Available online at www.sciencedirect.com

ScienceDirect

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

Computers & Security

The future of information security incident management training: A case study of electrical power companies

Maria Bartnes [a,b,*], Nils Brede Moe [b], Poul E. Heegaard [a]

[a] Department of Telematics, Norwegian University of Science and Technology, N-7491 Trondheim, Norway
[b] SINTEF ICT, N-7465 Trondheim, Norway

ARTICLE INFO

Article history:
Received 23 February 2016
Received in revised form 5 May 2016
Accepted 16 May 2016
Available online 19 May 2016

Keywords:
Information security
Incident management
Incident response
Cross-functional teams
Learning to learn

ABSTRACT

Recent attacks and threat reports indicate that industrial control organizations are attractive targets for attacks. Emerging threats create the need for a well-established capacity for responding to unwanted incidents. Such a capacity is influenced by organizational, human, and technological factors. We have conducted extensive fieldwork for 2.5 years in Norwegian electric power companies with the aim of identifying challenges for improving information security incident management practices. Semi-structured interviews, document analysis, a survey and participant observations have been performed as part of this case study.

We describe how training for responding to information security incidents is given low priority and that different types of personnel, such as business managers and technical personnel, have different perspectives and priorities in regard to information security. Moreover, there is a gap in how IT staff and control system staff understand information security. Furthermore, *cross-functional teams* need to be created to ensure a holistic view during the incident response process.

To improve the capacity for responding to incidents, organizations need regular training sessions and systematic evaluations after such sessions. There is also the potential for improvement in evaluating minor incidents. A transition from an ad hoc approach to a systematic approach in training and learning requires a reorientation not only by the electric power companies but also by management. We found that *learning to learn* will enable the organizations to improve their incident response practices.

1. Motivation and objectives

Emerging information security threats create the need for a structured capacity for responding to unwanted incidents. Such a capacity is influenced by organizational, human, and technological factors. Benefits from a structured approach to information security incident management include an overall improvement in information security, reduced impact of incidents, improved focus and better prioritization of security activities, and better and more updated information security risk assessment efforts (ISO/IEC, 2011; Cusick and Ma, 2010).

Basic structures are needed, such as well-documented procedures and clear definitions of roles and responsibilities.

This work has mainly been funded by the Norwegian University of Science and Technology through the project *Smart Grids as a Critical Infrastructure*. Partial funding has been provided by the Norwegian Research Council under grant no. 217528 (DeVID).

* *Corresponding author.* Tel.: +47 45218102.
E-mail addresses: maria.bartnes@item.ntnu.no (M. Bartnes), nils.b.moe@sintef.no (N.B. Moe), poul.heegaard@item.ntnu.no (P.E. Heegaard).

http://dx.doi.org/10.1016/j.cose.2016.05.004
0167-4048/

However, during an incident there is a need for a more dynamic process that requires coordination and improvisation, where exceptions and violations are managed and experienced incident handlers are valued. Therefore, personnel who will be involved in responding to incidents that may compromise business operations require training.

Industrial control systems will undergo major technological changes in the near future (ERCIM, 2015). There is a lack of research and experiences related to incident response in such environments (NIST, 2010), hence there is a need for investigations in this area. A study of current practice and challenges is needed to identify potential improvements. This work was guided by the following research question:

What are the challenges for improving information security incident management practices?

We have conducted an empirical study of current practices for information security incident management in Norwegian electric power organizations. The level of cyber situation awareness was surveyed to analyze their level of preparedness for targeted attacks. Furthermore, we investigated which challenges were met during preparedness exercises for information security incidents.

This paper is structured as follows: Section 2 presents background and related work. Research methods and the industrial case context are introduced in Section 3. Section 4 describes our findings, while Section 5 discusses these findings in light of the research questions and proposes implications of the results for both practice and research. Finally, Section 6 provides the study's concluding remarks.

2. Background

The purpose of information security incident management training is to strengthen the capabilities of an organization in responding to incidents that may compromise business operations (ISO/IEC, 2011). Involved personnel need to be familiar with the overall information security incident management process. Training involves cooperation, coordination, and technical expertise. Human factors in incident management are described below as principles from the area of resilience engineering, and the relation between the incident management process and resilience engineering is discussed. Furthermore, specific attention is given to cyber situation awareness and preparedness exercises as means of enhancing the incident management process, as well as the importance of coordination in incident response teams, including the issues of making decisions and sharing knowledge. In the following, we will introduce the concepts of information security management and preparedness exercises, resilience engineering, cyber situation awareness, and coordination in incident response.

2.1. *Information security preparedness tabletop exercises*

Tabletop exercises are discussion-based exercises. They are usually performed in a classroom setting without the use of any specific equipment, and a facilitator presents a scenario and initiates the discussion (Grance et al., 2006). Tabletop exercises allow for discussions of roles, responsibilities, procedures, coordination, and decision-making and are a reasonably cost-efficient way of reviewing and learning documented plans and procedures for incident response (Grance et al., 2006). Functional exercises, alternately, involve practical simulations of incidents with the use of physical equipment and the execution of procedures, such as alerting and reporting. Both tabletop exercises and functional exercises prepare personnel for responding to an incident (Grance et al., 2006). Exercises provide a means for personnel to train for making the right decisions under pressure (Hollnagel, 2009). Wrong decisions may cause the incident to escalate and lead to severe consequences. According to National Institute of Standards and Technology (NIST) (Grance et al., 2006), both types of exercises should consist of the following four phases:

- *Phase I: Design* the event by identifying objectives and participants,
- *Phase II: Develop* the scenario and guides for the facilitator and the participants,
- *Phase III: Conduct* the exercise, and
- *Phase IV: Evaluate* by debriefing and identifying lessons learned.

Tabletop exercises and functional exercises supplement each other: tabletop exercises do not provide practical demonstrations of the effects of an incident or the emergency management's true response capabilities (FEMA, 2003), while this is exactly what is supported by functional exercises.

Creating realistic scenarios for training (Hove et al., 2014) and making sure that the right people perceive the exercise as relevant are challenging, and even though an exercise is based on a realistic scenario, there are no guarantees that a real incident will be successfully responded to (Rykkja, 2014).

2.2. *Information security incident management*

A number of standards and recommendations describe the information security incident management process: ISO/IEC (2011), NIST (Grance et al., 2008), ITIL (Brewster et al., 2012),[1] and ENISA (2010).[2] They provide a useful baseline for organizations about to implement their own scheme or looking for inspiration for improvements. ISO/IEC 27035 should be regarded as the most comprehensive and internationally recognized documentation of what is currently the recommended practice in this field, as it is consensus-based and developed by independent non-governmental and non-profit organizations (ISO[3] and IEC[4]). The standard is therefore used as a basis for the interview studies performed in our work. It describes the incident management process in five phases, as illustrated in Fig. 1:

[1] ITIL: Information Technology Infrastructure Library.
[2] ENISA: European Union Agency for Network and Information Security.
[3] ISO: The International Organization for Standardization.
[4] IEC: International Engineering Consortium.