal and external networks; communications and connections (e-mail, internet connections, connections with the ASX, etc.); local systems and hardware (PC's, servers, printers, etc.); software (financial software, trading software, banking software, etc.); database (client information, etc.), and the list goes on. For S&B to be competitive, efficient and responsive, it carries out many of its business functions online and this adds additional responsibilities and pressures on Robert to ensure that the day to day running of the organization's systems, networks and so on, are available (up-time of the server), consistent and reliable (integrity).

Due to Robert's position and responsibilities as the IT manager, any incidents related to the information systems of S&B will be relayed to him as the first response to the incident is his responsibility. Furthermore, Robert feels that security is unquestionably a necessity given the industry and the business. To him, it is a critical component of the operations of S&B.

"Definitely!! Security of the data. . We are holding client's personal information and wealth so security of the data is paramount"

From a skills perspective, both Michael and Robert lack any formal training in incident handling, security investigations and/or computer forensics. For both of them, their awareness, understanding and familiarity with information security, computer forensics, incident handling and other related issues are purely from experience.

"Ah minimal myself, I have been in companies in which we have to have it so obviously in a management environment you'll always know a little bit about security." [Michael's Reply]

and

"No, just a little at the hotel and the school [*referring to previous places of employment], I was doing [information] security there"* [Robert's Reply]

THE 'INCIDENT HANDLING MANAGEMENT MODEL

In order to fully understand managerial decision-making and the perceptions that might influence it, Straub and Welke's (1998) model of managerial perceptions of security risk was adapted. This model was originally designed to analyse [managerial] decision making related to security risk and in particular, managerial concern about the organization's security based on three underlying components of risk: organizational environment, information systems environment and individual characteristics (Straub & Welke, 1998; Simon, 1960).

Although not focused on security risk, this same model, with a few modifications may be adapted for this study by offering insights into how managers make decisions and cope with security incidents. The modified model was similarly useful in guiding the analysis of the results and in structuring the discussion of the results with the three decisions that can be made in relation to incident handling being discussed with relation to the three underlying components of risk.

Figure 1, the 'Incident Handling Management' model, is a result of synthesizing Straub and Welke's (1998) perceptions to security risk model with possible organizational reactions to security incidents.

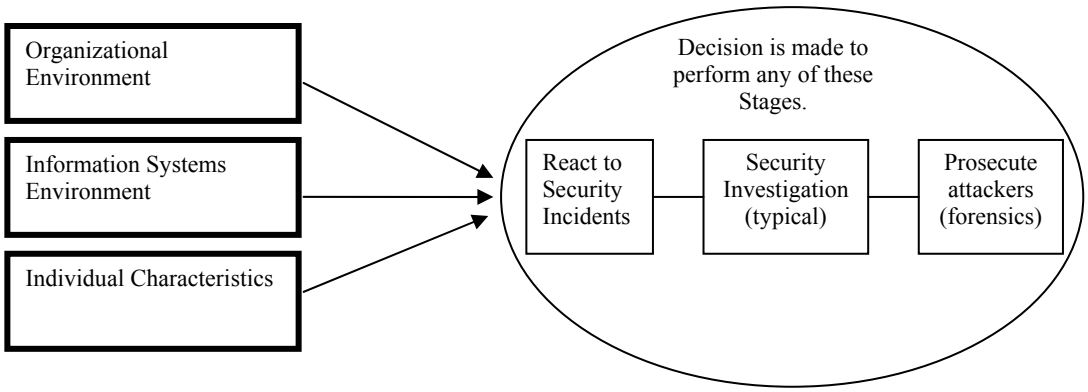

Figure 1: "Incident Handling Management" Model

The first piece of the model relates to those risks inherent in the industry or environment that the organization is in. For example, we would expect a manager in the banking industry to express more concern about security incidents and react by investigating and prosecuting. This is so as the banking industry faces a high industry risk and a higher potential gain for perpetrators to illegally disclose, modify and/or destroy the organizations assets.

The second piece of this model, "Information System (IS) Environment", reflects the actions already taken by an organization to protect the organization's information assets. For example, in an organization that has invested extensive amounts of resources towards providing a high level of security, the model predicts that management would perceive the organization to be highly secure and hence would possibly not react to a security incident as they would have a lower perceived security risk.

The last construct of the model, "Individual Characteristics" specifies that a manager's awareness and knowledge of security investigations will be a major factor influencing their decisions. With regards to this study, managers with a background in law enforcement/security and/or have had some exposure to security

issues are expected, are more likely to react to security incidents, investigate and follow through with prosecution.

SECURITY INCIDENTS & INCIDENT HANDLING

Before proceeding on to the case, a number of important issues related to incident handling needs to be discussed. This quick introduction to the intricacies of effective incident handling will not only be informative, but will also allow the reader to fully appreciate the mistakes that S&B has made in preparing itself and it's employees for incident handling.

In most organizations, resources are limited. As such one of the most important aspects to effective incident handling is the ability to not waste resources on "non-incidents". The question then asked is when is an incident an incident?

Theunissen (2001) indicates that "anomalies" can be extremely visible and disruptive, such as a widespread virus outbreak, or entirely unnoticed but extremely damaging such as loss of confidential customer information. According to Spruit (1998) and Pasikowski (2001), security incidents often occur due to a concurrence of circumstances. For example, individuals may make decisions or perform actions that seem to be correct yet lead to a security breach nevertheless.

Security incidents then can be defined as an unintended disruption or complication which results in the disability, discontinuance or cost (monetary, "face value", etc) to an organization (Theunissen, 2001; Pasikowski, 2001; Spruit & Gerhardt, 1997). These incidents are usually caused by a combination of small 'anomalies'. Incidents strangely have a knack of occurring at the least convenient time and when the right people are not available (Spruit, 1998; Pham, 2001). For these reasons, it is important to have well documented incident handling plans and procedures in place before an incident.

Incident handling procedures allow the organization and particularly those handling the incident to know what to do (Osborne, 2001). For most organizations, anticipation of scenarios before they happen is crucial as this allows for decisions to be made about them in advance (Pham, 2001). For instance, simply deciding who to tell when an incident occurs can be hard to decide as some things are confidential and should be kept at the strictly 'need to know' principle (Theunissen, 2001). Other incidents may require support staff to respond quickly and this in turn brings up issues such as after hours support, overtime and personnel to be on call. An organization dealing with an incident may need external support, which costs money and takes time and effort to select appropriate partners.

Similarly, incident handling guidelines assist in situations whereby the potential for prosecution of an offender may occur (Sommer, 2001; Pham, 2001; Saudi, 2001; Pasikowski, 2001; Osborne, 2001). Depending on the level of intrusion and corresponding criticality (eg. using a 'ladder of escalation'), an organization may decide to perform a forensic investigation (Osborne, 2001). Briefly, a forensic investigation will allow the affected organization to gain a better understanding of the intrusion and the attacker (Sommer, 2001). Lunn (2001) and McKemmish (1999) further add that this investigation process may result in a great deal of new information being learnt/gained. Such information includes security vulnerabilities that exist, any changes to be made to the systems and/or applications, identification of the source(s) of the attack and methods of information disclosure, including acts of espionage (also see Sommer 1997 & 2001; Osborne, 2001, Braid, 2001; D'Amico, 2002).

Generally, organizations must be prepared to prosecute whenever an attack occurs and this information has to be outlined in their incident response plans/procedures before the attack occurs. If and when an incident arises, the organization will be prepared to handle the incident, and possibly pursue legal action if required. This early preparation is important as it does no good if an organization which had continued the process of resuming production (recovery) decides halfway through that they want to investigate and to prosecute instead. Furthermore, authors on incident handling agree that by having high-quality incident handling plans, organizations can learn from incidents (see Sommer, 1997; Lunn, 2001; Smith, 1998; D'Amico, 2002). This will greatly facilitate the organization in reducing the likelihood of an incident from reoccurring and improving their security overall.

THE CASE – S&B

Reacting to Security Incidents:

The analysis indicates that at S&B, decisions on classifying anomalies as incidents and actions in dealing with those incidents have not been made beforehand. As such, the decision making process of reacting to security incidents have been severely inhibited. Specifically, these decisions have been inhibited by:-

(a) An extremely regulated industry which penalises organizations heavily for security incidents which in turn leads to difficulties/differences in classifying anomalies as security incidents (Organizational Environment).

(b) A lack of preparation and planning in defining and dealing with security incidents by the organization (IS Environment).

With reference to the 'Incident Handling Management' model, it is evident that the organizational environment and the IS environment that S&B operates in contribute to inhibiting the participant's ability to react to security incidents. Individual characteristics on the other hand have been seen to be less of an influence/inhibitor.

Organizational Environment – S&B

At S&B, no clear definition or any clear guidelines on what a security incident is has been provided and hence there is no understanding by participants on what a security incident is. According to Michael, the way the industry and hence himself, distinguishes security incidents from anomalies is when there is a financial benefit to someone other than the client or company.

"…the way we look at it is to ultimately define who the beneficiary of the deed was. Is there a financial benefit to someone? ….in our industry, we define it as a financial benefit."

In contrast, Robert categorizes an anomaly as a security incident when:

"…client or staff information is compromised."

Furthermore, S&B operates in an extremely regulated industry with an extensive number of conditions and operational rules and guidelines. Interestingly, this same environment has inadvertently inhibited the participants' willingness to defining anomalies as incidents, as incidents have to be investigated and reported.

"…we can say it may not be in our best interest to involve statutory bodies in the investigation… there are quite high penalties levied against the company for breaches, we would try to resolve the situation without bringing in other bodies if we could." [Michael's Reply]

and

"...the trouble is if we report, we tend to get a very heavy fine. So we tend to, try to remedy the situation without ever reporting it." [Robert's Reply]

These differences in opinion of both participants in classifying security incidents may lead to a variation as to what anomalies are reacted to and hence classified as incidents and what anomalies are simply 'shrugged off'. This difficulty on its own proves to be an inhibitor to the participants making a decision to react to a security incident. Further analysis of the organizational environment indicates it is highly improbable for the participants to classify an anomaly as an incident. Otherwise, then the incident has to be investigated and reported resulting in the organization receiving a hefty fine. Hence this too will be an inhibiting factor to the participant's decision of declaring something an incident and then having to follow through on it. In fact, it is more likely that the participants will decide instead on resuming production.

Information Systems Environment – S&B

Apparently, the lack of planning and preparation of procedures and documentation in the IS environment has also severely inhibited the participants' abilities to react to security incidents.

"No, ah you can talk to the other guy about that, we probably have some procedure in place if something goes wrong like that…" [Michael's Reply]

and

"No, I'm in the process of doing that now [referring to developing incident handling guidelines]*"* [Robert's Reply]

Without proper and well-documented incident handling guidelines to assist the participants in classifying security incidents, evidence was found indicating that the participants instead were looking into (investigating) anomalies in order to classify them as incidents.

"I wouldn't say initially that that would be an incident, I'd say it would be a worry and investigate it and then possibly define it as an incident." [Robert's Reply]

and

"We have internal controls in the systems which help us monitor…we have an alarms program which 'flags' things done out of the ordinary. Now that might be ok when we have a look at it, but it might not." [Michael's Reply]

Due to the fact that no formal procedures, policies or guidelines exist, when faced with an anomaly, both participants will likely decide to react in different ways. Similarly, without incident handling procedures identifying the 'ladder of escalation' of an anomaly, the likelihood that participants will classify an anomaly as an incident is low, hence reaction to it will be slow. Then again, as shown above, these decisions to react only occur when an anomaly has been classified as an incident through an investigative process further inhibiting decisions to react quickly to an incident.

Performing a Security Investigation:

Once an anomaly has been classified as a security incident, according to the Securities Act (Government Law), it has to be reported and investigated. Referencing the 'Incident Handling Management' model, and based on evidence from the data collected, two inhibitors to the participants performing security investigations appear to be evident:-

(a) A time issue that places emphasis on recovery (organizational environment).

(b) The organization's failure to understand the benefits of performing a thorough security investigation (IS environment).

Organizational Environment – S&B

At S&B, in terms of investigating security incidents, participants are inhibited by a time constraint. In the financial industry, once an incident has been declared, the organization's systems are isolated instantly and the business comes to a halt. Michael and Robert informed that the investigative process then has to be quick and recovery essential:

"…if anything happened in our system, our system would be isolated instantly…under an Act of Parliament, if we can't do things within 24 hours, we must close our business…it is inconvenient when things go wrong but we can instantly set up business at another site very quickly." [Michael's Reply]

and

"…if a bomb exploded on this floor, we could set up business across the road within an hour…just reinstall the backups the night before." [Robert's Reply]

At S&B, some anomalies cannot be ignored and have to be declared as a security incident. Once declared however, the organization is required by law to report and investigate it. These are all conditions set out by the financial industry, which then further dictates that if the organization cannot resume operations within a limited time then the organization must 'shut down'. This condition will obviously place a huge amount of pressure on the participants to complete the investigative process quickly and to resume operations (concentrate on resuming production) hence inhibiting the investigation. It is also evident that the participants are unaware of the benefits of the investigative process and that the investigation does not just stop once recovery has been completed but may still continue and that this can offer a number of benefits after recovery. For example, lessons learned from the findings of the investigative process may lead to improved security.

Information Systems Environment – S&B

Due to the lack of planning and guidelines on incident handling, participants at S&B are under the impression that investigating security incidents are to find out what happened, to fix the problem and possibly to identify the attacker. When asked what they hoped to achieve from investigating security incidents, their reply was: -

"…to find out what happened, how it happened and then who did it." [Robert's Reply]

and

"To sack the guy! Pure and simple. Instantly." [Michael's Reply]

From the participants' responses, it can be deduced that their awareness of the benefits of performing a security investigation is limited. Within their IS environment, participants are neither aware nor encouraged to view security investigations as a means to improving the organization's overall security.

As can be seen, the IS environment at S&B has inhibited the participant's ability and hence the organization's ability to obtain all the benefits from the investigative process by failing to inform and educate the participants as to the benefits of a security investigation. In retrospect, the participants will instead be performing security

investigations to simply find the cause of a problem and fix it quickly so that business continuity may be preserved.

Prosecution of Offenders (Computer Forensics Investigations):

Evidence from the two participants indicates a willingness to consider prosecution. However, as with the other two incident handling decisions recognised in the model, a number of inhibitors exist, hampering the participant's ability to carry out forensics evidence collection (computer forensics investigation) thus hindering the organization's ability to prosecute. These inhibitors are derived from the organizational environment, the IS environment and the participants' individual characteristics and include: -

- Penalties by the industry which places emphasis on cost versus benefits (organizational environment).
- Failure of the organization to identify the full benefits of prosecution, such as using prosecution as a deterrent to other potential attackers (IS environment).
- Lack of expertise, knowledge and experience with computer forensics investigations (Individual characteristics).

Organizational Environment – S&B

Similar to the way in which the organizational environment inhibits the participants in reacting to an incident, the organizational environment also inhibits the participants' decisions to prosecute offenders. The organizational environment penalises the organization for incidents, and as the incident appears more serious, this penalty is similarly amplified. As such, participants have expressed that they will consider prosecution only after considering the costs:-

"Depending on what the damage done and the value of the damage… We wouldn't do it for five thousand dollars; we wouldn't do it for ten thousand dollars…maybe if it was a hundred or t\who hundred thousand dollars we might consider prosecution." [Michael's Reply]

and

"We will weigh up our cost. What it costs us to our rewards…" [Robert's Reply]

Information Systems Environment – S&B

Participants at S&B expressed the view that the importance of collecting forensics evidence and prosecution of offenders is to punish the offender for 'hurting' the organization. With the lack of guidance from the IS environment, participants were similarly not fully aware of the intangible benefits of prosecution such as using prosecution as a deterrent to future attackers. Evidence instead indicates that apart from issues of cost (mentioned above) the participants will consider prosecution to punish an offender if they have harmed the organization:

"…If they destroyed our systems, we mightn't be so lenient in our views… they would cause major disruptions to our business and I don't think we would be that lenient." [Michael's Reply]

and

"We will prosecute anything that is a breach…something's monetary values can't fix [referring to cost of prosecuting offenders]. *So it doesn't matter."* [Robert's Reply]

The participant's lack of awareness with regard to the benefits of prosecuting offenders (eg, as a deterrent to future attackers) is evident due to the lack of guidance offered by the organization. The IS environment has obviously inhibited the participants' likelihood to collect evidence and prosecute offenders if the crime was not all that serious. By understanding that prosecuting offenders may act as a warning/deterrent to other possible attackers, the organization may in fact benefit from fewer future attacks and a better awareness of security in general. However, due to the state of the IS environment, this is not to be so. Similarly, because of difficulties in defining security incidents, evidence that may be crucial to the forensics investigation will not get collected as investigations are only performed after an anomaly has been deemed an incident. Again, potentially crucial evidence may be lost and or corrupted by the time the investigative process commences and forensics evidence is collected.

Individual Characteristics – S&B

Michael and Robert lack any formal training in forensics investigations and as such are not fully aware of the processes and procedures that are involved. To the participants, the aim of a forensics investigation is:

"…to get to the bottom of how it is and what happened and fix the loop hole that created it, not necessarily go after the person that did it." [Robert's Reply]

and

"I don't think it's the ability to prosecute, that's not why you bring them in…you want to find out how, why, when to fix it…." [Michael's Reply]

From our understanding of computer forensics we can see that what the participants are describing is not a computer forensics investigation but a typical security investigation with emphasis being placed on fixing the problem quickly. Once the problem is fixed, according to Michael, "you can go after whom." It is obvious that their lack of training, education, awareness and experience in this area of information security will inhibit their ability to prosecute an offender. It is evident that the participants are unaware that in a forensics investigation, evidence must be collected before the decision to prosecute. In this respect, actions taken by the participants for what they believe is a computer forensics investigation may inadvertently destroy or contaminate evidence. Similarly procedures used by the participants in collecting evidence may not be the most appropriate procedures leading to evidence being legally inadmissible and the organization unable to prosecute.

CONCLUSION

This study has focused firstly on managerial perceptions related to incident handling and computer forensic investigations. It has then broadened its scope to include any other pertinent factors. In order to explore these areas, multiple case studies were performed of which one is presented in this paper – S&B.

From the investigations, it was clear that S&B had not performed any prior planning in relation to incident handling. In fact, further analysis indicated that the organization was unaware of the need to do so. As such, many anomalies will not be classified as security incidents and even if it were, reactions to incidents would be slow and as a result, valuable time, evidence and forensic data will be lost.

The study suggests that it is vital that management recognises there is a need to distinguish anomalies from security incidents, and following that to carry out evidence collection and appropriate investigations, whether to simply identify how the attackers 'broke in' (typical security investigation), or at a later point in time, to have the ability to identify and prosecute the offenders (forensics investigations).

It was also found that S&B expressed a willingness to investigate incidents and consider prosecution of offenders. However decisions to prosecute only came if the typical ad-hoc investigative process had identified someone to punish and if prosecution of the perpetrator is expected to provide tangible benefits. This obvious lack of planning and awareness of the importance of making decisions before an incident has proven to be a major inhibitor of security/forensics investigations in S&B. Hence, although our research indicates that the organizations are willing to investigate incidents; these organizations still have a lot to do and prepare in order to be fully competent in responding to incidents.

REFERENCES

AusCert, New South Wales Police and Deloitte Touche Tohmatsu (2002), 2002 Australian Computer Crime and Security Survey, Australian Computer Emergency Response Team (AusCert). (Online), <Available: http://www.auscert.com.au/render.html?it=2001> Date accessed: 13/10/2002

Bloombecker, B. (1990), Spectacular computer crimes: What they are and how they cost American business half a billion dollars a year, The Internet book (2nd edition), Upper Saddle River, NJ: Prentice Hall

Braid, M. (2001), Collecting Electronic Evidence after a System Compromise, Australian Computer Emergency Response Team (AusCert). (Online), <Available: http://www.auscert.org.au/Information/Collecting_Evidence_After_A_System_Compromise.htm> Date accessed: 26/3/2002

Computer Security Institute and Federal Bureau of Investigations Survey (2002), Results of 'CSI/FBI Computer Crime and Security Survey', (Online), <Available: http://www.gocsi.com> Date accessed: 6/10/2002

D'Amico, E. (2002), Cyber Crime is on the rise, but let's keep it quiet, Chemical Week, Vol 164, No. 17, 24-27

Darke, P., Shanks, G., and Broadbent, M. (1998), Successfully Completing Case Study Research: Combining Rigour, Relevance and Pragmatism, Information Systems Journal, Vol 8, 273-289

Hafner, K. and Lyon, M (1996), Where Wizards Stay Up Late: The Origins of the Internet, Simon & Schuster, New York

Haugen, S. and Selin, J. R. (1999), Identifying and controlling computer crime and employee fraud, Industrial Management and Data Systems, Vol 99, No.8, 340-346

KPMG Canada (1997), 1997 Fraud Survey Report, (Online), <Available: http://www.kpmg.ca/isi/vl/fsur97e.htm> Date accessed: 3/4/2002

KPMG Canada (1998), 1998 Fraud Survey Report, (Online), <Available: http://www.kpmg.ca/isi/vl/fsur98e.htm> Date accessed: 3/4/2002

Levy, S. (1984), Hackers: Heroes of the computer revolution, Dell Publishing, New York

Lunn, A. D (2001), Computer Forensics – An Overview, The SANS Institute. (Online), <Available: http://rr.sans.org/incident/forensics.php> Date accessed: 24/3/2002

McKemmish, R (1999), What is Forensic Computing? Australian Institute of Criminology - trends & issues in crime and criminal justice, No. 118

Neuman, W. L. (2000), Social Research Methods - Qualitative and Quantitative Approaches Fourth ed. Boston, Allyn & Bacon.

Osborne, T. T. (2001), Building an Incident Response Program To Suit Your Business, The SANS Institute. (Online), <Available: http://rr.sans.org/incident/program.php> Date accessed: 10/2/2002

Pasikowski, G. T. (2001), Prosecution: A subset of Incident Response Procedures, The SANS Institute. (Online), <Available: http://rr.sans.org/incident/prosecution.php> Date accessed: 13/8/2002

Pham, C. (2001), From Events to Incident, The SANS Institute. (Online), <Available: http://rr.sans.org/incident/events.php> Date accessed: 13/8/2002

Saudi, M. M. (2001), An Overview of Disk Imaging Tool in Computer Forensics, The SANS Institute. (Online), <Available: http://rr.sans.org/incident/disk_imaging.php> Date accessed: 28/8/2002

Simon, H. A. (1960), The New Science of Management Decision, Prentice-Hall Inc.

Sommer, P (1992), "Computer Forensics: an Introduction" Compsec 1992, Elsevier, 1992.

Sommer, P (1997), Computer Forensics: An Introduction, (Online), <Available: http://www.virtualcity.co.uk/vcaforens.htm#history> Date accessed: 20/8/2002

Sommer, P (1998), Intrusion Detection Systems as Evidence, RAID 98.

Spruit, M. E. M. and Gerhardt, W. (1997), Information Security and The Significance of Organization, First ACM Workshop on Education in InfoSec, Monterey

Spruit, M. E. M. (1998), Competing Against Human Failing, The IFIP TC11 14th International Conference on Information Security (IFIP/SEC'98), Vienna/Budapest

Straub, D. W. and Welke, R. J. (1998), Coping with Systems Risk: Security planning models for management decision making. MIS Quarterly, Vol.22, No. 4, 441-469

The Association of Certified Fraud Examiners (1996), Report to the Nation on Occupational Fraud and Abuse, Austin, TX.

Theunissen, D. (2001), Corporate Incident Handling Guidelines, The SANS Institute. (Online), <Available: http://rr.sans.org/incident/corp_guide.php> Date accessed: 13/8/2002

Yin, R. K. (1994), Case Study Research: Design and Methods, Sage Publications, Thousand Oaks, CA.

COPYRIGHT