Association for Information Systems
AIS Electronic Library (AISeL)

ACIS 2011 Proceedings | Australasian (ACIS)

2011

# Informal Learning in Security Incident Response Teams

Piya Shedden
*Deloitte*, pishedden@deloitte.com.au

Atif Ahmad
*The University of Melbourne*, atif@unimelb.edu.au

Anthonie B. Ruighaver
*Deakin University*, tobias@deakin.edu.au

# Informal Learning in Security Incident Response Teams

Piya Shedden
Deloitte Touche Tohmatsu
Melbourne, Australia
Email: pishedden@deloitte.com.au

Atif Ahmad
Department of Information Systems
University of Melbourne
Australia
Email: atif@unimelb.edu.au

Anthonie B. Ruighaver
School of Information Systems
Deakin University
Australia
Email: tobias@deakin.edu.au

## Abstract

*Information security incident response is a critical security process for organisations aiming to provide an effective capability to recover from information security attacks. A critical component of security incident response methodologies is the ability to learn from security incidents on how to improve the incident response process in particular and security management in general. Best-practice methodologies and existing research in this area view the incident response process as highly formal and structured while providing recommendations on learning in formal feedback sessions at the conclusion of the incident investigation. This contrasts with more general organizational learning literature that suggests learning in organizations is frequently informal, incidental and ongoing. This research-in-progress paper describes the first phase of a project. Results from a focus group of experts indicates that response to incidents is largely informal suggesting a new Incident Response model is needed that incorporates informal learning practices.*

**Keywords:**

Security incident response, organisational learning, incident learning

## INTRODUCTION

Information security incident response is a critical security process for organisations, providing an effective capability to identify, eradicate, recover from and learn from information security attacks. A critical component of security incident response methodologies is the ability of the Computer Security Incident Response Team (CSIRT) and the wider organisation (eg. senior management, the security risk team, the security policy team and other elements of the information security function) to learn from security incidents. Enabling effective learning within the CSIRT will improve training and readiness to any future instances of that attack. Learning and communication across the organisation will have wider-reaching impacts, such as the implementation of controls, changes to the organisational risk profile and additional budget allocations.

Best-practice security incident response methodologies such as NIST SP800-61 and SANS Six-Step view incident response as a highly structured and formal process. These methodologies provide recommendations on aspects of learning, such as formal presentations and reports to senior management in order to influence future security activities and add to the organisational body of knowledge.

However, more general organisational learning research outlines that formal learning paradigms must be aligned with the informal organisation and informal learning practices. For learning to be most effective, organisations must recognise the informal culture and undercurrents naturally occurring and developing within teams and groups. 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).

There is little research into effective security incident learning through follow-up activities in CSIRT methodologies. Research in this area emphasises learning about the technical aspects of intrusions, specifically around vulnerabilities, new attack vectors and their eradication (Mitropolous et al, 2006; Novak, 2007). While this focus is important in maintaining an outlook on the new threats and attacks that may cause harm to organisations, there has been little research on informal learning processes through which organisations can derive much value.

The scope of this paper is limited to learning within the incident response team only (as opposed to the organisation in general). Accordingly, although a focus group was conducted with leading security and CSIRT practitioners on a broad range of issues concerning incident response in organisations, the discussion in this paper will be limited to data collected about learning within the CSIRT. This paper argues that security incident response is a highly informal process despite literature and industry focus on formal and structured plans. Therefore, learning effectiveness can be increased through a combination of formal and informal approaches rather than just formal reporting as suggested by current leading methodologies.

The paper begins with background on the incident response process followed by a brief overview of literature in the organizational learning space. Results from the focus group are then presented after which the paper discusses the main theme on informal learning in organizations. Finally, an informal learning model for incident response will be presented which will be tested in the next phase of this research project.

## BEST-PRACTICE METHODS OF SECURITY INCIDENT RESPONSE

Security incident response refers to the process by which organisations engage dedicated or adhoc teams to identify and treat information security incidents (West-Brown, 2003; Wiik et al, 2005). Depending on the scope of the team, they can be either technical or multidisciplinary, featuring members across a variety of business lines, balancing a range of skills that may include the technical, diplomatic and organisational (Murray, 2007).

The formal process of security incident response is summarised in Figure 1:

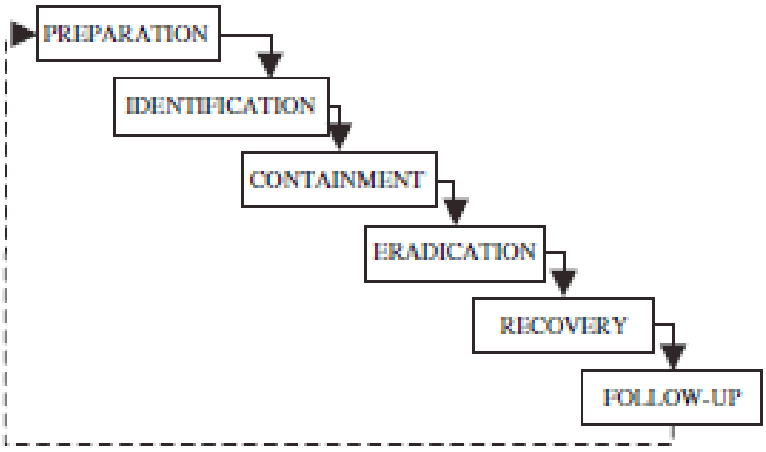


Figure 1: the Incident Response Process (Mitropolous et al, 2006)

The phases of this process are described in the following table:

| 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. |
| Identification | Identification procedures are engaged, determining whether an incident exists. The incident should be validated, the scope and potential impact determined and how the incident occurred. |
| Containment | Containment prevents incidents from worsening. Two key objectives are the prevention of further contamination of the system and the preservation of evidence for potential future legal proceedings. |
| Eradication | Eradication activities clean up after the incident for example removing attack vectors from , systems. |
| Recovery | Recovery restores 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: Incident Response Phases (Northcutt, 1998; Kelver, 2002; Grance et al, 2004; Murray, 2007)

The SANS and NIST methodologies state that follow-up activities should be engaged to learn from the incident and the response process itself to feed back into the preparation phase (Northcutt, 1998; West-Brown et al, 2003; Grance et al, 2004; Murray, 2007). Such activities can occur throughout the process, such as note-taking using predefined forms to document actions. Other activities may include official debriefing sessions, formal reporting to senior management and presentations. As such, effective follow-up activities are a key learning process that can be used to spread knowledge of threats and attacks, influence security risk profiles and improve the security incident response process itself. Successfully leveraging follow-up processes allows for better preparedness prior to further incidents, the spread of this knowledge will have a subsequent flow-on effect, advancing staff expertise and thinking.

However, despite its importance in the context of incident response, the 'follow-up' phase of the security incident response process is not widely researched. Current security incident response focuses on technical aspects, such as identification of new attack types, response techniques and forensics (Mitropolous et al, 2006; Novak, 2007). This technical focus is not surprising as security research tends to consider technical aspects rather than holistic, socio-organisational perspectives (Dhillon & Backhouse, 2001; Siponen, 2005; Zafar & Clark, 2009). Additionally, current security research does not consider the implications of the informal activities, undercurrents and processes within organisations that can often undermine structured, formal security perspectives.

## BACKGROUND ON LEARNING IN SECURITY 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 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).

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 Levitt & 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.

### The Informal Nature of Organisational Learning, Knowledge and Practice

Another important delineation within organisational learning refers to the formal and informal nature of learning. Formal learning is typically 'institutionally sponsored, classroom-based, and highly structured' (Marsick and Watkins, 1990, p.12). Whereas informal learning has the following characteristics (Marsick and Volpe, 1999):

- It is integrated with daily routines
- It is triggered by an internal or external jolt
- It is not highly conscious
- It is haphazard and influenced by chance
- It is an inductive process of reflection and action
- It is linked to the learning of others

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). 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' (Removed for Refereeing). 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) 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).

## ISSUES IN EFFECTIVE SECURITY INCIDENT RESPONSE: A FOCUS GROUP

To explore organisational learning concepts within follow-up processes, a focus group was conducted with leading information security and security risk professionals.

### Methodology

Focus groups are a capable research method for this form of research, providing a platform to gain insight through mutual discovery and interaction. Such interaction can in turn provide new insight and ideas that are useful for such exploratory studies where little is known. Though questions could be asked through interviews or case studies to draw upon the experiences of one person, the actual generation of ideas and often unexpected directions that result are a key element of focus group research (Kitzinger, 1995). Furthermore, focus groups are an ideal data collection method to operate prior to engaging in deeper organisational research, allowing for the researchers to refine ideas and concepts.The use of focus groups are appropriate for this form of research given that this is an exploratory study conducted prior to an in-depth series of cases. The objective of this study was to fill an existing gap in current understanding on how security incident response occurs in organisations and to gain insight into the effective means by which CSIRTs and organisations learn from security incidents.

We conducted a 2.5 hour focus group with five security and forensics experts (see table 2) to examine the nature of 'real' security incident response as opposed to the formalised methodologies and technically-oriented research currently on offer. Questions posed in this focus group were designed to be open-ended around the nature of security incident response in organisations at its most basic level. Perceptions of incidents and plans by management were explored, in addition to current learning activities (if they exist). Desired learning processes and links to concepts and propositions based on organisational learning literature were then discussed in an effort to generate debate and stimulate new ideas and directions.

| Name | Role Description and Experience |
|---|---|
| Risk Director | Set up CSIRT capability for an Australian bank and its forensics practice. Managed the CSIRT at the bank for many years whilst collaborating with law enforcement and security practitioners to investigate e-crime and protect from attacks. Currently a security consultant working with organisations in the retail and financial industries. |
| Forensics Director | A former security consultant who is now a senior manager of a forensics practice within a large international consulting organisation. Is responsible for investigations and the forensic technology team. Is involved in CSIRTs primarily through engagement in the follow-up processes to determine origin and methods of attacks and future preventative measures. |
| PenTest Director | A security consultant that provides services around proactive security measures and controls, implementing and reviewing the security of new software and penetration testing. Often involved in the preparatory phases of CSIRT methodologies. Has also examined environments post-incident to recommend control changes based on the method of attack. |
| Forensic Analyst | A former researcher who earned her PhD in the field of artificial intelligence, the Forensic Analyst has 5 years experience working as a forensics consultant, working on CSIRT projects in post-mortem activities. Has recently transferred into the provision of preparatory phases, providing advice for preparedness around security controls through penetration testing and web application security consulting. |
| CSIRT Manager | Holds 30 years' experience in IT security, notably in networking and perimeter security. Is currently the CSIRT manager of a major Australian bank. |

Table 2: Description of Focus Group Participants

**Focus Group Results: CSIRTs and Security Incident Response**

The participants presented an informal view of security incident despite the dominant focus on formal, structured response methodologies in literature. The issue of panic was a common theme when describing experiences with security incidents and CSIRTs who were either suffering from an incident or were attempting to recover and conduct post-mortem activities. When describing this current state, the Forensics Director explained that:

*'… we often go into organisations that I think are very mature in their security incident response process and procedures and teams that they've got in place. But it's fair to say, once an incident does actually happen with an incident that's of severe magnitude and impact, we get called in and no matter how well-polished you are and how well-trained you are, there's always that panic'*

The focus group traded experiences regarding ‘panic’, including the prevalence of non-dedicated CSIRTs in many organisations due to a lack of expertise and funding. The Risk Director further reinforced this:

*'You kind of have the conversation with the CSIRT team and saying 'OK, are you prepared for this particular event?'. 'Yes, yes, we're prepared'. 'Can you show me the plan you've got in place or can demonstrate what process you're going to follow?'. 'Yes, here it is'. And then, the moment that an incident comes in or hits the fan… it gets put on the corner of the table and things just go into - what do you call it? - informal communication channels...'*

Ultimately, the collective experience outlined that when faced with highly stressful situations, people tend to feel pressured and unsure, or turn to other sources of expertise in order to resolve the situation. People, even trained individuals, were described to tend to default to informal communication channels, with the official plan 'put in the corner' (Risk Director). Such actions can be as a result of improper training and knowledge transfer, the stress of the situation presented to the CSIRT, a lack of effective materials and equipment and a lack of senior management support.

However, the views of the focus group ran against those of the CSIRT Manager. The CSIRT Manager instead described that discipline and training through management of learning and solidification of a base process could lead to effective incident response:

*'Having the discipline to follow the playbooks and that you've practiced, knowing that the best way you're going to get out of it is to keep your head and follow the rules that you've laid out in advance and not invent it on the fly. Have a reproducible process that can then be refined and based on the post-incident analysis.'*

This is important in considering how incident learning should occur. The above emphasises that business practice and encoded knowledge are critical underpinnings for effectively and successfully responding to incidents. This is consistent with the SANS and NIST methodologies that recommend simulations be performed as part of effective incident response. Through simulations, CSIRTs would be able to hone their skills and gain familiarity with the process, activities, equipment, communication channels, administration and the other team members.

However, this view was tempered by the focus group's experiences around the motivations for building structured security incident response methodologies. The Risk Director admitted that many organisations that he has dealt with elected to implement formal methodologies and build dedicated teams. However, these processes were often driven, developed and implemented for reasons other than to improve the security incident response capability:

*'it's absolutely astounding to see people that have spent 3 months planning for a security incident previously with beautifully constructed documentation, throw it all out the window and go 'OK, yes, that's to keep the auditors happy. Now, what are we really going to do?"*

Though robust methodologies and documentation could be developed and key staff trained, the collective experience of the focus group was that this is often performed to meet external requirements. Once the methodologies had been engaged, there was often little involvement, simulation, update, preparation or follow-up to grow and improve the process over time. Learning activities, as a result, did not appropriately leverage the security incident response capability. Such security incident response can be effective, however, if driven instead by a requirement and desire to learn, adapt and improve.

**Focus Group Results: The Balance between Formal and Informal Learning**

As was indicated from the first quote by the Risk Director in the previous section, in the face of even heavily formalised and structured incident response processes, there is still a strong sense of panic in some cases and a high degree of informal communication and networks of knowledge. The participants described that the very nature of security incident response does have a formal basis, but more often than not, informal workarounds and routines are engaged.

The focus group explored the mechanisms by which CSIRT members typically learned, whether through formal or informal learning practices. The CSIRT Manager described his experiences in dealing with post-incident analysis:

*'…you can do just wargames on the desktop and you can say 'well, we would've ended up down here; do we have to mitigate for that?'. Well, we don't, we never thought of that particular sequence of events or scenarios. So it just goes to show that it depends on your imagination and how much time and resources you've got. You can ferret an incredible amount out of incidents.'*

The CSIRT Manager describes a casual process of brainstorming possible sequences of events followed by reflection on the likelihood that they would occur. The reflection and hapahazard approach are key characteristics of informal learning as described by Marsick and Volpe (1999). Further characteristics of informal learning can be seen from a statement of the Forensic Director:

*'When we take a client through a situation, as we go through that incident response process, as we're going through contain, solve, identify, investigate, etc, we're providing various stakeholders with informal learning through our conversations and sharing our experience with them.'*

The forensic director is acting in the capacity of a consultant. From the perspective of the client, this learning process involves linking to others and reflection on a (incident response) process. The focus group was adamant that the 'real learning' from security incidents occurs through informal learning processes. This links strongly to the manner in which an organisation engages in security incident response.

The group felt that informal learning was crucial to CSIRTs and to security practitioners in general. The Risk Director described that 'the emphasis on the informal is still absolutely vital. I can get someone straight out of university. I couldn't put them immediately into a role like [PenTest Director] has'. The argument of the panel was that informal learning played a key role in effective participation in CSIRTs and the education of new

members as they entered the learning community. This in turn facilitated a greater capacity and ability to response to incidents. Though formalised organisational learning processes such as induction, presentations and structured manuals could form part of an overall learning strategy, it is through informal knowledge acquisition that this learning will be assigned meaning.

This was reinforced when discussing the sources of learning within security incident response. While formalised training programs could prepare a team to a certain extent, the informal learning through experience, conversation and observation were critical, as the Risk Director elaborated:

*'[Pentest Director] and everyone else around the table here, as a result of a security incident, have you ever received formal training or learning that has come out of that? Typically, you learn from the incident itself.'*

The group agreed that informal learning was the basis upon which most critical learning was performed – the rationale behind frequent information security industry conferences, online forum activity and 'corridor conversations' (as described by the CSIRT Manager). Ideally, this informal learning should form the 'building blocks' of 'continuous improvement', with formal learning as a means of supporting the informal learning. The focus group pondered that perhaps the formal and informal boundaries of incident response and learning from the incident would shift, dependent on the nature of the incident and the maturity of the organisational CSIRT capability. When a description of formal and informal learning was provided, the CSIRT Manager provided insight based on experience:

*'It comes back to the level of maturity of the organisation. If there is no major incident management process which incorporates a post-incident review, the review being the formal bit, then it is all gonna be informal, so again, 'it depends' is the answer... [this description] captures what happens and the proportions and the exact widths of the rectangles with formal and informal, will slide back and forth and vary depending on the incident type and the maturity of the organisation and things like that. The concept of formal and informal learning is almost a self-evident truth - it's how we learn in life.*

This encapsulates the several key issues within security incident learning. Reinforcing the view that current follow-up processes are 'the formal bit', or a structured series of activities designed to drive change in the response capability in security-mature organisations. However, both formal and informal learning are mutually constituted, where one leverages off the other to drive effective security incident learning.

## DISCUSSION

The focus group established that organisational learning was key, in order to facilitate continuous improvement of the security incident process itself. The nature of security incident response was explored, with stories of panic and the common use of informal communication channels and knowledge networks in order to resolve incidents distinct from the formal, structured methodology. This in turn could be seen as one of the drivers for the informal learning requirement found in CSIRTs.

### Informal Response to Incidents

Despite the focus on formal planning for incident response in literature and best-practice standards, the focus group agreed that in their experience organisations tend not to consult their formal plans and procedures. They described the nature of the response from organisations as a 'panic'. It is therefore apparent that even in mature organisations with established security incident response processes, there is a default to workaround activities (Sasse & Flachais, 2005) and informal networks of knowledge. Indeed, they are not immune to the 'murkiness' described by Brown & Duguid (2002). Here, the socio-organisational view of processes – and information security – cannot be adequately expressed through formalised and technology-oriented perspectives (Dhillon & Backhouse, 2001; Siponen, 2005). Such informal undercurrents can often undermine the structured, rehearsed official view of organisational processes (Brown & Duguid, 2002).

Therefore, researchers and industry practitioners must accept that informal activities will occur below the surface in security incident response. The design and development of security incident response methods could subsequently factor informal approaches into the formalised structure. Such a method could possibly provide the rigour of the formal structure (a reproducible process that can then be refined and based on the post-incident analysis), whilst giving concession that during times of crisis, panic and stress, workarounds will drive different-than-expected activities and outcomes. Muhren (2008) has taken this a step further, suggesting that CSIRTs be given a degree of autonomy (but with accountability) in responding to incidents, free to leverage informal networks of knowledge and take action based on personal experience. This provides an understanding that, though limited purely to the containment and eradication stages, the recognition and integration of informal processes into structured methodologies could result in a highly effective security incident response capability.

**Informal Learning**

The focus group considered that the majority of key learning in the security incident response process was informal. The behavior described by the focus group participants had all of the six characteristics of informal learning described by Marsick and Volpe (1999). An incident can be characterised as a 'jolt' triggered by an external event which results in a 'panic' response from IR professionals where an available set of formal plans is ignored in favour of unsystematic activities (and corresponding reflections) that are strongly influenced by informal networks and channels of communication. This 'informal' reaction to an external event is integrated into the routine of the business and is about as frequent as incidents themselves (even if it is not a daily occurrence).

Most of the learning is performed 'from the incident itself', where an 'incredible amount' of information can be gleaned from a post-incident analysis. Such information and knowledge can only be acquired through experience and practice, whether it be through simulation and rehearsal or conversation and observing others. It appeared that the knowledge acquired and disseminated across CSIRTs is deeply tacit in nature. Formal metrics can be applied to quantify variables and outline effectiveness in specific response categories such as communication, the current control environment and timeliness in response. However, this does not necessarily lead to actionable learning outcomes. There must be recognition that critical knowledge is embedded within organisational processes (Davenport & Prusak, 1998; Hislop, 2009). Such knowledge can then be recognised and externalised, internalised or socialised to effect change in the process (Nonaka, 1994).

The focus group discussed learning relationships akin to apprenticeships (Removed for Refereeing). Here, new members would need to be integrated into the team in order to gain an adequate understanding of relevant activities, threats and attacks. The recognition of the need to socialise and internalise such tacit knowledge (Nonaka, 1994) within a CSIRT could provide greater adaptability and flexibility in the security response environment. CSIRT members would grow their knowledge and, as reported previously, incorporate new insights into organisational memory (Huber, 1991). This would in turn lead to great resilience when dealing with the unknown, a reduction in errors and increase in accuracy of future actions (Argyris & Schon, 1978, Shrivastava, 1983; Huber, 1991). Institutionalising this experience would also reduce the time of decisions made during security incidents (Shrivastava, 1983; Levitt & March, 1988). The emphasis on growing informal learning could subsequently increase the agility and flexibility of the security incident response process. The accuracy of informal learning from security incidents, however, must be monitored to ensure that the team is not 'sharing things that are wrong and incorrect, etc'.

## A LEARNING MODEL FOR SECURITY INCIDENT RESPONSE

Given all six characteristics of informal learning as stated by Marsick and Volpe (1999) exist in the security incident response process, it stands to reason that a learning model incorporating those characteristics might be useful for incident response. The model in figure 2 is an adaptation of Marsick and Watkins (2001).

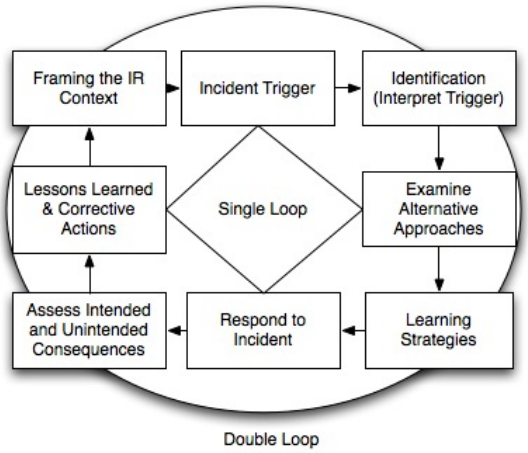


Figure 2: Informal and Incidental Learning Model (Adapted from Marsick and Watkins with Cseh)

The authors of the original model describe learning as 'unstructured' and a 'by-product of other activities, interpersonal interactions, experimentation or sensing the organisational culture' - a close fit to the description provided by focus group experts. This paper suggests the adapted model (figure 2) as an alternative to the traditional best-practice model (figure 1. The new model incorporates almost all of the steps in the traditional model (excluding 'preparation' which will be justified momentarily) into a learning model that has been further

enhanced with 'double loop learning'. The subsequent phases of this research project will test this model in the context of incident response through a series of further focus groups and case studies.

A significant difference between the traditional and the proposed model is the recognition that in practice learning is more of an 'ebb and flow' as individuals make sense of situations. Although figure 2 uses arrows to suggest a sense of sequential progression, the proposed model was originally designed with the belief that the steps are 'neither linear nor necessarily sequential'. Another difference is that the proposed model is an 'action learning' type model which represents the lifecycle of the post-event response to the incident trigger. Since 'preparation' takes place prior to the live response, it is out of the scope of the lifecycle represented in the figure. The outer circle in the proposed model represents double loop learning in the organisational context (which is in turn influenced by business, cultural, social and personal contexts) within which the incident response is taking place. The inner 'context' diamond represents the more simplistic single loop learning.

Single-loop learning is a simplistic, adaptive approach whereby employees simply detect and then correct deviations from policies, procedures or expected norms. An example could be a security incident involving an incorrectly configured firewall. A single loop response would be to correct the configuration without investigating why the situation happened in the first place. Double-loop learning involves questioning the very principles such as underlying policies and procedures, and is more generative in nature. When it comes to incident response, best practice guidelines encourage single-loop learning. In general, 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). Double-loop learning is akin to problem solving, involving continuous experimentation and feedback and is concerned with long-term change, rather than short-term goals.

Unlike the traditional model, which begins its post-event tasks with a focus on identifying the technical nature and type of incident, the proposed model makes two suggestions. Firstly, that the trigger is taking place in an organisational context (which is a dynamic environment). And secondly, that the incident interpretation applied by the incident response team is influenced by multiple factors – i.e. the events leading up to the incident, previous lessons that were learned (the 'Framing the IR Context' box) and their own prior experiences. Available strategies of action are influenced by past experiences but also include the possibility that personnel will explore new avenues through formal technical learning as well as informal discussion and consultation with peers. Marsick and Watkins point out that resources, knowledge, motivation and emotional capacity in a stressful situation play a role in assembling a range of choices and in the decision to select a course of action.

The 'respond to incident' step in figure 2 captures the containment, eradication and recovery phases in the traditional model. Once the response is completed, an assessment of the gap between intended and unintended outcomes can take place which leads to a 'lessons learned' or follow-up phase as in the traditional model.

## FUTURE WORK

As per its purpose, the focus group explored key issues within security incident learning and led to the generation of new paths of research and investigation. It is possible that case studies of CSIRTs in organisations could provide a deeper understanding of how informal learning practices can be leveraged effectively. Further work must be performed to profile how formal and informal learning should actually occur on the ground within a typical CSIRT post-incident. The specific, structured processes that are followed and the unstructured, organic activities and knowledge exchanges that also facilitate learning need to be explored in order to determine how informal learning can be effectively leveraged as per Muhren (2008). The model in figure 2 will be tested in the next phase of this project to determine if it can drive security learning in organizations.

## CONCLUSION

Incident response processes facilitate the identification, containment of and recovery from security incidents. A critical phase within this process is 'Follow Up' where CSIRTs learn from past experience to improve the security incident response process itself. However, current 'Follow Up' processes described in best-practice methodologies are highly structured and formalised in nature and do not consider tacit knowledge and informal learning that occurs during incident response. This is critical, given that incident response is often an informal affair, driven by unofficial workarounds, networks of knowledge and communication channels.

To address this shortcoming, we suggest that organisations need to recognise that response to incidents is frequently informal. Organisations must look to leverage their informal learning capability to realise the benefits of effective organisational learning – agility, flexibility, innovation and a greater resilience when dealing with unknown situations. Such a learning focus would also need to incorporate a balance between informal learning and formal learning structures, whereby one channel reinforces the other.

Unfortunately, many organizations do not have a learning culture. Therefore, to drive learning we presented a new incident response model where learning is informal, incidental and ongoing. Future research aims to test the effectiveness of this model towards improving the security incident response function in organizations.

## REFERENCES

Argyris, C. 1976. "Single-Loop and Double-Loop Models in Research on Decision-Making", Administrative Science Quarterly, (21:3), pp.363-375.

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

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

Davenport, T. H. and L. Prusak 1998. Working knowledge: how organizations manage what they know. Boston, Harvard Business School Press.

Dhillon, G. and J. Backhouse 2001. "Current directions in IS security research: towards socio-organizational perspectives". Information Systems Journal, (11:2), pp. 127-153.

Grance, T., Kent, K. and 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 Organization in Strategic Decision-Making". International Studies of Man and Organization. (9:4), pp.37-62.

Fiol, C.M. and Lyles, M.A. 1985. "Organizational Learning", The Academy of Management Review, (10:4), pp.803-813.

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

Huber, G.P. 1991. "Organizational Learning: The Contributing Processes and the Literatures', Organization Science, (2:1), pp.88-115.

Jaikumar, V. 2002. "Organizations should build an incident response team", ComputerWorld Canada, (9:16).

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

Kitzinger, J. 1995. "Qualitative research: Introducing focus groups". British Medical Journal, (311: 7000), pp. 299-302.

Levitt, B. and March, J.G. 1988. "Organizational Learning", Annual Review of Sociology, Vol.14, pp.319-340.

March, J.G. and Olsen, J.P. 1976. Ambiguity and Choice in Organizations. Universitetsforlaget, Bergen, Norway.

Marsick, V. J., and Volpe, M. "The Nature of and Need for Informal Learning." In V. J. Marsick and M. Volpe (eds.), Informal Learning on the Job, Advances in Developing Human Resources, No. 3. San Francisco: Berrett Koehler, 1999.

Marsick, V. J., and Watkins, K. 1990. Informal and Incidental Learning in the Workplace. London and New York: Routledge.

Mitropolous, S., Patsos, D. and Douligeris, C. 2006. "On Incident Handling and Response: A state-of-the-art approach", Computers and Security, (25:5), pp.351-370.

Muhren, W., van den Eede, G. and van de Walle, B. 2008. "Organizational Learning for the Incident Management Process: Lessons from High Reliability Organizations". Journal of Information Systems Security, (4:3), pp.3-23.

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

Nonaka, I. 1994. "A dynamic theory of organizational knowledge creation." Organization Science. (5:1), pp. 14-37.

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

Novak, C.J. 2007. "Investigative response: After the breach". Computers and Security, (26:2), pp.183-185.

Sasse, M. A. and 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. "Organization theory: an overview and an appraisal". Journal of the Academy of Management, (4:1), pp2-26.

Shrivastava, P. 1983. "A Typology of Organizational Learning Systems", Journal of Management Studies, (20:1), pp.7-28.

Simon, H.A. 1991. "Bounded Rationality and Organizational Learning", Organization Science, (2:1), pp.125-134.

Siponen, M. T. 2005. "Analysis of modern IS security development approaches: towards the next generation of social and adaptable ISS methods". Information and Organization, (15:4), pp.339-375.

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.

Wiik, J., Gonzales, J.J., and Kossakowski, K-P. 2005. "Limits to Effectiveness in Computer Security Incident Response Teams". in Proceedings of the Twenty-Third International Conference of the System Dynamics Society. The System Dynamics Society, Boston, MA.

van Niekerk, J. and von Solms, R. 2004. "Organisational Learning Models for Information Security", in Proceedings of the ISSA 2004 Enabling Tomorrow Conference, 30 June-2 July, Gallagher Estate, Midrand.

## COPYRIGHT