International Journal of Information Management 35 (2015) 717–723

Contents lists available at ScienceDirect

International Journal of Information Management

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

Case study

# A case analysis of information systems and security incident responses

Atif Ahmad*, Sean B Maynard, Graeme Shanks

*Department of Computing and Information Systems, The University of Melbourne, VIC 3010, Australia*

ARTICLE INFO

*Article history:*
Received 6 August 2015
Accepted 7 August 2015
Available online 21 August 2015

*Keywords:*
Information Security Management
Security learning
Incident Response Teams
Organizational learning

ABSTRACT

Our case analysis presents and identifies significant and systemic shortcomings of the incident response practices of an Australian financial organization. Organizational Incident Response Teams accumulate considerable experience in addressing information security failures and attacks. Their first-hand experiences provide organizations with a unique opportunity to draw security lessons and insights towards improving enterprise-wide security management processes. However, previous research shows a distinct lack of communication and collaboration between the functions of incident response and security management, suggesting organizations are not learning from their incident experiences. We subsequently propose a number of lessons learned and a novel security-learning model.

## 1. Introduction

Incident Response Teams (IRTs) respond to information systems security process failures or violations. IRTs diagnose incidents, contain them from spreading, eradicate their (technical) causes, and facilitate organizational recovery to normal business operations (Tøndel, Line, & Jaatun, 2014). Few studies address how the experiences of IRTs can be used to improve security processes. This is significant because IRTs accumulate considerable experience in addressing security failures and attacks first-hand. Incident investigations into security failures can expose inaccurate risk assessments, insufficient, misleading or contradictory advice in policies, ineffective or misaligned strategies, and inadequate security education, training and awareness (SETA) (Shedden, Ahmad, & Ruighaver, 2010).

Whilst best-practice incident response methodologies (Cichonski, Millar, Grance, & Scarfone, 2012) include a ‘feedback’ or ‘follow-up’ phase where lessons learned are discussed and documented in a formal report, these methodologies focus narrowly on the ‘response’ aspect of the process. They do not explicitly mention the need to leverage opportunities for wider learning such as improving security risk assessment and security policy development. Without a clear intent to draw broad security lessons to benefit the larger organization, there is little prospect of improving the security of information systems in general (e.g., see Desouza and Vanapalli (2005) on how insights from breaches can improve systems).

We describe a case that examines how an organization in the Australian financial sector, *OZFinance*, learns from security incident response. We chose the financial sector because of the increasingly sophisticated attacks on its information infrastructure (e.g., see Smith (2013) for news coverage of attacks on the Reserve Bank of Australia). We use the 4I Organizational Learning Framework (Crossan, Lane, & White, 1999; Zietsma, Winn, Branzei, & Vertinsky, 2002) to analyze the *OzFinance*’s learning processes as the 4I Framework focuses on (1) process improvement, (2) incorporates double-loop learning principles, and (3) provides a structured approach to learning across individual, group and organizational levels.

## 2. Incident response practice in organizations

An incident is a violation (or imminent threat of violation) of computer security policies, acceptable use policies, or standard security practices (Hansman & Hunt, 2005). Therefore, denial of service, unauthorized sharing of sensitive information, a malicious attack on a computing system or network and the inadvertent deletion of an important document all qualify as incidents. The literature broadly agrees that when dealing with an incident, IRTs generally engage in six sequential stages: preparation, identification, containment, eradication, recovery and follow-up (Cichonski et al., 2012; West-Brown, Stikvoort, Kossakowski, Killcrece, & Ruefle, 2003). The purpose of the follow-up phase is to reflect on the incident handling experience and identify ‘lessons learned’ that can be incorporated into standard operating procedures.

* Corresponding author. Fax: +61 3 9349 4596.
*E-mail addresses:* atif@unimelb.edu.au (A. Ahmad), sean.maynard@unimelb.edu.au (S.B. Maynard), gshanks@unimelb.edu.au (G. Shanks).

http://dx.doi.org/10.1016/j.ijinfomgt.2015.08.001
0268-4012/Crown Copyright © 2015 Published by Elsevier Ltd. All rights reserved.

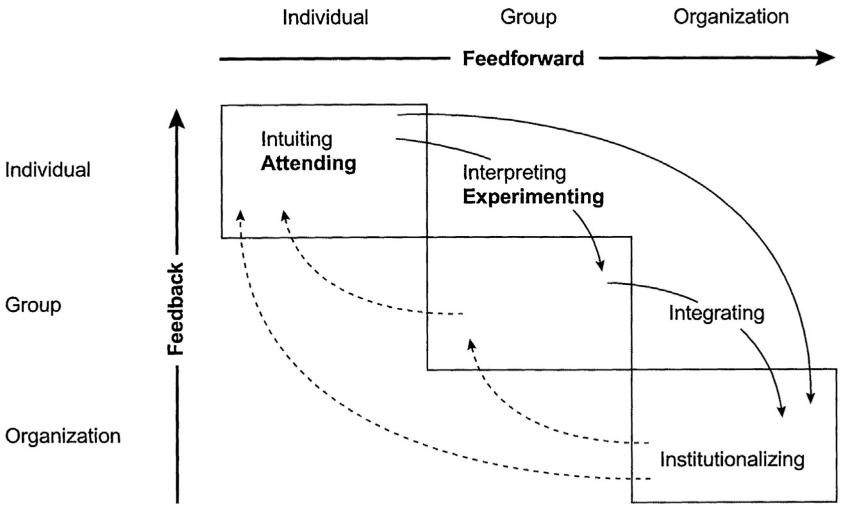

**Fig. 1.** The 4I model, Zietsma et al. (2002).

### 2.1. How lessons are learned from the incident response process

Professional incident response literature places great importance on post-incident learning (Killcrece, Kossakowski, Ruefle & Zajicek, 2003, & Organizational models for 2003). However, the focus tends to be on improving corrective actions towards lowering cost and improving efficiency (Tan, Ruighaver, & Ahmad, 2003). Learning typically takes place formally in meetings and management presentations and through the sharing and reviewing of reports (Cichonski et al., 2012).

Tøndel et al. (2014) identified a number of challenges that relate to learning practices including: (1) a lack of willingness to share incident-related information outside the organization (e.g., with industry) (Hove & Tårnes, 2013); (2) poor communication and collaboration between the IRT and teams from other organizational areas (Hove & Tårnes, 2013); (3) lack of motivation driving learning activities (Hove & Tårnes, 2013); and (4) inadequate sharing of lessons learnt internally within organizations (Shedden, Ruighaver, & Ahmad, 2010).

Therefore a key objective of this study is to explain how the three key stakeholders in organizations (i.e., the IRT, security management team and senior management team) should communicate, collaborate and share security lessons to improve security management processes.

## 3. Organizational learning

Organizational learning, as a research field, examines how organizations develop knowledge and 'routines' to guide their behaviors (Levitt & March, 1988). Learning in organizations takes place at the individual, team and organizational level (Chan, 2003; Rashman, Withers, & Hartley, 2009) Understanding the interplay and interaction between these learning levels is a major theme in organizational learning (Crossan et al., 1999).

To meet our research objectives we had three requirements for the learning framework. The framework must (1) adopt a multi-level approach explicitly linking incident responder to key stakeholders (e.g., security management team and senior management); (2) not be entirely cognitive, but rather link cognition to action so individual recognition of unusual patterns of security activity leads to change in security process, and (3) employ double-loop learning principles. Only the 4I (intuiting and attending, interpreting and experimenting, integrating, institutionalizing) framework of organizational learning (Crossan et al., 1999; Zietsma et al., 2002) met all three requirements (see Fig. 1).

The 4I framework explicitly targets learning at individual, team and organizational levels whilst incorporating double loop learning principles. The framework encourages organizations to manage the tension between *exploring* new ideas and *exploiting* what has already been learnt. This 'strategic renewal' challenges institutional norms - a particularly useful characteristic as we expect that lessons learned from security incidents will challenge compliance culture - a key obstacle to the development of effective security strategy (see Tan, Ruighaver, & Ahmad, 2010).

The *intuiting and attending* processes aim to develop individual capability to discern new patterns of activity without conscious effort. *Interpreting and experimenting* are social activities designed to allow individual insights to be shared and enacted with a group (i.e., discussions and trying out new ideas). *Integrating* allows group collective and coordinated action to ensue. Finally, important routines are formalized into structures, systems and procedures to retain individual and group learning through *institutionalization*.

## 4. *OzFinance*: a case study

The choice of organization for this case was based on three key criteria: (1) their IR practice has remained relatively stable for three to five years; (2) their IR practice to be complying with 'best practice' guidelines; and (3) they had to be willing to make the relevant stakeholders available, which is rare in studies that focus on security issues (Kotulic & Clark, 2004).

*OzFinance*'s incident response capability comes from two teams. The Network Incident Response Team (the '*Incident Response Team*') is a full-time, four-person team, which resides in the Information Security Department. Their primary responsibility is to secure *OzFinance*'s core network. The High-Impact Incident Response Coordination Team (the '*Coordination Team*') reports to the CIO and acts in a management or coordination capacity and is only activated in the case of incidents deemed to be 'high-impact'. The *Coordination Team* starts with a team of four but can quickly recruit large numbers of front-line personnel as the situation demands. The team will typically be called in for significant events such as mission-critical server crashes. They will be involved in writing the mandatory post-incident report for high-impact incidents. The *Incident Response Team* and the *Coordination Team* work independently of each other but may cooperate if the need arises. In this case the *Coordination Team* will take over the coordination role and liaise