Available online at www.sciencedirect.com

SciVerse ScienceDirect

journal homepage: www.elsevier.com/locate/cose

Computers & Security

Incident response teams – Challenges in supporting the organisational security function

Atif Ahmad [a,*], Justin Hadgkiss [a], A.B. Ruighaver [b]

[a] Department of Computing and Information Systems, University of Melbourne, Australia
[b] School of Information Systems, Deakin University, Melbourne, Australia

ARTICLE INFO

Article history:
Received 12 February 2012
Accepted 9 April 2012

Keywords:
Information security
Security management
Incident response
Security models
Organizational processes
Security learning

ABSTRACT

Incident response is a critical security function in organisations that aims to manage incidents in a timely and cost-effective manner. This research was motivated by previous case studies that suggested that the practice of incident response frequently did not result in the improvement of strategic security processes such as policy development and risk assessment. An exploratory in-depth case study was performed at a large global financial institution to examine shortcomings in the practice of incident response. The case study revealed the practice of incident response, in accordance with detailed best-practice guidelines, tended to adopt a narrow technical focus aimed at maintaining business continuity whilst neglecting strategic security concerns. The case study also revealed that the (limited) post-incident review process focused on 'high-impact' incidents rather than 'high-learning' (i.e. potentially useful incidents from a learning perspective) incidents and 'near misses'. In response to this case study, we propose a new double-loop model for incident learning to address potential systemic corrective action in such areas as the risk assessment and policy development processes.

1. Introduction

Many organizations retain an incident response capability to address information security attacks. The response process consists of preparation for, identification, containment, eradication and recovery from incidents. Responsibility for this function typically lies with a computer security incident response team (CSIRT) that is part of a multi-layered approach towards protecting business information assets. Among the many motivations for the existence of such teams is the increasing numbers of security incidents as well as the realization that specialist skills are required in managing incidents. Within organisations, CSIRTs are often seen as 'fire-fighters' (Jaikumar, 2002) since their overt function is reactive – responding to intrusions and other such security incidents in order to minimize the effects of attacks and managing a successful recovery (van Wyk, 2001; Wiik et al., 2005).

Much incident response literature consists of industry white papers that outline recommended (technical) practices for implementing an incident response capability in organisations. For example, best-practice guidelines provide detailed step-by-step procedures and actions to handle incidents (SANS, n.d.; NIST, 2008). In particular, identification of new attack types and corresponding responses attract particular interest (Mitropolous et al., 2006; Novak, 2007). The fact that incident response research focuses on a technical view and gives relatively less attention to holistic socio-organisational perspectives is consistent with trends in information security research as a whole (Dhillon and Backhouse, 2001; Siponen, 2005; Zafar and Clark, 2009). Recently though, some research

* Corresponding author.
E-mail addresses: atif@unimelb.edu.au (A. Ahmad), justinh@unimelb.edu.au (J. Hadgkiss), tobias@deakin.edu.au (A.B. Ruighaver).
0167-4048/$ – see front matter © 2012 Elsevier Ltd. All rights reserved.
doi:10.1016/j.cose.2012.04.001

has been published by Werlinger et al. (2010) that considers the (technical) incident response process from a broader perspective by examining tasks, skills, strategies and tools employed by practitioners in their diagnostic response.

However, despite some researchers exploring less traditional angles on the incident response process, there remains little research on the interface between CSIRTs and the greater organisational environment, in particular during the 'lessons learned' phase. In this phase issues arising from the recent experiences of personnel are discussed with a view to improving the overall incident response process. There is some literature that highlights the importance of this phase in the overall incident response process. Tan et al. (2003) emphasises the need for organisations to establish learning practices, whereas West-Brown et al. (2003) suggest that the lack of literature on lessons learned may be due to the difficulty in gaining access to potentially sensitive organisational information. However, even in this area most advice is based on anecdotal evidence (Wiik et al., 2005) and comes from industry white papers and other industry guides.

For the preceding reasons this paper explores issues facing incident response teams that affect the greater organisational security function. The paper begins with motivations the authors had in conducting this research followed by background on the incident response process. An in-depth case study is presented featuring two kinds of incident response teams operating within the same environment. A discussion follows that explores organisational issues arising from the response process. The paper concludes by discussing the shortcomings in organisational learning and presents a model designed to address the identified learning issues.

2. Background and motivation

The motivation for this research began with multiple case studies on the reporting of incidents in medium to large organisations in the Australian financial sector. The organisations in these case studies were chosen on the basis that they were likely to be represent similar organisations in the financial sector. From this study we noted that although senior management declared a willingness to investigate incidents, there were a number of factors that discouraged formal reporting. These included potential impact on reputation as well as financial penalties and onerous follow-up procedures applied by regulators as a consequence of incidents. Therefore, organisations that participated in this study classified incidents as 'anomalies' until a decision was made to prosecute an individual or if prosecution provided tangible benefits to the organisation. Unfortunately, as a result of not reporting incidents, key security lessons were not identified in the formal investigation and follow-up phases implying the organisation was not learning from its security experiences.

A second series of case studies were performed in three medium to large organisations which consisted of a utility company, a state government department and a local government organisation (Shedden et al., 2010). The aim of this research was to examine how organisations conduct information security risk assessments using standard methodologies and why they choose to conduct these assessments in their particular ways. During this research it was noted that from an incident response perspective, risk assessment processes in the organisations were not informed by data on previous incidents including impact and probability of occurrence. This was an important outcome because security assessment relies heavily on estimation of probabilities and impacts of potential hazards which would benefit from a history of past incidents. This study revealed the lack of communication between related security functions in the organisation which, once again, implied that organisations were not using their security experiences to best advantage.

This paper reports on a third series of case studies (one of these will be presented in this paper) which have been motivated by our observations from previous studies. That being the proposition that security incident response, like security risk management, is being conducted in an insular environment where organisations are not using their incident response function to best advantage.

3. Incident response teams: handling security attacks

An information security incident occurs when there is a direct or indirect attack on the confidentiality, integrity and availability of an information asset. Such incidents can include attacks such as malicious software, theft of information, the loss of power and supporting utilities and information leakage (Ahmad et al., 2005; Whitman and Mattord, 2005). It is inevitable at some stage that organisations will suffer an information security incident. Such an incident may result in multiple negative impacts, such as a loss of company reputation and customer confidence, legal issues, a loss of productivity and direct financial loss (Alberts and Dorofee, 2004).

The main aim of an incident response team is to mitigate the impact of a potential major incident. Many large international organisations see an incident response team as a crucial element of their information security portfolio (Killcrece et al., 2003a). At its most basic level, incident response teams may be purely reactionary, with the team forming together in an adhoc fashion once an incident has been detected. However, more advanced computer security incident response teams tend to adopt a proactive role, seeking out vulnerabilities before they become incidents (Smith, 1994) and provide advice and educate employees on information security matters (Killcrece et al., 2003a).

Kossakowski et al. (1999) identify three main areas of recommended practice for incident response teams: preparing; handling; and follow-up, as listed in Table 1.

The focus of this study is on the 'follow-up' category, where learning and information dissemination occur. Conducting an incident follow-up means sacrificing short-term goals (such as correcting technical incidents) for long-term goals (such as implementing an improved incident tracking system; (Wiik et al., 2005)). This may include performing a post-mortem, hardening systems and updating incident response policies and procedures (Killcrece et al., 2004).

Incident response literature places great importance on the post-incident learning (Killcrece et al., 2003b). However, compared with the level of detail devoted to technical

Table 1 – Summary of recommended practices (Kossakowski et al., 1999).

Category	Recommended practice
Prepare	1. Establish policies and procedures for responding to intrusions 2. Prepare to respond to intrusions
Handle	1. Analyse all available information to characterize an intrusion 2. Communicate with all parties that need to be made aware of an intrusion and its progress 3. Collect and protect information associated with an intrusion 4. Apply short-term solutions to contain an intrusion 5. Eliminate all means of intruder access 6. Return systems to normal operation
Follow-up	1. Identify and implement security lessons learned

improvements, there are few clues as to how this process should actually be implemented. Tan et al. (2003) have found that "many organisations are ill-prepared for incident handling and/ or choose to react to security incidents by focussing not on collecting evidence … but on resuming production as their first and perhaps only priority". This study emphasised the need for organisations to learn from security incidents. Incident response teams should be "a key player in providing risk data and business intelligence to the organisation, based on the actual incident data and threat reports they receive. This information can then be used in any risk analysis or evaluation" (Killcrece et al., 2003a).

4. Security incident response: an exploratory case study

Our research used an exploratory multiple case study approach, with interviews as the primary method of data collection, using documentary evidence to support our findings. Our aim was to provide a deeper understanding and description of information systems practice within this field (Shanks et al., 1993; Walsham, 1995; Darke et al., 1998). Case studies were selected due to their excellence in studying information systems phenomena in-situ and their allowance for in-depth exploration of new contexts and phenomena (Benbasat et al., 1987; Yin, 2003).

This case study is one of three exploratory studies performed by the authors to evaluate issues faced by incident response teams that affect the greater organisational security function.

4.1. *The FinanceOrg case study*

FinanceOrg is a large global financial services organisation with offices on four continents. The organisation conducts a wide range of financial transactions and investments to both consumer and corporate clients. FinanceOrg has over 20,000 employees around the world, and well over a million customers. As a major financial services organisation, its incident response process is subject to compliance regulation through Basel II and Sarbanes Oxley. Therefore, all incidents have to be assessed and reported. Being a publicly listed financial institution, the security of financial and customer information is of paramount concern. High-reliability is essential, as if systems go down, the organisation does not make money. The organisation is hierarchical, with a strong base of middle and executive management.

Information security is governed globally by the Information Security Department. Personnel in this department report to the Chief Information Security Officer (CISO) who, in turn, reports to the Chief Information Officer (CIO). A separate department, located in a different building, is dedicated to Business Continuity. Both areas are funded by a set annual charge from each of the business departments, based on their size. Each of the business areas has an assigned Information Security and Risk Manager that (officially) resides in the Information Security Department.

Risk is governed from the Information Security Department, but each business assesses and manages its own technical and process risk. Risk assessment data is stored in local databases within the different business areas, and collated monthly by the information security department. Business areas are responsible for managing their own risks, and their level of exposure is monitored at an enterprise-wide level. All incidents must be recorded in the business department's risk database.

Security policy and procedure documentation exists on two main levels. General security policy documents are written from the Information Security Department whereas technical teams write their own policies based on the framework the general policies provide. The Information Security Department enforces governance for this. If security policies are broken in a business area, for example, it is the responsibility of the business to enforce that policy, but advice and recommendations are provided from the Information Security Department.

4.2. *Incident response structure and reporting*

Incidents are reported through the organisation's helpdesk. An incident tracking system is used to monitor and log the progress of information security incidents. The system facilitates communication between the technical teams about their activities, and provides a timeline of activities and chain of evidence for incident handling. Incidents are classified by the level of impact they have on the organisation. High-impact incidents are classified as such because of their criticality to the organisation's ability to function, high level of risk, customer impact, and financial considerations. Low-impact incidents are those that have more of an internal focus, do not have a direct customer impact, and are lower risk.

The Network Incident Response Team (NIRT) team of four resides in the Information Security Department. The team work full-time in an incident response capability, and the size of the team is fixed. Their role is to ensure that the core network at FinanceOrg is protected at all costs. The NIRT deal with both low- and high-impact incidents using the ITIL and ISO17799 frameworks. The NIRT's day-to-day activities include proactive vulnerability and penetration testing of networks globally and responding to incidents that pose a threat to networks such as virus infestations.

The High-impact Incident Response Coordination Team (HIRCT) sits higher in the hierarchy. They coordinate incident response. The team of four can quickly expand to dozens of incident responders if necessary, recruiting anyone in the organisation from their normal role in order to rectify an incident. Their role is full-time in dealing with high-impact incidents, and includes conducting post-incident reports for incidents such as the loss of a mainframe or the crashing of a critical website. The two teams work independently, but are not mutually exclusive. When a high-impact incident strikes, the HIRCT manage the response and control of the incident until resolution, liaising with the Network Team (and any others) via teleconferencing, phone, e-mail and the helpdesk system.

4.3. *Interview participants*

To provide an overall picture, and to see how incident response teams are informing information security in general, half the interviewees were selected from outside of the incident response team. Two of the participants work full-time in an incident response capability, while the other two interviewees have been chosen from areas that (according to literature) should be informed by the incident response team (see Table 2).

NIRT MGR is the manager of the organisation's Network Security Incident Response Team which operates under the information security department. NIRT_MGR is highly educated with two postgraduate qualifications in computing. She has been working at FinanceOrg for two and a half years and has much experience in networking, and security.

HIRCT_MGR is the manager of FinanceOrg's High-impact Incident Response Coordination Team, which operates under the business continuity department. He has a vast technical and business knowledge of the company's staff and information systems. HIRCT_MGR's main role involves managing the high-severity information security incidents that may reach FinanceOrg's systems. He coordinates with business representatives, technical teams and numerous others until the incident reaches resolution.

ISR_MGR is the Information Security and Risk Manager for the organisation's Corporate Business Department. ISR_MGR has a strong background in security spanning many years. The role of ISR_MGR in each of the business departments is to act as a spokesperson and champion for the cause of information security, manage information security risk, and handling of minor incidents.

ISPPT_MEMBER is a senior member of FinanceOrg's Information Security Policy and Procedure Team based in the Information Security Department. He has a very strong technical background, including years of experience in security. ISPPT_MEMBER works in a team of four, and is responsible for producing and managing the general information security policies for FinanceOrg. This role is not an enforcement role.

A previously mentioned, ISR_MGRs of various departments reside in the Information Security department with ISPPT_-MEMBERs and the NIRT_MGR. All three roles report to the Chief Information Security Officer (CISO) who reports to the Chief Information Officer (CIO).

All interviews were conducted during normal working hours and taped. They lasted between 1 h and 2 h. Five template and procedural documents were gathered for further analysis. Recorded interviews and notes were later transcribed and analysed via open, axial and selective coding and through the use of specialised software (Neuman, 2006). The transcribed date was further cross-referenced with the collected documents for triangulation.

Table 2 – Names and roles of interview participants.

Role/pseudonym	Role
NIRT MGR	Manager of Network Incident Response Team (based in the Information Security Department)
HIRCT MGR	Manager of High-impact Incident Response Coordination Team (based in the Business Continuity Department)
ISR MGR	Information Security and Risk Manager of the Corporate Business Department
ISPPT MEMBER	Senior Member of Information Security Policy and Procedure Team (based in the Information Security Department)

4.4. *Case study results: incident response and knowledge gathering*

Incident response at FinanceOrg is divided by impact level. High-impact incidents are coordinated by the HIRCT and 'fixed' primarily by the NIRT. Low-impact network security incidents are dealt with independently by the NIRT. Both teams have a very different approach to knowledge gathering, which will be demonstrated in this section.

4.4.1. *Network incident response team (low-impact)*

The knowledge gathering process of the Network Incident Response Team is focused on identifying direct causes, rather than the underlying causal structure. NIRT Mgr explained:

> *NIRT Mgr: "[We] basically go through standard steps of standard procedure what's going on, how's it effecting [systems], [and] what can we do to remedy it. Part of what we do is quick and tactical; how do we stop it today – right now…"*

> *NIRT Mgr: "…making sure the process executes seamlessly, smoothly and effectively. And there isn't that much trivial administrative burden to deal with during the incident… when the team are working on an incident, I want them working on that incident, not filling out paperwork and detail while the rest is going on… There are certain processes we can follow and they can log certain things… but the bottom line is – you've got to get it done."*

While the network incident response team, resolves incidents effectively and efficiently, the information gathered from these low-impact incidents exhibits a strong focus on technical information, over policy and risk. Although the team does gather a large amount of this technical information in order to solve problems, gathering additional information, crucial to future learning is not being considered. The use of an incident tracking system could also facilitate learning

down the track, but that would require more than a technically-based log which is only filled out on completion of an incident.

4.4.2. *High-impact incident response coordination team*

The HIRCT does not work independently on incidents. They deal with the coordination of high-impact incidents called into the Helpdesk and the NIRT. How incidents receive their impact rating is considered sensitive, thus cannot be discussed in any detail. Documentation analysis shows that there is a clear, standardised method of determining an incident's impact level. The process of gathering operational knowledge during high-impact incidents is highly mature, and can involve large numbers of technical and business staff.

> *HIRCT Mgr: "…after a high severity incident occurs, two conferences calls are setup (a technical and a business one)… Two main parties are involved - technical problem managers (me) and respective business heads will ring in… to get the latest update."*

The role of the business conference call is to communicate progress in a non-technical way, so that the business is fed information that is relevant and understandable. This also shows that there is significant business-technology communication during high-severity incidents.

4.4.3. *Post-incident knowledge creation process*

In terms of low-impact incidents, the only formal post-incident practice that occurs is to write a log entry in the incident tracking system to say that the issue is fixed.

The actual incident review process is only informal. NIRT Mgr explained that while their processes were adhoc, they still attempted to learn and determine if they could be improved. However, ISPPT Member (Senior Member of the Policy and Procedure Team) confirmed the lack of root cause analysis for incidents:

> *ISPPT Member: "…however with incidents… you really should be doing the last stage of it. The… debrief [or] root-cause analysis… I think FinanceOrg is still immature in that respect."*

In terms of knowledge creation, the difference between low-impact incidents and high-impact incidents is stark. For high-impact incidents, the process is strictly formalised; a review occurs for *every* high-impact incident. The result of these meetings is a post-incident report (PIR). The HIRCT Mgr explained that his team aims to conduct investigations within 24 h of the system services being restored. The immediacy of the response shows how mature the knowledge creation process is, and the level of effort devoted to learning from incidents, especially through causal analysis:

> *HIRCT Mgr: "Once the incident is over, we then conduct a formal investigation into what went wrong. Identify a number of causal factors, and mitigation actions to prevent it reoccurring."*

The review process involves at least three meetings. Typically, the first sessions involve brainstorming and do not include members from the risk area and the business in general (perhaps to prevent outsiders from arriving at premature conclusions). Whilst the intention seems honourable, the backlash from that is that only the technical groups are involved in the input, creating bias, and excluding others from the learning process. Later, a second meeting takes place where they examine the causal factors and potential mitigation for these factors. The same technical staff are present at the second meeting. The final post-incident report contains the causal analysis, a new risk assessment of the system in question and a list of tasks that multiple parties must complete.

4.4.4. *Case study results: information dissemination*

For low-impact incidents, the NIRT produces several formal reports for management where the focus is on technical aspects. The management report is a statistical document containing only generalised learning information. However, the NIRT does use limited informal communication channels in order to disseminate incident knowledge.

> *NIRT Mgr: "…identify [risk-related] information and pass that off to the risk assessment group because then they have more of an over-arching view of what the infrastructure in the organisation is."*

These informal channels are largely due to NIRT Mgr's own initiative. Furthermore, the ISPPT Member (Senior Member of the Information Security Policy and Procedure Team) also works in the same office as NIRT Mgr.

The silo structure of the organisation, a trait shared by many large corporations, is a serious hindrance. Those outside of the Information Security Department such as ISR Mgr (Information Security and Risk Manager for Corporate Business) are 'out of the loop'. ISR Mgr experiences great difficulty in finding relevant incident knowledge to apply to her own security requirements, demonstrating large information dissemination problems.

When asked about her biggest challenge in the job, the Corporate Business Information Security Risk Manager commented:

> *ISR Mgr: "It's the sharing, or rather the finding of information. The information is there. Each day I find a new resource that's got great information."*

ISR Mgr provides an interesting perspective on why this is so:

> *ISR Mgr: "I think it's just because people get focused on what they do… so I think we get very insular about it… In our groups we work, we're all 'techies'… I'll let maybe the server guys in because I know they're 'my people' and will understand. And I don't think we've quite made that bridge between technology and business. We've still away to go. I don't think that it's they don't want to give the information, they probably just think that it's not relevant."*

Due to a lack of formal policy on information dissemination and communication channels, the silos of information remain a problem. ISR Mgr receives the post-incident reports because she is now on the distribution list. ISPPT Member, however, has little knowledge that PIRs even exist. After some

explanation, ISPPT Member acknowledged that such information would be very useful for development of policy and procedure.

4.4.5. *Case study results: extent of incident learning*

Through the analysis and coding of information, a critical element that we searched for was evidence of learning both in thought as well as practice. Also, the sophistication of the learning processes taking place in the organisation.

In the previous section on Incident Response and Knowledge Gathering, the quotes from the NIRT demonstrated that members were focused on resolving the direct causes of incidents. In this kind of investigation, the learning that typically takes place arises from incident response personnel taking corrective actions. Here, learning bridges the gap between what should have happened in the environment and what did happen – i.e. expected and obtained outcomes. The members of the NIRT understand this kind of learning and practice it in the course of their duties.

However, the manager of the HIRCT demonstrates an understanding of a higher and more sophisticated type of learning which involves questioning the technological, organisational and human factors that influenced the circumstances within which the incident occurred:

> *HIRCT Mgr: "Everything we do feeds into something else. Most incidents you will find that the actual cause of the incident is an underlying gap in the process somewhere. It might be a process that allows... like people often say someone put a typo in, that's your recourse… If we have a process that allows a single human error, to cause a high-severity incident, that process needs to incorporate more checks and balances."*

The HIRCT Mgr is questioning the system itself, rather than the user as the cause:

> *HIRCT Mgr: "…Any time we actually go through… to find root causes, and even some of the contributing causes, a number of those I think are actually the big-wins… if it's contributed to that one incident, it could contribute to others … and by looking out for those shared issues, we solve a lot of potential problems."*

These responses from our interviews demonstrate a desire or understanding of the need to engage in causal analysis and to question the system or methods.

5. Discussion

FinanceOrg is a large, complex, high-reliability, global organisation. Secure operation depends on having a strong information security backbone with incident response capabilities – a core component of its portfolio. Our case study has found that the organisation is closely following the guidelines found in much of the incident response literature such as described in white papers published by various CERTs (Smith, 1994; West-Brown et al., 2003). By following these guidelines, FinanceOrg exhibits a mature incident response practice, however there are several significant issues that affect the greater organisational security function.

5.1. *Disparity in incident response approaches*

There is a positive incident response culture at FinanceOrg, where those who report incidents are not punished. Once incidents have been reported, systems are in place (Helpdesk, e-mail and telephone contacts) for incidents to be classified and the appropriate incident response team is notified. There is a comprehensive incident response structure with both incident responders and incident coordinators (West-Brown et al., 2003).

The NIRT is extremely effective at solving incidents that affect the network of FinanceOrg. They focus on technical aspects, gather large amounts of forensic data and respond rapidly to resolve the direct causes of incidents. Their focus is on protecting the core network with containment and escalation implemented if necessary. The NIRT's involvement with proactive security measures such as vulnerability and penetration testing are further evidence of the maturity of their response.

The communication channels used by NIRT are typically informal and adhoc. Informal communication channels are opened up to policy and procedure staff, management and the respective information security and risk managers for each of the business departments. Post-incident, the incident tracking system which is used to log the incident is closed, legal ramifications of the incident are followed up and relevant parties are notified of the repair.

The process undertaken by the HIRCT is vastly different. As an incident occurs and is classified as a high-impact incident, the HIRCT team consisting of four people can quickly expand to dozens, with communication facilitated by conference calls for both technical- and business-related information. Incidents are resolved rapidly and cost is not a constraint. Within 24 h of resolution, an investigation begins. Many technical staff are invited to the PIR meetings, through which a comprehensive post-incident report is produced. This report details the causal structure of the incident, and identifies gaps in policy, or maintenance issues. A risk assessment is conducted, and tasks are allocated via the incident tracking system to the relevant staff. This process has seen a reduction in incidents of around 200 per month from 2002 down to only 16 at the time of this study.

5.2. *Lack of a formalised information dissemination process*

On the topic of information dissemination, previous case studies found that key security processes were not communicating such as information security risk assessment and incident response. Our findings from this case study reinforce these observations.

Both participants in our case study from outside the incident response team complained of a lack of incident knowledge being distributed effectively and agreed that better information dissemination would assist in improving their security practices and therefore the security of the organisation. As organisations, such as FinanceOrg, are often simply following the CERT literature and frameworks such as ITIL and ISO17799, this finding is hardly surprising. Without formalised processes, dissemination is made difficult by the

siloed nature of FinanceOrg. A formal process for disseminating incident knowledge – particularly the PIR reports – is required to ensure that the valuable information produced by the HIRCT team (at great expense) should not go to waste.

Other social, operational and technological interventions may also be required to solve the information dissemination problem. The Information Security and Risk Manager alleged that part of the problem was cultural. That 'techies' talk to 'techies' and organisations tend to be insular. It is proposed that by formalising the information dissemination process, organisational silos would be broken down and the business-technology gap would be reduced. To facilitate cultural change a formalised process is required for the conversion of post-incident reports in to a learning document, that is easily understood by many in the organisation. Both Cooke (2003) and Bishop (2003a) support the notion that distributing such reports to users, particularly those that reported the incident, increases their awareness of incidents and the incident response process in general.

However, the extent to which information is disseminated is also influenced by learning impact. High-impact incidents result in post-incident reports with valuable information that must be disseminated. However, low-impact incidents do not result in such reports despite the fact that they may potentially be more useful from a learning perspective. In other words, there is a subtle but important difference between 'high-impact' and 'high-learning' incidents. The distinction is key to an efficient learning process in organisations.

5.3. *Focus on technical learning over policy and risk*

Technical information is well structured through the incident tracking system, and technical tasks are automatically logged and allocated. These measures are rapidly implemented by the relevant technical teams and checks are put in place to make sure technical deliverables are completed. As our case study shows, technicians are present at all PIR meetings but business and risk staff are often excluded, especially from the early stages. Hence, both high-impact and low-impact incidents exhibit a focus on technical issues rather than gathering information on an inadequate risk assessment or a gap in policy. Unfortunately, policy and procedure are often seen as 'soft' issues in information security even though the biggest threats to information systems are often internal (Whitman and Mattord, 2005).

In FinanceOrg low-impact incidents, knowledge gathered is almost purely technical with the aim to solve the problem quickly and effectively. There is a reluctance to do anything outside of responding to the incident, including logging and recording information. As such, costing of incidents and gathering additional information to facilitate organisational learning does not take place. Since there is little follow-up procedure as well, current knowledge creation and dissemination is purely based on statistic reports sent to management and is biased towards technological knowledge.

For high-impact incidents the technical focus remains, even though non-technical issues are also considered. Again, it may be a lack of a wider perspective in literature on incident response that results in poor practices in the workplace. Almost all CERT guides exhibit a strong emphasis on technical aspects from firewalls and proxies (Smith, 1994) to forensics (Killcrece et al., 2003a). The aim of the post-incident process, however, is to get to the root cause of a problem, which is often not a technical problem (eg. a firewall setting requiring adjustment) but a policy problem (eg. not having a policy for blocking certain ports on all firewalls). Despite this, business and risk staff are excluded from the first two post-incident report meetings which severely limits incident learning in those areas.

5.4. *Organisational learning*

The most interesting observations relate to organisational learning. In particular, learning in thought as well as practice and the sophistication of learning processes applied in incident response. To assist in analysis, some background in organisational learning theory is useful.

Organisational learning theories are concerned with organisations learning and adapting its behaviour (van Niekerk and von Solms, 2004). The origins of organisational learning theory stem from the work of Argyris and Schon (1978) who argued that there are two types of learning: single-loop and double-loop.

Single-loop learning is a simplistic, adaptive approach that most organisations use day-to-day whereby employees simply detect and then correct deviations from policies, procedures or expected norms. An example could be a security incident involving a firewall that has taken place because of a configuration problem. A single-loop response would be to simply correct the configuration without an in-depth root cause investigation that examines the current process and policy for establishing the firewall configuration.

Double-loop learning involves questioning the very principles such as policy and procedure that organisations function on, and is more generative in nature. In the above situation, a double-loop response would be to begin with a root cause analysis followed by an investigation into the process that resulted in the mis-configuration of the firewall. If the process, hypothetically, handled requests from business units to open up ports in the firewall to make way for new avenues of network traffic then double-loop learning would include the decision to improve this process such that the risk of future mis-configuration was minimized.

Most companies focus on single-loop learning. When organisations do look at the more generative learning or 'double-loop' learning, however, more organisational value will be derived as a result (Argyris, and Schon, 1978; Malhotra, 1996). Double-loop learning is akin to problem solving, involving continuous experimentation and feedback (van Niekerk and von Solms, 2004), and is concerned with more long-term change, rather than short-term goals. Naturally, double-loop learning is more difficult and future-focused. Carrying out such learning activities as an organisation involves complex dependencies across individuals and groups (Kim, 1993).

In terms of incident response, bridging the gap between the localised, single-loop learning of the incident response team, and wider, double-loop learning requires a system in place to facilitate learning from the incident response team to a wider audience. Dixon (1999) argues that organisational learning is

not simply the sum of all that its members know, but instead it is the collective use of learning capability. So it is not just the knowledge itself that is of most importance, but the ability to work together, synthesise and translate that knowledge.

Literature on organisational health and safety reports that continuous improvements across the organisation can be achieved by the implementation of an Incident Learning System as part of their incident response process (Cooke, 2003). Such a system should also aim to encourage the reporting of incidents. Bishop (2003a) demonstrates that when an incident learning system is successfully applied, the reporting rate increases while serious accidents/incidents are reduced.

Melara et al. (2003) applies the Cooke et al. (2006) Incident Learning System (see Fig. 1) to a study of an insider attack on organisational information security. By analysing pre-incidents as well as incidents in-depth, the researchers found that a serious insider attack could have been averted. However, without an incident learning process, the malicious insider caused serious damage to the internal systems of the case study organisation (Melara et al., 2003). Failure to learn from precursor incidents is an ubiquitous trait in all kinds of security incidents.

Both Cooke (2003) and Bishop (2003a) stress the need for causal analysis of incidents so that the underlying issues leading to the incident can be identified. By conducting a causal analysis, new knowledge is created which through generalisation can be used to facilitate organisational learning. Causal analysis is typically part of a wider post-incident review process that may include a timeline of events, risk assessments, and root cause analysis (Bishop, 2003a).

The amount of effort spent per incident will need to be relative to the incident's learning potential (Bishop, 2003b) as post-incident reviews are costly, challenging, and require great skill and expertise to perform (Stephenson, 2003). However, post-incident reviews are a necessary component of the incident learning process. Unless at least some small review of an incident occurs, learning will be lost to organisational memory (Cooke, 2003).

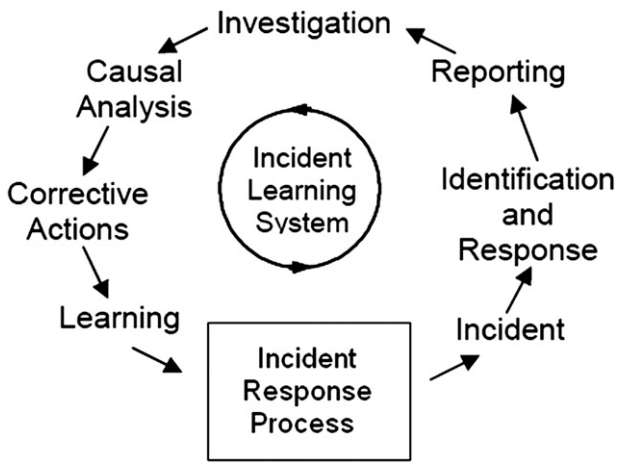

Fig. 1 – Incident learning system (modified from Cooke et al. (2006)).

5.5. *Learning at FinanceOrg*

At FinanceOrg, high-impact incidents have a follow-up procedure in which a causal analysis is conducted and corrective action is taken. As a result there has been a rapid and significant reduction in incidents. However, the only learning in FinanceOrg identified by this case study is confined to the incident response team. This is unfortunate, as the organisation as a whole has much to learn from incidents, in particular the security risk management function can use incident data to inform its risk assessment function (especially estimation of probabilities of risks).

In the case of FinanceOrg, as noted in the section on the Extent of Incident Learning, the NIRT was largely engaged in single-loop learning as it was focused on resolving the direct causes of incidents. However, HIRCT_Mgr seemed to appreciate the concept of double-loop learning as he questioned the system itself, the governing variables and the need for a 'root cause analysis'.

However there is no evidence that FinanceOrg actually practices double-loop learning. In fact, there was evidence to the contrary. FinanceOrg documentation showed that HIRCT does not respond to incident precursors (a confluence of events that have the immediate potential to cause a high-impact incident). Further, the fact that information dissemination issues have not been addressed and key areas such as policy and risk have not benefited from incident based data suggests that double-loop learning is not practiced.

To facilitate double-loop learning FinanceOrg should attempt to tighten and integrate technical incident response, risk assessment and policy and procedure practices (Meijer and Tucker, 2003). Hence, we argue that the risk management team and security strategy and policy developers should be formally included in incident information dissemination and could have a greater participation in the casual analysis as well. True double-loop learning is only achieved when an organisation is capable of systemically correcting the issues identified through causal analysis. Identifying why a risk has not been identified, or why its mitigation has not been addressed properly, may lead to corrective measures for other risks not directly related to this incident. Similarly, identifying why a potential incident was not adequately covered by the current security policy, may lead to further improvements to that policy that may prevent future incidents not directly related to this incident.

It is reasonable to expect that for FinanceOrg to implement true double-loop learning, both low-impact incidents and precursor incidents would have to be examined for high-learning incidents. According to Cooke (2003), critical incidents are caused by the ignorance of low-impact incidents and precursor incidents. While high-impact incidents have a follow-up procedure in which a causal analysis is conducted, low-impact incidents only have a small review process. Cooke's (2003) Incident Learning System argues that *all* incidents should be used for incident learning and the focus should be on causal structures. This is currently not occurring in FinanceOrg. Even when moderated by Bishop's (2003a) assertion that the level effort devoted to learning should be commensurate with the level of learning that can be gathered from incidents, the current approach in FinanceOrg to low-impact incidents is still inadequate. At the very least, clusters of incidents recognised across the organisation should be

tackled as a whole. A large number of low-impact incidents are potentially as damaging as a single high-impact incident.

Cooke argues that serious disasters can be averted by learning from precursor incidents in the same way as actual incidents. As discussed earlier, Melara et al. (2003) found that by analysing pre-incidents as well as incidents in-depth, a serious insider attack could have been averted.

Although FinanceOrg does follow the full cycle of the Cooke et al. (2006) incident learning system, further analysis indicates that there are limitations in the current system. The process of conducting the causal analysis, combined with an investment in resources in improving the reports themselves was found to be the most effective tool in reducing incidents. However, at no stage did we uncover any elements of the kind of systemic corrective action that Cooke et al. (2006) describe as being the precursor to double-loop learning (that is, the questioning of the system and core, fundamental principles). While FinanceOrg did follow the incident learning system model as it currently stands, the model is not a true reflection of what double-loop learning actually entails and what significant changes could be made through the questioning of the organisation's processes and principles.

In Cooke's model, learning is the last step of the system. In this step, the supervisor of the incident writes a 'lessons learned' report that is disseminated according to the value of the lessons learnt to various roles in the organisation. While this report is supposed to be submitted to a Quality Assurance type committee to consider systemic changes if need be, our experience from this case study is that there is currently little understanding in the incident response team on what double-loop learning really involves. We believe that the lack of an explicit double-loop learning loop in Cooke's model may also have influenced how the actual Causal Analysis is performed and possibly limit its focus.

Hence, we suggest that the Cooke et al. (2006) model should be modified to better reflect the difference between conducting more direct corrective actions (eg. altering user behaviour) and more systemic, in-depth, fundamental actions that will change the system itself. The new model (Fig. 2) still emphasizes that causal analysis is the catalyst for corrective actions and associated learning processes as dictated by the original model and confirmed by our research. However, we believe that by making the relationship between Causal Analysis and Systemic Corrective Action more explicit, it will not only be likely that those stakeholders responsible for Systemic Corrective Action will be identified by the organisation, but that they could potentially have a larger involvement in the Causal Analysis stage as well and ensure a broadening of its focus.

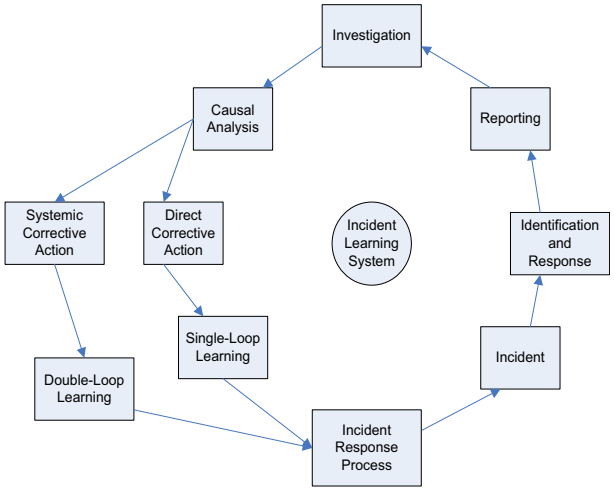

Fig. 2 – Revised incident learning system (modified from Cooke et al., 2006).

6. Conclusion

Incident response teams are viewed as the 'fire-fighters' of modern organisations, responding to and solving security incidents as they arise. However, there is often a lack of attention to the learning aspects of incident response and post-incident functions. The importance of double-loop learning as the driver of organisational learning is paramount, enabling organisations to learn effectively from the past and not suffer repeat incidents or mistakes. Though single-loop learning is more often exhibited in organisations, double-loop learning ensures that organisations achieve strategic and competitive benefit in the longer term. Causal analysis, post-incident reporting and appropriate information dissemination are important for organisations to determine the cause of the incident and to apply learning procedures.

To explore organisational learning of incident response we conducted an exploratory, in-depth case study. Through semi-structured interviews with the incident response teams of a global financial institution (FinanceOrg), we established that while FinanceOrg fields a mature, effective and experienced incident response team, they are found lacking in their ability to exploit their organisational learning capability. This is partly due to their focus on high-impact incidents and their wholesale neglect of low-impact and precursor incidents in their incident learning. FinanceOrg's learning practices are further harmed by the lack of incident information dissemination to all interested or involved parties and their predominantly technical approach to incident reporting.

Though our case study has uncovered evidence that FinanceOrg does recognise the need for double-loop learning, we found that there was little understanding of what double-loop learning involves and as a result their approach to learning from security incidents fell mostly into a direct, single-loop learning capacity. We suggest that by explicitly identifying potential double-loop learning opportunities in such areas as risk assessment and policy development, organisations may be better able to address double-loop learning. Hence, we proposed a modification of the Incident Learning System model by Cooke et al. (2006), to encourage a broader focus of the causal analysis of security incidents and ensure that any systemic corrective actions to risk management and policy development process are considered.

REFERENCES

Ahmad A, Ruighaver AB, Teo WT. An information-centric approach to data security in organizations. In: Proceedings of Tencon 2005: IEEE Region 10, Melbourne, Australia; 2005.

Alberts C, Dorofee A. Managing information security risks. Pittsburgh, PA: Mellon Software Engineering Institute; 2004.
Argyris C, Schon D. Organisational learning: a theory of action perspective. Addison-Wesley; 1978.
Benbasat I, Goldstein DK, Mead M. The case research strategy in studies of information systems. MIS Quarterly 1987;11(3): 369–86.
Bishop PG, Johnson C, Black W, Hamilton V, Koorneef K. Learning from incidents involving E/E/PE systems: part 1 – review of methods and industry practice. Adelard, http://www.hse.gov.uk/research/rrpdf/rr179.pdf; 2003a.
Bishop PG, Johnson C, Black W. Learning from incidents involving E/E/PE systems: part 2 – recommended scheme. Adelard, http://www.hse.gov.uk/research/rrpdf/rr181.pdf; 2003b.
Cooke DL. Learning from incidents, http://www.albany.edu/cpr/sds/conf2003/proceed/PAPERS/201.pdf; 2003.
Cooke DL, Dubetz M, Heshmati R, Iftody S, McKimmon E, Powers J, et al. A reference guide for learning from incidents in radiation treatment, www.ihe.ca/documents/HTA-FR22.pdf; 2006.
Darke P, Shanks G, Broadbent M. Successfully completing case study research: combining rigour, relevance and pragmatism. Information Systems Journal 1998;8:273–89.
Dhillon G, Backhouse J. Current directions in IS security research: towards soci-organizational perspectives. Information Systems Journal 2001;11(2):127–53.
Dixon N. The organisational learning cycle: how we can learn collectively. 2nd ed. Hampshire: Gower; 1999.
Jaikumar V. Organizations should build an incident response team. ComputerWorld Canada 2002;9(16).
Killcrece G, Kossaowski P, Ruefle R, Zajicek M. State of the practice of computer security incident response teams (CSIRTs), http://www.sei.cmu.edu/publications/documents/03.reports/03tr001.html; 2003a.
Killcrece G, Kossaowski P, Ruefle R, Zajicek M. Organizational models for computer security incident response teams (CSIRTs), http://www.cert.org/archive/pdf/03hb001.pdf; 2003b.
Killcrece G, Ruefle R, Zajicek M. Creating and managing computer security incident response teams (CSIRTs), http://www.first.org/conference/2004/papers/t1_01.pdf; 2004.
Kim DH. The link between individual and organizational learning. Sloan Management Review 1993;35:37–50.
Kossakowski K-P, Allen J, Alberts C, Cohen C, Ford G, Fraser B, et al. Responding to intrusions, http://www.potaroo.net/t4/docs/sim006.pdf; 1999.
Malhotra Y. Organizational learning and learning organizations: an overview, http://www.brint.com/papers/orglrng.htm; 1996.
Meijer RJ, Tucker R. State-full risk assessment & automated security incident policy environment, version 0.3.1. ISECOM, 2003. Unknown: ISECOM, http://isecom.securenetltd.com/sipes_goal_0.3.1.pdf; 2003.
Melara CA. System dynamics model of an insider attack on an information system, http://www.albany.edu/cpr/sds/conf2003/proceed/PAPERS/294.pdf; 2003.
Mitropolous S, Patsos D, Douligeris C. On incident handling and response: a state-of-the-art approach. Computers and Security 2006;25:351–70.
National Institute of Standards and Technology. NIST special publication 800–61, computer security and incident handling guide. Revision 1, http://csrc.nist.gov/publications/; 2008.
Neuman WL. Social research methods – Qualitative and quantitative approaches. 6th ed. Boston MA: Pearson Education, Inc; 2006.
Novak CJ. Investigative response: after the breach. Computers and Security 2007;26(2):183–5.
SANS Institute. Computer security incident handling step by step. Available from: http://www.sans.org; n.d.
Shanks G, Rouse A, Arnott D. A review of approaches in research and scholarship in information systems. In: Proceedings of the 4th Australian Conference on Information Systems; 1993. p. 29–44. Brisbane.
Shedden P, Ruighaver AB, Ahmad A. Risk management standards – the perception of ease of use. Journal of Information Systems Security 2010;6(3).
Siponen M. Analysis of modern IS security development approaches: towards the next generation of social and adaptable ISS methods. Information and Organization 2005;15.
Smith D. Forming an incident response team. In: Proceedings of the FIRST Annual Conference. Brisbane, Australia: University of Queensland; July 1994.
Stephenson P. Conducting incident post mortems. Computer Fraud and Security 2003;4(3):16–9. Elsevier.
Tan T, Ruighaver AB, Ahmad A. Incident handling: where the need for planning is often not recognised. In: Proceedings of the 1st Australian Computer Network, Information & Forensics Conference; 2003. Perth, Nov 24.
Van Niekerk J, von Solms R. Organisational learning models for information security, http://icsa.cs.up.ac.za/issa/2004/Proceedings/Full/043.pdf; 2004.
Van Wyk K, Forno R. Incident response. NY: O'Reilly; 2001.
Walsham G. Interpretive case studies in IS research: nature and method. European Journal of Information Systems 1995;4:74–81.
West-Brown MJ, et al. Handbook of Computer Security Incident Response Teams (CSIRTs). 2nd ed., http://www.cert.org/archive/pdf/csirt-handbook.pdf; 2003.
Werlinger R, et al. Preparation, detection, and analysis: the diagnostic work of IT security incident response. Information Management and Computer Security 2010;18(1):26–42.
Whitman ME, Mattord HJ. Principles of information security. Thomson Course Technology; 2005.
Wiik J, Gonzales JJ, Kossakowski K- P. Limits to effectiveness in computer security incident response teams. In: Proceedings of the Twenty Third International Conference of the System Dynamics Society. Boston, MA: The System Dynamics Society; 2005.
Yin R. Case study research. 3rd ed. Thousand Oaks: Sage Publications; 2003.
Zafar H, Clark J. Current state of information security research in IS. Communications of the Association for Information Systems 2009;24. Article 34.

Atif Ahmad is an information security researcher and independent security consultant based at the Department of Information Systems, University of Melbourne. His research interests are in asymmetric warfare and information security risk assessments especially where knowledge artifacts are concerned. In previous years Atif has worked as a consultant for Pinkerton and Worley Parsons where he applied his expertise to Internet corporations and critical infrastructure installations. Atif is a Board Certified Protection Professional (CPP) with the American Society for Industrial Security and holds an adjunct position at the secau Security Research Centre at Edith Cowan University.

Justin Hadgkiss was an honours student enrolled in the Bachelors of Information Systems where he completed a research project on Information Security Incident Response in Organizations. Justin was a recipient of the prestigious Honours Scholarship awarded to the student with the highest average grade with first class honours (H1) in the third year of their bachelor degree. Justin has since taken up full time employment in one of Australia's iconic multinational corporations.

Tobias Ruighaver is currently an Honorary Research Fellow at the School of Information Systems of Deakin University and was previously the Head of the Organisational Information Security Group at the University of Melbourne. His research interests are in Security Culture, Security Governance and the Economics of Information Security.