2010

Organisational Learning and Incident Response: Promoting Effective Learning Through The Incident Response Process

Piya Shedden
University of Melbourne

Atif Ahmad
University of Melbourne

A B. Ruighaver
Deakin University

DOI: 10.4225/75/57b6771734788
Originally published in the Proceedings of the 8th Australian Information Security Mangement Conference, Edith Cowan University, Perth Western Australia, 30th November 2010

Organisational Learning and Incident Response: Promoting Effective Learning Through The Incident Response Process

Piya Shedden[1], Atif Ahmad[1] and A.B. Ruighaver[2]
[1]Department of Information Systems
University of Melbourne
Victoria, Australia
[2]School of Information Systems
Deakin University
Burwood, Victoria, Australia
psheddon@unimelb.edu.au
atif@unimelb.edu.au
anthonie.ruighaver@deakin.edu.au

Abstract
Effective response to information security incidents is a critical function of modern organisations. However, recent studies have indicated that organisations have adopted a narrow and technical view of incident response (IR), focusing on the immediate concern of detection and subsequent corrective actions. Although some reflection on the IR process may be involved, it is typically limited to technical issues and does not leverage opportunities to learn about the organisational security threat environment and to adapt incident response capabilities. Given the science of incident response is rooted in practice, it is not surprising that the same criticisms can be applied to much of IR literature. However, a review of literature in the area of organisational learning suggests that improvements can be made to the incident response process. This paper proposes that future incident response research must incorporate a learning focus, improve feedback timing on learning activities, facilitate double-loop learning and incorporate an informal learning perspective within both formal, procedural incident response processes as well as unstructured, informal environments.

Keywords
Security incident response, organisational learning, incident learning, informal organisation, knowledge management.

INTRODUCTION

Security incident response is a critical process, ensuring that organisations have a capability to effective respond to, eradicate, recover from and learn from security attacks perpetrated against them. The ultimate goal is to minimise the effects of a successful attack and to ensure an expedient recovery (van Wyk et al, 2001; Wiik et al, 2005). Successful security incidents can cost organisations severely across a variety of impact criteria, including reputation, productivity and direct financial costs attributed to lost business as well as legal and regulatory penalties. Standard incident response methodologies exist for organisations to use in their response to security incidents across a wide range of impact severities (eg. Northcutt, 1998; West-Brown et al, 2003; Grance et al, 2004; Murray, 2007).

A seminal report by Knight & Pretty (1996) established a direct causal relationship between organisations that successfully recovered from catastrophes and their effective response to the incident. In fact, the paper asserts that the perceived success of the incident response was a more significant factor in share-value recovery than whether catastrophe insurance was used to limit negative impact. Further, although not all incidents necessarily turn into catastrophes, the ability of an organisation to effectively mitigate an incident plays a key role in preventing incidents from escalating into a catastrophe.

There are many factors that determine effectiveness of incident response. Among these are resourcing of the incident response capability, availability and application of technical expertise, and support from senior management. These factors are duly noted in the standard incident response methodologies available in the public domain (SANS and NIST references here). However, at least one expert has pointed out that one of the biggest mistakes in the practice of incident response is the lack of effective learning (Chuvakin, 2005).

Recent studies reinforce this observation, indicating that organisations have adopted a narrow and technical view of IR, focusing on the immediate concern of detection and subsequent corrective actions. Although standard incident response methodologies incorporate a ‘feedback’ or ‘follow-up’ phase where lessons are to be learned, reflection on IR is typically limited to the technical process and does not leverage opportunities to learn about the security threat environment and effectiveness of internal procedures, controls, training and policies in order to strengthen the organisation's incident response capabilities (Cooke, 2003; Hadgkiss, 2006).

A key activity in the incident response process is the capacity of the process to learn from the errors or mistakes made during the incident, learn which policies and activities are effective or ineffective, identify concerns in staffing and skills and to feed this knowledge back into the process (Northcutt, 1998; Killcrece et al, 2003; Grance et al, 2004). While major incident response methods such as the SANS and NIST models include 'post-mortem' or 'follow-up' activities post-incident, there is little evidence to suggest that organisations actively engage in adequate organisational learning and improvement of these incident response processes (Cooke, 2003). Current incident response literature instead focuses upon technical responses to incidents, the initial phases of the process and forensic activities (Mitropolous et al, 2006; Turner, 2007; Zhang et al, 2009). However, if organisations were to appropriately learn from and manage their incident response capability, they would be able to leverage opportunities to learn from incidents to their best advantage and realise the benefits of a robust process and fortified security strategy.

Organisational learning literature can be used to develop deeper insights into how incident learning activities can be examined and improved. They outline and detail how organisations are able to effectively learn from events and modifying behaviours to adapt to changes in their environments (Fiol & Lyles, 1985; Huber, 1991). The effects of a capable learning organisation are lower turnaround times, a greater capacity to deal with change in the organisational environment and innovative strategies (Goh, 1998). However, work conducted in incident learning (Cooke, 2003; Hadgkiss, 2006; Muhren et al, 2008) has attested that organisations are not effectively learning through their incident response capabilities, despite the detailed actions that should be taken during post-mortem phases of the SANS and NIST incident response models. Muhren et al (2008) describes how 'considerable opportunities remain unseized' in this space.

This paper will subsequently present a literature review of incident response and organisational learning literature, outlining security incident response processes, how organisations learn effectively and the importance of double-loop learning. A series of propositions will be presented, suggesting that the incident response process must have adequate knowledge capturing methods to ensure quicker turnaround times for learning, feature the application of double-loop learning to question fundamental processes and principles and that learning processes must ensure that both formal and informal learning methods are applied.

INCIDENT RESPONSE METHODS AND INCIDENT LEARNING

Incident response refers to the formal, structured methods by which organisations engage teams to detect and eradicate information security incidents (West-Brown, 2003; Wiik et al, 2005). Incident response teams are the 'firefighters' within organisations, devoted to the preparation, identification, analysis and recovery from security incidents (Jaikumar, 2002). On the timeline of business continuity, incident response is the immediate action taking to a security breach, whereas disaster recovery and business continuity are longer-term concerns (Whitman & Mattord, 2005). Incident response is therefore the considerations and actions undertaken upon the detection of the security incident and the immediate actions taken in the short-term to reduce the organisation's exposure.

However, a security incident response team is responsible for more than just direct actions against incidents. Instead, such teams will actively advise on security, develop security policy and conduct security training and awareness programs (West-Brown et al, 2003). Therefore, the value of fielding effective and capable incident response teams is that they will firstly be effective in their response to security breaches. However, in their wider organisational role, incident response teams can provide knowledge and information to the organisation as a whole. An incident response team must have a variety of qualities, including technical skill, organisational skill and diplomatic skill in dealing both with the incident, management of the team and effective at negotiating during heated and stressful situations.

There are several published incident response processes that organisations may follow, including the SANS and NIST SP800-61 methods. Both methods offer a similar approach in responding to and treating incidents. The methods centre around a common process, incorporating initial preparatory phases, the detection and containment of incidents, recovery from incidents and a 'post-mortem' analysis. Specifically, the SANS method features six steps: preparation, identification, containment, eradication, recovery and lessons learned (Northcutt, 1998; Murray, 2007). The NIST 800-61 model follows an iteration of four steps: preparation, detection and analysis, containment, eradication and recovery and post-incident activities (Killcrece, 2003; Grance et al, 2004). Ultimately, both models perform the same functions through a similar process, encapsulating preparatory actions before an incident occurs, the identification and analysis of the incident, attempts to contain the spread of the incident, to remove the incident from the organisation's systems, restore original operations and engage a learning process (Kossakowski et al, 1999; Osborne, 2001; Kelver, 2002; West-Brown et al, 2003; Mitropolous et al, 2006). Figure 1 demonstrates a synthesis of this incident response process.

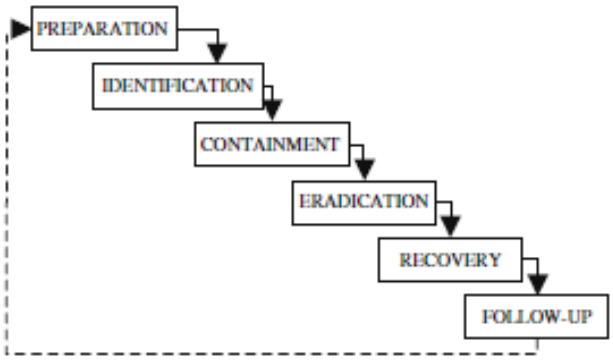

Figure 1: the Incident Response Process (Mitropolous et al, 2006)

This process aims to firstly establish preventative measures, identify when an incident actually occurs, contain the incident, remove the incident, facilitate recovery of organisational systems and networks and conduct a post-mortem review to establish key learning notes. Table 1 further describes the phases of the incident response process in further detail.

Phase	Description
Preparation	The preparation phase is where preventative measures such as security policies and threat models are established. A 'response kit' is built, featuring tools that will be used to assist during an incident, such as USB jump drives, laptops, software, stationary and cabling There is also an emphasis on proactive prevention of incidents through effective patch management and user security awareness training.
Identification	When an incident occurs, identification procedures are engaged, determining whether an incident exists. Here, the incident should be validated, the scope and potential impact determined and how the incident occurred.
Containment	Once the incident has been identified, it must be contained. This will attempt to ensure that the incident does not worsen. Two key objectives are present under containment: the prevention of further contamination of the system and the preservation of evidence for potential future legal proceedings. The incident response team must contain the incident so that it does not spread across the organisation's systems and network.
Eradication	Eradication activities attempt to clean up after the incident, based on the information gathered on the incident. The team will attempt to neutralise the attack (eg. deleting malicious code).
Recovery	Recovery concerns the transfer of the system back into regular organisational use, though with monitoring and involvement from business heads to ensure that the system operates smoothly.
Follow-Up	the incident response team will validate and improve the incident handling process. This will involve the completion of incident reports, presentation of these reports to management, improvement of the incident response process from technical and managerial perspectives and to define a strategy and plan for implementing these changes.

Table 1: Description of Incident Response Phases (Northcutt, 1998; Kelver, 2002; Killcrece, 2003; West-Brown et al, 2003; Grance et al, 2004; Murray, 2007)

Incident response literature shows a disposition towards the technical aspects of intrusions and their eradication (Mitropolous et al, 2006; Novak, 2007; Turner, 2007). Additionally, there is a strong tendency in incident response literature to focus more on the initial phases of incident response over incident learning (Mitropolous et al, 2006; Zhang et al, 2009). Incident response methods are recognised as being tightly coupled with digital forensics (Mandia & Procise, 2002; Novak, 2007), whereby the focus is not upon effective learning and the knowledge gain post-incident. Rather, a digital forensics focus on incident response will lead to an emphasis on technical competence in responding to incidents and the capability of tracing the incident back to its perpetrator for legal processing (Mitropolous et al, 2006).

This technical perspective is consistent with the assertions by Dhillon & Backhouse (2001), Siponen (2005), Shedden et al (2011) and Zafar & Clark (2009) that highlight how current security research is focused upon the technical elements of security and security models rather than socio-organisational issues. Current security methods and models tend to present a focus on the IT infrastructure of organisations, technical risks and technical controls without focusing on humans and practice (Dhillon & Backhouse, 2001; Spears, 2006; Zafar & Clark, 2009). However, these socio-organisational perspectives have the capacity to offer unique insight into security methods, beyond the technical, systematic space and into the 'murky' reality of business and security practice (Brown & Duguid, 2002; Shedden et al, 2009).

The concept of a 'post-mortem' or 'follow-up' phase in incident response has achieved little attention in current literature. It is evident that effective incident response is not a pure technical concern as is currently appreciated. The focus is currently upon forensic, technical and procedural perspectives. However, incident response methods are an iterative learning process that must allow for the flow of information into its phases in order to build the expertise and knowledge base of the individuals. Although learning is a key feature of every fundamental IR model given the presence of feedback loops, knowledge management and learning are not given much attention in literature. Further, the scope of incident learning has never been explicitly defined.

Effective learning from incidents will feed back into the procedures followed, the information received by the incident response team and will identify actions, steps and activities that may have inhibited the recovery of the organisation. Feeding this information back to the organisation's preparedness phase will fortify policies, determine if additional tools are required, increase security budgets, improve training programs and lead to alterations to the incident response procedures, activities and processes themselves.

The post-mortem activities typically consist of analysis and reporting based on the incident, actions taken, what worked and how the incident response procedures and responses could be improved (Kelver, 2002). Incident learning is usually enacted through a series of formal reports, meetings and presentations to management (Northcutt, 1998; Grance et al, 2004). Meetings are held and communicative notes are gathered to address responses, disagreements, suggestions and additions to security policies and the incident procedures (Northcutt, 1998). Issues to document include an estimation of the damage caused, actions taken during the incident, policies and procedures that require an update and any electronic evidence that can be used for pursuing those responsible (Mitropolous et al, 2006). The response to these lessons learned should cycle relevant knowledge and changes into the procedures for the incident response process, training processes for the incident response team, improving the incident response policies and procedures and the creation of further reference material on how to respond to similar incidents (Grance et al, 2004). Such activities effectively feed information back to the preparedness phase as shown in Figure 1 in order to reduce the likelihood of that incident occurring again (Osborne, 2001).

Incident response post-mortem reviews are in need of further study. More research is required to establish how organisations can effectively learn from the incident response process, despite the apparent focus on technical intrusion detection and the initial phases of the incident response process. As both the NIST 800-61 and SANS model demonstrate, it is imperative that key learning notes are documented, reviewed, presented and integrated back into the incident response process for future improvement. However, it is unsure as to how organisations can effectively learn and respond to this information.

ORGANISATIONAL LEARNING FOR INCIDENT RESPONSE

Organisational learning as a field of research examines how organisations are able to develop knowledge and 'routines' in order to guide their behaviours (Levitt & March, 1988). Organisational learning is a process, whereby organisations aim to incorporate and disseminate valuable experience and knowledge across its communities of practice over time, updating and replacing 'organisational memory' (Huber, 1991). Learning takes place through a variety of stimuli in order to correct errors, develop a new knowledge base, gain competitive advantage through innovation and reduce the time it takes to undertake actions and make decisions (Argyris & Schon, 1978; Shrivastava; 1983; Huber, 1991). The more an organisation is willing to learn and incorporate new knowledge and insight into its 'organisational memory', the more agile the organisation will be when faced with unknown situations and the likelihood of errors made in decisions and actions will be reduced. A learning organisation is described as being skilled at creating, acquiring and transferring its knowledge, modifying behaviours in order to reflect the new insights gained (Sinkula et al, 1997).

Organisational Learning Processes

Organisational learning is accomplished across a variety of processes, perspectives and methods. Organisations learn by encoding inferences from its own history into 'routines' (Levitt & March, 1988). These routines then guide behaviour among the organisation's communities of practice through forms, rules, procedures and strategies. There are several

views on how organisations learn: through direct knowledge acquisition, information distribution, information interpretation and organisational memory (Huber, 1991). Organisations can learn through direct experience, through interpreting the experiences of others and a history of events and through encoding knowledge and information into organisational memory (Levitt & March, 1988). These perspectives illustrate that organisations can learn through planned learning practices, directly seeking information through surveys and research, by distributing information across its communities of practice, govern how this information is best framed and interpreted and how the learning notes, information or knowledge is stored (Levitt & March, 1988; Huber, 1991).

Organisations also learn through four perspectives. These are adaptation, assumption sharing, development of knowledge base and institutionalised experience (Shrivastava, 1983). Adaptation outlines how organisations adapt to changes in their environment over time, adjusting behaviour to remain competitive (Cyert & March, 1963; Cangelosi & Dill, 1965; March & Olsen, 1976). Assumption sharing refers to how organisations respond to change within their internal and external environments, detecting and correcting errors (Argyris & Schon, 1978; Mitroff & Emshoff, 1979). This is performed through the sharing of assumptions and mental 'maps' between individuals. The development of a knowledge base is the process by which organisations build knowledge based upon the actions, outcomes and effects that these actions have had on their internal and external environment (Duncan & Weiss, 1978; Shrivastava, 1983). Institutionalised experience involves learning by doing, subsequently reducing the time it takes to produce goods and make decisions due to the repetition of activities over time (Abernathy & Wayne, 1974).

These learning processes are important when planning incident learning activities within the incident response capability. Current incident learning procedures and guidelines are action-oriented, focused upon the scheduling of meetings and the creation of reports. There is, however, no comprehensive or recognised meta-structure or learning model situated beyond this. Current incident learning literature focuses upon the acquisition of direct knowledge from staff involved in the incident and the distribution of this information to select parties. However, there are a wide range of direct knowledge acquisition processes available, including experiments, self-appraisals, experiments, unsystematic learning, vicarious learning, searching and noticing and grafting (Huber, 1991). There are also broader recommendations for comprehensive information dissemination to enable broad organisational learning that have not been actioned in incident learning (Huber, 1991). Information interpretation must be considered in how the incident information is assigned meaning by other staff, including the rapidity of feedback, the individual's personal knowledge and how they frame or view a problem. Organisational memory must also be considered - ie. how the organisation stores and retrieves that information over time (Levitt & McEvoy, 1988). An incident knowledge database can subsequently be used to store past incident data, successful actions and key learning notes.

Effective organisational learning, when combined with the post-mortem reviews of incident response processes provide an area for leverage. Simon (1991) describes how effective learning organisations are capable of innovation, assimilating new ideas and fighting 'entropy'. Shrivastava (1983) and Levit & March (1988) highlight that organisational learning can allow for the effective institutionalisation of cumulative experience, reducing the time it takes to produce goods and make effective decisions due to the repetition of activities over time. Ultimately, organisations must learn and 'unlearn' knowledge in order to reflect and adjust to its changing environment (Fiol & Lyles, 1985). Doing so will permit flexibility in their strategy, competitive advantage, a healthy corporate culture conducive to learning and an organisational structure that will permit innovation and the development of new insight. When related to incident response, the benefits of effective learning can be seen, potentially increasing agility and flexibility in process, increasing accuracy in decision-making, increasing efficiency in the incident response process and a wider understanding of security incidents and appropriate issues distributed among the incident response team due to the ingestation of a wider body of knowledge.

Single- and Double-Loop Learning Perspectives in Incident Learning

Through effective learning, organisations are able to detect and correct errors and issues within their structures, processes and activities in order to either carry on present policies or to question their underlying structures as a precursor to change (Agyris, 1976; McElroy, 1999). This discussion refers to the notion of single-loop and double-loop learning.

Single-loop learning is concerned with a more narrow and short-term focus concerning an organisation's 'action strategies', or those plans and rules that enforce organisation structures and beliefs. This is the position of most organisations (Rowe, 1996). An example, in the context of incident response, would be modifying the implementation of a control to better enforce a security policy.

In order for effective organisational learning to actually occur, organisations must focus on double-loop learning (Agyris, 1976). Double-loop learning questions the fundamental governing variables of the organisation behind its actions. The underlying rules, principles and knowledge of organisations will be challenged, leading to the 'active construction' of

different actions to take and rules to follow (Agyris, 1976; McElroy, 1999). When using double-loop learning, organisations will reconsider and alter their fundamental rules, policies, systems and processes in order to promote long-term change (van Niekerk & von Solms, 2004). Questioning the fundamental principles of policies and incorporating deep conceptual changes as part of a wider security change strategy is evidence of double-loop learning.

The difference between single-loop and double-loop learning is important when learning from incidents. Figure 2 illustrates this difference, highlighting that single loop learning will only establish specific actions in response to an issue.

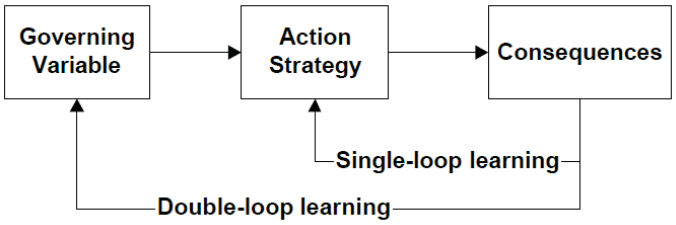

Figure 2: Organisational Learning for Incident Response (van Niekerk & von Solms, 2004)

The Informal Nature of Organisational Learning, Knowledge and Practice

Another important delineation within organisational learning refers to the formal and informal nature of learning. The concept of the 'informal' organisation refers to the understanding that, despite formalised structures, procedures and policy, an informal culture and routines will exist. The informal organisation consists of those activities not specified or represented in the official blueprints of the formal organisation (Scott, 1961). The informal organisation is represented by those communities, behaviours and actions that are not officially recognised by the formal organisation structures, but are still integral to the function of the formal organisation (Farris, 1979; Simon, 1979). Informal working communities, networks of individuals and knowledge, informal practices, workarounds and the like are all representative of the informal organisation.

Brown & Duguid (2002) describe the concept of business 'practice' and the informal organisation, whereby organisations and process can be viewed as 'machines' that are predictable in their behaviours and routines. However, the 'real view' of organisations are that they can be unpredictable and 'messy' (Shedden et al, 2009; Shedden et al, 2011). Parties must collaborate unofficially, share information, tell stories, share experiences and improvise in order to achieve their work goals. Organisational members will indulge not only in formalised process, but will also aim to find shortcuts and workarounds (Sasse & Flachais, 2005). Those informal organisational routines populated and acted upon via effective organisational learning infrastructures will include structures of beliefs, frameworks, paradigms, codes, cultures and knowledge that support formal routines (Levitt & March, 1988).

These routines can be transferred through formal means, such as education, mergers and personnel movement; however, informal learning will occur through socialisation within teams, imitation of others with more experience and 'professionalisation'. When examining organisational and individual learning and knowledge, Davenport & Prusak (1998), Brown & Duguid (2001) and Hislop (2009) outline that knowledge is informally embedded within the processes and practices of organisations. Though the formalised variants of learning and knowledge embedded through policy and training will exist, there will be a parallel and related level of learning via informal means through process and participation. Therefore, it is suggested in literature that effective organisational learning can be performed through formal classes, procedures, process and events, but informal learning mechanisms are just as critical (Shrivastava, 1983).

Though formal mechanisms of learning and change can be incorporated and are more likely to be recognised by organisations, an effective incident learning process must incorporate an informal focus as well. Formal training programs, alterations in policy and knowledge management systems are capable of capturing official records and perspectives. However, the focus in current incident response methods such as the NIST and SANS models ignore the 'soft side' of learning. That is, they do not leverage the workarounds, informal networks and workarounds that people pursue in conjunction with formal aspects of learning. Effective learning must therefore recognise and leverage those unofficial activities and networks of knowledge in addition to the formal mechanisms in order to best learn from and respond to future incidents.

Informal practice considerations are critical when learning from security incidents. Incident response occurs in stressful environments with a heavy emphasis on teamwork. Under such circumstances, workarounds and informal activities or

procedures will occur: Muhren et al (2008) demonstrates that during incidents, individuals default to their own informal networks of knowledge and procedures even though incident response processes may be highly structured.

Therefore, incident response will require both formal and informal learning activities and strategies in order to complement and reinforce the knowledge gained from incident learning. This is important for effective, holistic learning given Farris' (1979) and Shrivastava's (1983) assertions that informal learning and practice will support formal learning. Furthermore, recognising and reinforcing informal practices, knowledge and workarounds can enhance an organisation's ability to learn from incidents and improve future incident response. As Muhren et al (2008) has shown, incident response team members can successfully be given the freedom to pursue their own workarounds outside formalised structure. That is, informal practices can be leveraged to more effectively respond to incidents rather than pure reliance on formalised procedures. Building in flexibility and reinforcing informal avenues of knowledge acquisition, analysis and decision-making can lead to a more effective incident response capability.

PROMOTING LEARNING IN THE INCIDENT RESPONSE PROCESS

An effective incident response process must incorporate a learning strategy. Though quality incident response processes must ensure that they prepare, identify and eradicate incidents, the importance of post-mortems must be recognised. Effective post-mortem activities lead to the strengthening of organisational security policies, security management, improved training programs and alterations to incident response activities. The effects of learning through incident response has been demonstrated to avert major attacks and to lead to improvements to the incident response method as a whole (Melara et al, 2003; Stephenson, 2003).

This paper suggests that further research must be conducted to promote organisational learning research and theory in the context of incident learning activities. Currently, incident learning is focused upon activity-level procedures and recommendations. There are no higher learning models and processes associated with incident learning. Organisational learning literature provides a series of learning models and processes that can be incorporated into a meta-level incident learning method. This could be used to develop a holistic, insightful and comprehensive incident learning model that could acquire knowledge and insight across a variety of processes, disseminate the findings in a structured and recognised manner and store this information in organisational memory. In doing so, double-loop learning should be incorporated into incident response methods in order to gain comprehensive learning and feedback on the base structures and principles of the model itself, in addition to the activities, polices, management structures, tools and staff in the incident response process. There is the need to improve the expediency in incident response process feedback, moving away from an 'after the fact' approach as is the current norm and to move towards a more agile approach. Finally, the current emphasis is on providing feedback and learning through formal policy, presentation and reports. However, there is the need to recognise informal learning approaches and mechanisms prevalent in all organisations and incident response processes. These views are encapsulated in subsequent sections.

The incorporation of these propositions into existing models has the potential to significantly impact incident response methods. These perspectives will alter the incident learning activities conducted within the final phase of the method found in Figure 1. The application of organisational learning processes may lead to higher-level structures that would surround or sit above the incident response process. Faster turnaround in feedback may lead to additional learning loops in each phase, linking to the initial preparation phase but also to each independent phase. This view ensures that organisations are capable of learning from incidents during the activities, feeding this information and learning directly back to the incident response team at the time. However, formalised methods of incident response may change completely when considering unstructured incident response methods and informal learning.

Organisational Learning Strategies and Incident Learning

It is hence suggested that effective incident response processes must lean on organisational learning practices throughout the process. The current linear models loop back to the initial stage of the process in order to conduct post-mortem meetings, as demonstrated in Figure 1. Current methods are also focused on pinpoint activities to operate rather than providing comprehensive learning strategies and wide-perspective learning models. Little research has been conducted in examining effective learning activities and how to improve incident response activities. Cooke (2003) and van Niekerk & von Solms (2004) outline double-loop learning as a means of effectively gaining knowledge from security incidents. These studies aim to feed the consequences of an incident back through to improve the underlying organisational policies and security processes, improving the incident response capability as a whole.

For effective organisational learning to occur, there must be a higher-level view of incident learning utilising the models and processes from literature. This will in turn lead to a systematic, structured and comprehensive strategy for effective

incident learning. Organisational learning theory states that individuals and groups must adopt direct knowledge acquisition, information distribution, information interpretation and also consider the effects of organisational memory (Huber, 1991). From an incident learning perspective, relevant knowledge and information must be shared among relevant parties and dispersed through relevant functions in order to enable double-loop learning systems in the first instance and to subsequently improve incident learning processes, management, response times, procedures, manuals and training. The effective consideration of organisational learning effects such as effective knowledge acquisition and information distribution will allow organisations to obtain knowledge across departments and spread this knowledge and information throughout the organisation to any relevant party. The encoding of relevant information and knowledge into a repository and back into its routines will ensure that they exist in organisational memory. Therefore, we suggest that:

> **Proposition 1:** incident learning models must be developed to appropriately map effective organisational learning processes to incident response.

Double-Loop Incident Learning

Double-loop learning is critical for incident learning activities. Learning models from Agyris (1976), Agyris & Schon (1977), Cooke (2003) and van Niekerk & von Solms (2004) emphasise the use of double-loop, generative learning over single-loop learning. Double-loop learning is crucial for the incident response process, ensuring that base values, policies and strategies are brought to question, possibly resulting in the redevelopment of ideals, culture, strategy, policies and procedures at a base level. By contrast, single loop learning attempts to invoke responses to shift or alter current policies, focusing upon the immediate actions (van Niekerk & von Solms, 2004). McElroy (1999) links double-loop learning to '2nd generation knowledge management', articulating that double-loop learning deals with the creation of knowledge itself, propagating this knowledge through formal and internal channels to update and refresh norms at a fundamental level.

However, while double-loop learning is indeed critical for incident response, how incident response teams actually learn from incidents and manage this knowledge is unclear. As previously mentioned, most incident response literature focuses upon technical intrusion types and specific technological controls. There are few studies that specifically discuss how organisations learn and adapt their incident response processes and activities in the wake of attacks, barring the incident response methodology literature themselves. Therefore, this paper makes the following proposition:

> **Proposition 2:** double-loop learning must be facilitated in incident learning activities to ensure that not only plans and policies are questioned, but their underlying structures and 'governing variables'.

An interesting role for IR processes relates to security risk management. The values assigned to the probability and impact of individual risks is typically ‘gut-feel’ or hypothetical. Incident response can be a source of concrete data, reflecting what is actually happening in the organisation. This data can be used to inform the risk assessment process resulting in much more accurate risk assessments and subsequent strategies. However, this facility will only be available if organisations take the necessary steps to learn from incidents and provide feedback into related organisational security processes such as security risk management.

Agility in Incident Learning Feedback

Greater speed and agility in learning from incidents and of the incident response activities is required. The current emphasis of current incident learning is to engage formal learning mechanisms ‘after the fact’, or upon completion of an incident. However, feeding such information back post-incident may result in an erosion of knowledge and insight if left for too long (Northcutt, 1998). Greater speed in response is necessary to ensure that all relevant information, key learning notes and knowledge are captured and disseminated to the team as quickly as possible, perhaps even as the incident occurs. Through faster turnaround of feedback during incidents, relevant insight and knowledge can be gained to be used in order to reinterpret how incident response is performed. This in turn may improve incident response procedures and practices with greater expediency, leading to the following proposition:

> **Proposition 3:** organisations must incorporate feedback from incident learning activities through shorter learning cycle turnarounds.

The Need to Incorporate Informal Approaches in Incident Learning

Organisational responses to major incidents tend to be haphazard and complex (Northcutt, 1998). It is known in incidents that individuals will revert to their personal networks, skills and knowledge when responding to stressful events during

the course of an incident (Welks, 2003; Muhren et al, 2008). Formal mechanisms such as process and procedure can and often do break down due to the evolving and difficult environments created by such incidents.

In informal environments, formal learning processes may not be effective in isolation as individuals will need to support formal knowledge and learning mechanisms with informal learning. Muhren et al (2008) illustrates how individuals can effectively leverage informal knowledge throughout the organisation when responding to incidents. Specifically within high-reliability organisations, it was found that formalised routines and procedures tended to break down during incidents. Empowerment of employees was determined to be more effective, permitting greater flexibility and innovation when able to leverage their own experience and networks of knowledge, distributed among individuals across the organisational structure. Formal learning practices in informal environments such as this must be used in conjunction with informal methods that support the informal practices upon which the official process relies upon.

Effective incident learning even in formalised incident response processes and environments must still incorporate an informal focus, given that informal 'messy' view of organisational practice embedded in process (Brown & Duguid, 2002; Shedden et al, 2011). However, current post-mortem activities generally rely on formal reports and presentations to articulate the effect of policies, procedures and performance (Grance et al, 2004). While this may be an effective means of feeding learning notes and knowledge to security managers and the incident response team, there is the need to recognise informal routes for learning to ensure complete and holistic knowledge transfer and understanding. the imposition of formalised policy, procedure and management can be performed, there must be opportunity for incident response teams to learn through informal networks. Different types of recognised learning procedures and steps can be incorporated to promote effective knowledge management and organisational learning through informal procedures, such as organisational self-appraisal, unintentional or unsystematic learning and grafting (Huber, 1991). These learning mechanisms take the product of group interactions and knowledge discovered through informal, interpersonal networks, however unstructured they may be, in order to grow organisational knowledge pools.

Understanding how knowledge is managed and spread at the individual and team levels can assist in the facilitation of effective knowledge management and organisational learning. For instance, ‘grafting’ refers to learning by a team through the acquisition of a new member, with their own knowledge and insights that can be shared. This individual can codify their knowledge, or train others through seminars and personal interactions to scaffold this knowledge across to informally improve team procedures and process. Leading from this, we have made the following propositions to suggest an informal learning and practice perspective to incident response and incident learning:

> **Proposition 4:** to promote effective and holistic learning, incident learning activities must include formal and informal perspectives. This will disseminate key knowledge to management and staff in a comprehensive manner, facilitating and assisting formal processes through supportive informal practices.
>
> **Proposition 5:** incident learning must still occur in environments and situations where incident response activities are unstructured and informal (eg. Muhren et al, 2008).

CONCLUSION

Current incident follow-up and post-mortem activities represent a critical phase in the incident response process. However, incident learning is not a current research focus. Incident learning is currently viewed as a formal mechanism for improving organisational security incident response processes and as a source of information, used to improve procedures, policies, security training activities and implement new controls. However, current approaches are formalised and high-level. Organisational learning literature suggests that the implementation of organisational learning processes can result in the realisation of large benefits in incident learning and incident response. Through the implementation of organisational learning processes that acquire and make sense of knowledge across a variety of means, incident response and security structures can be improved and disseminated. Organisational learning concepts such as double-loop learning are also critical to ensure that organisations learn appropriately, not only focused upon short-term changes, but are also capable of questioning underlying security and incident response structures to facilitate long-term, rigorous change where necessary. Finally, incident learning must be able to incorporate both formal and informal means of learning. While current incident learning activities focus upon formalised methods of learning such as meetings, presentations and reports, informal learning processes such as socialisation, imitation and the movement, or 'grafting', of personnel. Through effective incident learning, organisations will be more capable of managing the incident response capability, making improvements where necessary and feeding key learning notes back into security processes, management structures, policies and procedures.

REFERENCES

Abernathy, W.J. & Wayne, K. 1974. 'Limits of the learning curve'. *Harvard Business Review*, vol.52, no.5.

Argyris, C. 1976. 'Single-Loop and Double-Loop Models in Research on Decision-Making', *Administrative Science Quarterly*, vol.21, no.3, pp.363-375.

Argyris, C. & Schon, D. 1978. *Organisational Learning*. Reading, MA. Adderson-Wesley.

Brown, J.S. & Duguid, P. 2001. 'Knowledge and Organisation: A Social-Practice Perspective'. *Organisation Scien*ce, vol.12, no.2, pp.198-213.

Brown, J. S. and P. Duguid (2002). *The Social Life of Information*. Harvard Business School Press.

Cangelosi, V.E. & Dill, W.R. 1965. 'Organisational learning: observations toward a theory. *Administrative Science Quarterly*, vol.10, pp.175-203.

Chuvakin, A. 2005. *Five mistakes of incident response*. [online] Available at: http://www.computerworld.com/s/article/100720/Five_mistakes_of_incident_response?taxonomyId=17&pageNumber=1. Last accessed 19th September, 2010.

Cooke, D.L. (2003) 'Learning from Incidents'. *Proceedings of the 21st International Conference of the System Dynamics* Society, NY, USA.

Cyert, R.M. & March, J.G. 1963. *A Behavioural Theory of the Firm*. Englewood Cliffs, NJ. Prentice-Hall.

Davenport, T. H. & L. Prusak (1998). *Working knowledge: how organisations manage what they know*. Boston, Harvard Business School Press.

Dhillon, G. & J. Backhouse (2001). 'Current directions in IS security research: towards socio-organisational perspectives'. *Information Systems Journal*, vol.11, no.2.

Duncan, R.B. & Weiss, A. 1978. 'Organisational learning: implications for organisation design'. *Research in Organisational Behaviour*, Greenwich, Conn. JAI Press.

Goh, S.C. 1998. 'Toward a Learning Organisation: The Strategic Building Blocks', *SAM Advanced Management Journal*, Spring.

Grance, T., Kent, K. & Kim, B. 2004. *Computer Security Incident Handling Guide – Recommendations of the National Institute of Standards and Technology*. Technology Administration, US Department of Commerce.

Farris, G. F. (1979). 'The Informal Organisation in Strategic Decision-Making'. *International Studies of Man and Organisation*. vol.9, no.4, pp.37-62.

Fiol, C.M. & Lyles, M.A. 1985. 'Organisational Learning', *The Academy of Management Review*, vol.10, no.4, pp.803-813.

Hadgkiss, J. 2006. *Computer Security Incident Response Teams: Exploring the Incident Learning Capability*. Department of Information Systems. Melbourne, University of Melbourne.

Hislop, D. (2009). *The practice-based perspective on knowledge*. Knowledge Management in Organisations. New York, Oxford University Press: 27-40.

Huber, G.P. 1991. 'Organisational Learning: The Contributing Processes and the Literatures', *Organisation Science*, vol.2, no.1, pp.88-115.

Jaikumar, V, 2002, “Organisations should build an incident response team”, *ComputerWorld Canada*, vol.9, no.16.

Kelver, L. (2002). *Incident Response in a Global Environment*. GSEC Version 1.2b, SANS Reading Room.

Killcrece, G., Kossakowski, K-P. et al (2003). *Organisational Models for Computer Security Incident Response Teams (CSIRTs)*. Pittsburgh, PA, Carnegie-Mellon Software Engineering Institute.

Knight, R. & Pretty, D. (1995). *The Impact of Catastrophes on Shareholder Value*. The Oxford Executive Research Briefings, University of Oxford.

Kossakowski, K-P., Allen, J. et al. (1999). *Responding to Intrusions*. Pittsburgh, PA, Carnegie Mellon University.

Levitt, B. & March, J.G. 1988. 'Organisational Learning', *Annual Review of Sociology*, Vol.14, pp.319-340.

Mandia, K. & Procise, C. (2002). *Incident response: investigating computer crime*. New York, Osborne/McGraw-Hill,

March, J.G. & Olsen, J.P. 1976. *Ambiguity and Choice in Organisations*. Universitetsforlaget, Bergen, Norway.

McElroy, M.W. 1999. *Double Loop Knowledge Management*. Macroinnovation Associates, LLC.

Melara, C., Sarriegui, J.M. et al. (2003). *A System Dynamics Model of an Insider Attack on an Information System*. From modeling to managing security: Kristiansand, Norway, Høyskoleforlaget AS - Norwegian Academic Press.

Mitroff, I. & Emshoff, J.R. 1979. 'On strategic assumption-making: a dialectical approach to policy and planning'. *Academy of Management Review*, vol.4, no.1.

Mitropolous, S., Patsos, D. & Douligeris, C. (2006). 'On Incident Handling and Response: A state-of-the-art approach', *Computers & Security*, vol.25, pp.351-370.

Muhren, W., van den Eede, G. & van de Walle, B. 2008. 'Organisational Learning for the Incident Management Process: Lessons from High Reliability Organisations'. *Journal of Information Systems Security*, vol.4, no.3, pp.3-23.

Murray, J. (2007). *Analysis of the Incident Handling Six-Step Process*. SANS Reading Room.

Northcutt, S. (1997). *Computer Security Incident Handling, Step-by-Step*. The SANS Institute.

Novak, C.J. (2007). 'Investigative response: After the breach'. *Computers & Security*, vol.26, no.2, pp.183-185.
Osborne, T.R. (2001). *Building an Incident Response Program to Suit Your Business*. GIAC Security Essentials, SANS Reading Room.

Rowe, C. (1996). 'Evaluating management training and development: revisiting the basic issues', *Industrial and Commercial Training*, Vol. 28 Iss: 4, pp.17 - 23.

Sasse, M. A. & I. Flechais (2005). *Usable Security: Why do we need it? How do we get it?*. Security and Usability, O'Reilly Media: 13-30.

Scott, W.G. (1961). 'Organisation theory: an overview and an appraisal'. *Journal of the Academy of Management*, vol.4, no.1.

Shedden, P., W. Smith, et al. (2009). 'Towards a Knowledge Perspective in Information Security Risk Assessments – an Illustrative Case Study'. *20th Australasian Conference on Information Systems, Melbourne, Australia*.

Shedden, P., W.Smith, et al. (2011). 'Incorporating a Knowledge Perspective in Security Risk Assessments'. *VINE Journal of Knowledge Management*. Article in press.

Shrivastava, P. 1983. 'A Typology of Organisational Learning Systems', *Journal of Management Studies*, vol.20, no.1.

Simon, H. A. (1979). "Rational Decision Making in Business Organisations." *The American Economic Review* vol.69, no.4, pp.493-513.

Simon, H.A. 1991. 'Bounded Rationality and Organisational Learning', *Organisation Science*, vol.2, no.1.

Sinkula, J.M., Baker, W.E. & Noordewier, T. 1997. 'Organisational Learning: Linking Values, Knowledge and Behaviour', *Journal of Academy of Marketing Science*, vol.25, no.4, pp.305-318.

Siponen, M. T. (2005). 'Analysis of modern IS security development approaches: towards the next generation of social and adaptable ISS methods'. *Information and Organisation*, vol.15.

Spears, J. (2006). *A Holistic Risk Analysis Method for Identifying Information Security Risks*. Security Management, Integrity, and Internal Control in Information Systems. Boston, Springer Boston. 193/2006, pp.185-202.

Stephenson, P. (2003). 'Conducting Incident Post Mortems', *Computer Fraud and Security*, April.

Turner, P. (2007). 'Applying a forensic approach to incident response, network investigation and system administration using Digital Evidence Bags'. *Digital Investigation*, vol.4, no.1, pp.30-35.

West-Brown, M.J., Stikvoort, D. et al. (2003). *Handbook of Computer Security Incident Response Teams (CSIRTs), Second Edition*. Pittsburgh, PA, Carnegie-Mellon Software Engineering Institute.

Whitman, M. E. & H. J. Mattord (2005). *Principles of Information Security*, Thomson Course Technology.

Wiik, J., Gonzales, J.J., & Kossakowski, K-P. (2005). 'Limits to Effectiveness in Computer Security Incident Response Teams'. *Twenty-Third International Conference of the System Dynamics Society*. The System Dynamics Society, Boston, MA.

van Niekerk, J. & von Solms, R. 2004. 'Organisational Learning Models for Information Security', *The ISSA 2004 Enabling Tomorrow Conference*, 30 June-2 July, Gallagher Estate, Midrand.

van Wyk, K. & Forno, R. (2001) *Incident response*. New York. O'Reilly.

Zhang, Z., Ho, P-H et al. (2009). 'Measuring IDS-estimated attack impacts for rational incident response: A decision theocratic approach'. *Computers & Security*, vol..28, no.7.