COMPUTERS & SECURITY 45 (2014) 42–57

Available online at www.sciencedirect.com

ScienceDirect

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

Computers & Security

Information security incident management: Current practice as reported in the literature

Inger Anne Tøndel [a,*], *Maria B. Line* [b,a], *Martin Gilje Jaatun* [a]

[a] *SINTEF ICT, N-7465 Trondheim, Norway*

[b] *Dept. of Telematics, Norwegian University of Science and Technology, N-7491 Trondheim, Norway*

ARTICLE INFO

Article history:
Received 5 July 2013
Received in revised form
17 March 2014
Accepted 19 May 2014
Available online 28 May 2014

Keywords:
Information security
Incident management
Incident response
ISO/IEC 27035
Systematic review

ABSTRACT

This paper reports results of a systematic literature review on current practice and experiences with incident management, covering a wide variety of organisations. Identified practices are summarised according to the incident management phases of ISO/IEC 27035. The study shows that current practice and experience seem to be in line with the standard. We identify some inspirational examples that will be useful for organisations looking to improve their practices, and highlight which recommended practices generally are challenging to follow. We provide suggestions for addressing the challenges, and present identified research needs within information security incident management.

1. Introduction

Today, Information and Communication Technology (ICT) plays an important role in all organisations. ICT has brought a lot of benefits to our society. At the same time, it has made us vulnerable to failures and attacks that come via the ICT systems. As organisations have become more and more dependent on ICT, the threats towards these systems have become more prominent. The current situation can be summarised by the following quote by Ahmad et al. (2012):

> "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 loss of company reputation and customer confidence, legal issues, a loss of productivity and direct financial loss."

Although a lot of measures can be taken in order to prevent information security incidents from taking place, it is not economically feasible to fully protect all systems (Anderson et al., 2012). Thus organisations need to prepare for what to do in case of incidents in their ICT systems.

The main motivation of this paper is to provide a comprehensive overview of current practice and experiences documented in the literature on information security incident management. A further motivation is to identify the challenges organisations experience when trying to follow existing standards.

The remainder of the paper is structured as follows: In Section 2 we describe our research method. Section 3 provides an overview of the most recognised and well-known standards and guidelines related to information security incident management, and Section 4 presents findings from relevant studies and experience reports. We summarise current

* *Corresponding author*. Tel.: +47 97088476; fax: +47 73594302.
E-mail addresses: inger.a.tondel@sintef.no (I.A. Tøndel), maria.b.line@item.ntnu.no (M.B. Line), martin.g.jaatun@sintef.no (M.G. Jaatun).

http://dx.doi.org/10.1016/j.cose.2014.05.003
0167-4048/

practice, present inspirational examples, and discuss aspects that are particularly challenging, as well as future research needs, in Section 5. Section 6 offers concluding remarks.

2. Research method

The work presented in this paper has been organised as a systematic review and conducted based on recommendations by Kitchenham and Charters (2007). The goal with performing the systematic review was to identify current practice for information security incident management, and in particular experiences made. The research questions that guided the review were thus:

- Q1. How is information security incident management performed in practice?
- Q2. What experiences are reported in literature on information security incident management; what works well, what is difficult?

In the analysis work we also aimed at answering the following research question:

- Q3. To what degree does current practice resemble recommended standards and guidelines?

We limited our study to literature documenting real-life experiences and practices, either in form of experience reports or in form of empirical studies. Furthermore, we only included literature published after 2005.

Relevant literature was identified through a Scopus[2] search using search terms intended to identify all literature that covered incident management of information security incidents: ("incident management" OR "incident response" OR "incident reporting" OR "computer emergency response" OR "computer emergency management") AND ("information security" OR "cyber security" OR "ict" OR "computer security" OR "information technology").

The identified literature was then manually included or excluded in the study by one researcher. A first Scopus search was performed in March 2012, and then a second search was performed in August 2013 in order to identify any literature published since the first search. In addition, we manually went through the publicly available information from the Terena[3] and FIRST[4] conferences, whitepapers etc. from CERT/CC,[5] publications from SANS[6] and the latest IMF[7]-conference.[8] When going through the literature that was included in the study, we studied the references in order to identify additional literature. We added one study from a local university.[9]

One of the papers was analysed by two researchers. The other papers were analysed by one researcher. In the analysis the reported practices and experiences were identified and related to one of the incident management phases described in standards. We particularly identified the experiences and practices that were related to communication and collaboration during incident management, as this was a topic that was considered important in several of the identified papers and spanned all phases.

3. The incident management process

An information security event can be defined as an *"identified occurrence of a system, service or network state indicating a possible breach of information security, policy or failure of controls, or a previously unknown situation that may be security relevant"* (ISO, 2011). An information security incident is then a *"single or series of unwanted or unexpected information security events that have a significant probability of compromising business operations and threatening information security"* (ISO, 2011).

ISO/IEC 27035 "Information security incident management" (ISO, 2011) and NIST Special Publication 800-61 "Computer Security Incident Handling Guide" (Cichonski et al., 2008) stand out as two of the main standards and guidelines related to information security incident management. Both offer a structured approach to incident management, including planning and preparing for incident response, what to do when incidents strike, and how to extract lessons learnt afterwards. SANS (Kral, 2011) and ENISA (ENISA, 2010) have also provided guidelines for incident handling, which resemble the structure offered by ISO/IEC and NIST. The guide from SANS is quite short and contains just an overview of which activities belong to each phase. ENISA has excluded the preparations phase and just focused on the activities performed by a response team in case of an incident. ITIL (Brewster et al., 2012) describes the incident management process as consisting of six components; Incident detection and recording, Classification and initial support, Investigation and diagnosis, Resolution and recovery, Incident closure, and Ownership, monitoring, tracking, and communication during the progress of the incident handling. Activities related to planning and preparations are included in other parts of ITIL and hence not presented as part of the incident management process itself. FIRST provides a couple of guidelines on how to set up an incident response team within an organisation. These are specifically concerned with planning and preparations, and do not cover the complete incident management process. CERT/CC describes comprehensive guidelines for establishing and operating an incident response team in their CSIRT handbook (West-Brown et al., 2003). Furthermore, they describe their CERT/CC Incident Handling Life Cycle process.

[2] http://www.scopus.com.
[3] Trans-European Research and Education Networking Association, www.terena.org.
[4] Forum for Incident Response and Security Teams, www.first.org.
[5] www.cert.org.
[6] www.sans.org.
[7] IT Security Incident Management and IT Forensics.
[8] The proceedings from this conference were not available at Scopus at the time of the search, and was included because relevant material had been published at previous IMF conferences.
[9] This study was in form of a student thesis and would thus not be available in a Scopus search. Furthermore, we have performed a search for related student work from other universities, but without results (this may be because such student papers may be difficult to access outside the respective universities).