Available online at www.sciencedirect.com

SciVerse ScienceDirect

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

Computers & Security

Incident response teams – Challenges in supporting the organisational security function

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

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

ARTICLE INFO

Article history:
Received 12 February 2012
Accepted 9 April 2012

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

ABSTRACT

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

© 2012 Elsevier Ltd. All rights reserved.

1. Introduction

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

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

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

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

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

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

2. Background and motivation

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

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

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

3. Incident response teams: handling security attacks

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

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

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

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

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

Download English Version:

https://daneshyari.com/en/article/456056

Download Persian Version:

https://daneshyari.com/article/456056

Daneshyari.com