Published in "Innovations for Community Services", Vol 648 of the series Communications in Computer and Information Science pp 129-139, 13 Nov. 2016
http://link.springer.com/chapter/10.1007/978-3-319-49466-1_9

Zebras and Lions:
Better Incident Handling Through Improved Cooperation

Martin Gilje Jaatun[1], Maria Bartnes[2], Inger Anne Tøndel[1]

[1] Department of Software Engineering, Safety and Security,
SINTEF ICT, Trondheim, Norway

[2] SINTEF Group Head Office,
Trondheim, Norway

Abstract. The ability to appropriately prepare for, and respond to, information security incidents, is of paramount importance, as it is impossible to prevent all possible incidents from occurring. Current trends show that the power and automation industry is an attractive target for hackers. A main challenge for this industry to overcome is the differences regarding culture and traditions, knowledge and communication, between Information and Communication Technology (ICT) staff and industrial control system staff. Communication is necessary for knowledge transfer, which in turn is necessary to learn from previous incidents in order to improve the incident handling process. This article reports on interviews with representatives from large electricity distribution service operators, and highlights challenges and opportunities for computer security incident handling in the industrial control system space.

Keywords: Information security, Incident response

1 Introduction

In the power and automation industry, there has long been a trend towards more use of Information and Communication Technology (ICT), including Commercial-Off-The-Shelf (COTS) components. At the same time, the threats towards information and the ICT systems that are used to process information are steadily increasing, with Advanced Persistent Threats (APTs) receiving growing attention in the information security community. Organizations face attackers with skills to perform advanced attacks towards their ICT infrastructure, with resources to perform long-term attacks, and with goals of achieving long-term access to the target. In such an environment, organizations must expect that, eventually, their systems will be compromised.

Far from being science fiction, ICT security incidents targeting industrial control systems are already happening. During the last ten years, there have been several examples of power outages or other types of damage to automation and control systems caused by hackers, malicious insiders or software failures. The most famous attack up till now is Stuxnet[1], which appeared during the summer of 2010 as an advanced piece of malware created to cause physical harm to advanced equipment connected to industrial control systems. However, more recent malware such as Dragonfly, Duqu, Flame and the Night Dragon attack, demonstrate that threats related to reconnaissance and espionage also are relevant for industrial control systems. The underlying threats of these recent attacks are well known to ICT security experts. Such attacks have been around for a long time, and several technical and organizational security measures exist that contribute to reducing the risks. However, there should always be a balance between the accepted level of risk and the amount of investment in security measures. It is impossible to prevent all types of incidents, and thus the ability to appropriately prepare for, and respond to, information security incidents is therefore essential for companies in critical industries that need to ensure and maintain continuous operation of their systems.

This article reports on specific aspects of a larger study on information security incident response management in power distribution service operators (DSOs) [1-3]. Based on a number of semi-structured interviews, we venture to shed light on how communication and cooperation influence how information security incidents are being handled and responded to. We look at responses in terms of both technical measures and human actions, and we pay particular attention to how the follow-up activities are performed; information sharing, lessons learnt, and how experiences in the process control domain are transferred into the overall information security work in the organization. This is studied with respect to both ICT systems and the power automation systems in order to identify possible synergy effects from improved cooperation and communication.

The informants represent three different roles in a set of large DSOs; Chief Information Officer (CIO), Chief Information Security Officer (CISO), and Head of control room/power automation systems. The choice of informants was made based on the intention of identifying current cooperation patterns and possible synergy effects from future cooperation, and viewing the overall management system in general.

2 Background

Incident management is the process of detecting and responding to incidents, including supplementary work such as learning from the incidents, using lessons learnt as input in overall risk assessments, and identifying improvements to the implemented incident management scheme. ISO/IEC 27035 Information security incident management [4] describes the complete incident management process. The process comprises five phases; 1) Plan and prepare, 2) Detection and reporting, 3) Assessment and decision, 4) Responses, and 5) Lessons learnt (see Figure 1, where the phases have been abbreviated as Plan – Detect – Assess – Respond – Learn). The guideline is quite extensive and would be costly to adopt to the letter, but it is a collection of practical advice, key activities and examples, and is useful for

[1] see http://www.symantec.com/connect/blogs/w32stuxnet-dossier

companies establishing their own security incident organization. The ISO/IEC standard addresses corporate systems in general, and does not contain any considerations specifically related to industrial systems. In addition to the ISO/IEC standard, several other guidelines and best practice documents are available.

As indicated by the circular arrow around the Plan phase in Figure 1, this is where the average organization will spend most of its time, waiting and (hopefully) preparing for the next incident. It is in the planning phase that the groundwork for successful incident management is laid, including establishment of communication channels and an information sharing culture, both between the different disciplines within an organization, and between organizations. Although not the focus of this article, it is also here that other general improvements of the information security controls and mechanisms are performed, guided by evolving best practices and industry standards.

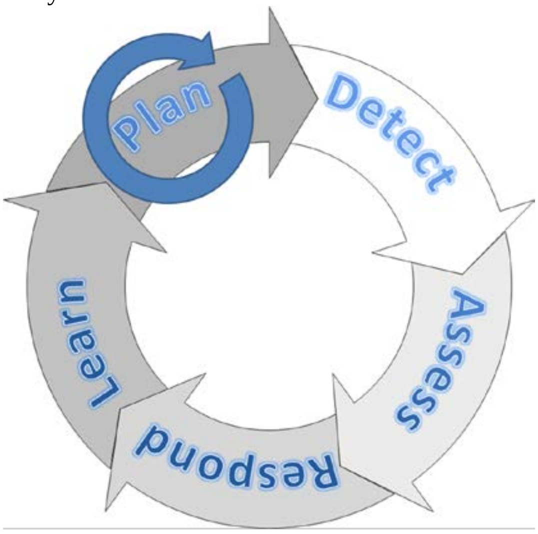

Figure 1: The Incident Handling Cycle

Whereas standards and recommendations exist in the area of incident management, also with respect to critical infrastructures, limited research is available related to managing incidents in an operating environment where automation systems and ICT systems are closely integrated [5]. An efficient incident management process is just as important as technical information security measures when continuous operation is a governing requirement.

3 Stumbling blocks for process control incident response

There are usually many obstacles to overcome in order to implement a successful scheme for incident management in an organization. However, the power industry, as well as other process industries, faces one in particular that is not shared by all other industries: the integration of ICT systems and power automation systems; which implies that ICT staff and power automation staff or process control engineers need to cooperate extensively during both daily operations and crisis situations. These two groups differ in several ways, to the extent that some industry observers have referred to them as "zebras and lions". They usually have different backgrounds; information technology or computer science on one side, electrical or process engineering on the other side. They are used to operate different systems with quite different requirements; as an example, confidentiality is quite commonly the most important security concern in ICT systems, while availability is first priority for automation systems. Wei et al. [6] exemplify this further by pointing out four main differences between these types of systems, regarding security objectives, security architecture, technology base and quality-of-service requirements.

Power automation staff are used to their proprietary systems not being connected to any external network[2], and hence not used to think about the outside world as a possible threat towards their systems. They do not even necessarily recognize their systems as actually being ICT. ICT staff are used to computers failing from time to time, needing a re-boot before they work all right again. Downtime is unfortunate, but sometimes necessary, and does not always have large financial consequences, especially not if it is planned. Testing and installing patches is thus business as usual in most ICT systems. In power automation, however, testing and installing patches is extremely difficult, as this most probably leads to some downtime. Downtime can be extremely costly in many industrial control environments, and engineers go to great lengths to avoid it. *If it works, don't touch it* is thus a tacit rule of thumb, which results in large parts of such industrial control systems being outdated and unpatched, and hence vulnerable to a great number of known attacks.

Another difference between ICT personnel and process control engineers is that the former tend to be concerned with *security* (e.g., preventing unauthorized access to information), while the latter are more concerned with *safety* (e.g., preventing a generator from overheating and exploding). Interestingly, *availability* may be an element of both safety and security, but is likely to be interpreted differently by the two camps. The fields of safety and security have different terminologies. As an example, a safety breach may be denoted as a *fault* or an *accident*. Security breaches, on the other hand, may exploit what are denoted as *bugs* or *flaws*[3]. A *safety hazard* may loosely correspond to a *security threat*, but there are substantial differences when it comes to methods and methodologies between the two fields of safety and security.

Recognizing an information security incident is difficult if one is not trained for it. Experiences from the oil and gas industry show that a computer may be unstable for days and weeks without anyone recognizing it as a possible virus infection [7]. Ensuring that the organization detects and handles such an incident is a cultural challenge just as much as a technical one.

Facilitating and achieving understanding and well-functioning collaboration in this intersection between ICT staff and power automation staff will be the most important task on the way to successful information security incident management for process control environments.

[2] Although this is generally no longer the case.

[3] A bug is a programming error, while a flaw is a more high-level architecture or design error.

4 Collaboration and communication in incident management

From the literature, we are aware of three main interview studies with the aim of identifying practices regarding incident response. Werlinger et al. [8] studied the practices related to diagnostic works during incident response in a variety of organizations. Ahmad et al. [9] studied incident management in a large financial institution, and Jaatun et al. [7] studied incident response in the petroleum industry. In the following, we summarize the main findings from these studies when it comes to collaboration and communication related to incident management.

Planning of incident management can include a large number of diverse of activities, including getting management commitment, establishing policies, plans and procedures, putting together an incident response team, establishing technical and other support, and performing awareness briefings and training. Studies in the petroleum industry [7] revealed that the organizations usually had several plans covering different aspects of the incident management process, and that there was a need for a short and common plan. It was also found that suppliers were not adequately involved in planning for incidents, although the operator would in many cases depend on them during incident management. Individual information security awareness was also not at a satisfactory level. Scenario training that could have improved this was not performed for ICT incidents as it was done for HSE incidents. Finally, and maybe most disturbing, the study revealed a "deep sense of mistrust" between process control engineers and ICT network administrators.

The identified issues can be interpreted as symptoms of unsatisfactory collaboration and communication when it comes to information security, and incident management in particular. This is disturbing since incident management is collaborative in nature. This is exemplified by Werlinger et al. [8], who found that:

- configuration of monitoring tools for incident response require extensive knowledge of issues that are rarely explicitly documented and obtaining this knowledge may involve also external stakeholders
- the complexity of the IT systems, and also the lack of resources for monitoring, means that incident detection relies on notifications from various stakeholders – including end-users
- verification that there actually is an incident – not a false alarm – may require collaboration with external organizations
- managers often need to be involved in decision making.

The importance of collaboration and communication is also reflected in the procedures for responding to high-impact incidents at the financial organization studied by Ahmad et al. [9]. Technical and business conference calls are set up in order to gather knowledge and communicate progress; in general, the management of the incident relies heavily on communication via teleconferencing, phone, e-mail and the helpdesk system. It is not without reason that Werlinger et al. [8] list 'communication' as one of the five key skills required for diagnosis work.

The challenges related to collaboration and communication are often revealed when studying the learning process that take place after an incident. In the financial institution studied by Ahmad et al. [9] incidents were handled differently depending on their impact ranking. This also influenced the learning process afterwards. For high-impact incidents, the post incident learning process was formalized, and involved at least three meetings. The first two meetings however only included the members of the incident response team. Thus, members from the risk area and the business in general were involved only to a limited extent. For low-impact incidents, the only formal practice was to write a log entry in the incident tracking system. The team involved however still attempted to learn and identify how they could improve based on the experiences from the incident.

The study of the petroleum industry [7] revealed that information security was viewed merely as a technical issue. This technical focus was also found in the study of the financial organization [9]. Especially for low-impact incidents, the emphasis was on technical information, over policy and risk. For high-impact incidents, there was an understanding that it was important to identify root causes that goes beyond the technical issues (e.g. underlying gaps in the processes). However, the learning process also for high-impact incidents involved only technical personnel in the first phases. Reporting from incidents was also technical. Based on the low-impact incidents, several reports were produced for management. This was typically statistical information with a focus on the technical aspects. From the high-impact incidents, the reports were more detailed and a bit broader in scope, but dissemination also to non-technical personnel was not performed satisfactorily. There was a lack of formal policy on how information should be disseminated. In addition, the silo structure of the organization was a hindrance for effective sharing of experiences. The practice can probably be summarized by a finding by Werlinger et al. [8] where the representative from one of the organizations studied explained that security incidents were discussed weekly so that **security practitioners** could learn about new threats and assist in solving challenging incidents.

Despite the obvious weaknesses in the learning process used at the financial organization studied [9], the organization found that the introduction of the formalized learning process for high-impact incidents had resulted in an enormous reduction in the number of high-impact incidents. The importance of learning was also stressed in the study of the petroleum industry [7]. Learning was however considered to be difficult, and the representatives from the industry knew that they did not perform learning at a satisfactory manner. One of the problems highlighted was that they had several reporting systems, of which none was tailored to information security. In addition, the study revealed a lack of openness about incidents. Suppliers were not adequately involved in learning from incidents – although they could play a crucial role. There was also a lack of willingness to share information about incidents to the industry as a whole.

5 Incident management at large DSOs - results from interview study

We have performed a large study of information security incident management at several large DSOs [1, 2, 10]. The current introduction of Advanced Metering Infrastructure (AMI) results in – from the point of DSOs – more ICT, and more distributed ICT, and more pathways into their core systems. This has implications for their work on information security, including incident management. In order to know more about the level of maturity in this industry when it comes to management of information security incidents, and also the main challenges faced in this respect, we are performing interviews with key personnel at large DSOs; both personnel from the ICT side and the power automation side. We will in the following highlight the input from the informants that relate to cooperation and communication aspects of incident handling. The results concern practices and experiences in the incident management phases Lessons learnt, Plan and prepare, and Detection and reporting.

5.1 Lessons learnt

There are large differences between the DSOs when it comes to the post-incident activities. Some report on having routines for regular meetings, or at least evaluation meetings after certain incidents, in order to go through what happened, how they responded, which changes need to be implemented in the near future, and for mutual information exchange. Others do not perform regular reporting or evaluations, neither in the team, nor with the top management. In general, the DSOs do not perform learning activities in connection with incidents with low impact.

Self-experienced incidents form an excellent foundation for internal raising of awareness. Some DSOs seem to do this, whereas others have a rather unstructured approach to these sorts of activities. The respondents state that there are few information security incidents directly related to their industrial control systems, which may influence the experienced level of urgency when it comes to learning activities related to incidents.

The use of indicators or metrics related to information security does not seem to be established. For some specific incidents the interviewees are able to estimate a cost for the work of fixing the problems and reestablishing regular operations. Again, the low frequency of events may contribute to a sentiment that "there is nothing to measure".

5.2 Plan and prepare

The DSOs do not seem to have established their own Computer Security Incident Response Team (CSIRT) within the organization. They are however required to have an emergency preparedness organization for incidents described in the national regulations for preparedness and contingency. Such incidents are typically those that may have consequences for the power generation and distribution. Some information security incidents can be considered a subset of these.

Plans for incident management are not established in all DSOs. Some are currently working on this, others have not identified the need for such plans. Testing preparedness plans and training on information security incident management routines does not seem to be common practice. This may come as a natural consequence of the lack of plans. Also, this type of exercise does not get high priority compared to other pressing tasks that are needed to ensure daily operations. Some DSOs report that they perform frequent training on emergency preparedness in general, where information security incidents may be part of the problem.

The DSOs confirm that there is insufficient cooperation between ICT and ICS staff, but there are notable exceptions where different respondents from the same company offer dissenting views on this issue. This needs to be studied further, but one possible explanation may be that there are differing views on what constitutes "good cooperation". In general, they agree that the evolving Smart Grid landscape with introduce new challenges that will require improved cooperation in the future.

5.3 Detection and reporting

The respondents all have technical detection systems like IDS/IPS, antivirus, firewalls and similar in place for their administrative ICT systems. For the power automation systems this is a bit more unclear. This lack of clarity may be due to our respondents lacking detailed knowledge; it does not necessarily mean that such detection mechanisms are not in place. However, failures, or irregular events, in these systems are just as often detected by the personnel operating them. Also, incidents to the administrative ICT systems are sometimes detected by employees. All respondents report of a culture where reporting is accepted and appreciated, such that the employees are not reluctant to report in the fear of being suspected for doing something wrong.

6 Discussion

Our study of incident management practices and experiences among DSOs reveals much of the same challenges as have been pointed out in other studies. Lack of plans and lack of training was also pointed out as challenges in the petroleum industry [7]. Limited learning activities was also a problem in that industry, and in the study of the financial organization [9]. The reliance on users when it comes to detection of incidents was also reported in the studies by Werlinger et al. [8]. The level of preparedness and the amount of learning activities performed however varies a lot from DSO to DSO. We have seen examples of organizations who are diligent in their application of good incident response practices, but there are also other organizations that are less aware of (or concerned with) incident response in particular, or information security in general.

Our interviews confirm that information security activities often are not considered part of "core business" for the DSOs, but rather more or less implicitly subsumed under the broader category of "ensuring electricity delivery". This also implies that communication between ICT personnel and process control still leaves something to be desired. A naïve cause-and-effect analysis might seem to indicate that the current incident management processes work as intended, and that there thus is no need for improved communication and coordination in this sector. However, we think it is just as likely that the low number of incidents simply means that the would-be attackers at the moment are just having too much fun elsewhere. Just as the malware industry has moved from more or less malicious pranks fueled by idle curiosity to for-profit botnets and extortion, we believe that we have so far seen only the tip of the iceberg when it comes to computer security incidents in the process control industry.

Learning from others' mistakes is generally accepted as being less expensive than learning from your own, and thus there has long been a culture for full-disclosure information sharing[4] among accredited information security incident handling professionals in (particularly academic) Internet Service Providers. The lack of a coordinating Computer Security Incident Response Team in many process control industry segments is also an obstacle to improved information sharing. In Norway, there has been talk of an "Oil CERT" and an "Energy CERT" for years, but the latter was only formally established at the end of 2014[5], and it is still not entirely clear how it will interact with other players. There are commercial alternatives that purportedly document security incidents in the process control industry, such as the RISI database[6], but since these require a quite costly membership to access, it is difficult for independent research groups to assess their content and usefulness.

Despite the interviews giving a clear impression of a practice that seems to work satisfactory, we are hesitant to conclude that the "fire-fighting approach" is something that would work in general. If there are few occurring incidents with high impact, they are likely handled by a single person or a small group, which could imply that tacit knowledge covers who to contact and who does what. It could be argued that introducing a more rigid process with more documentation, reporting, and just "paper work" is not an efficient use of resources if current practice covers the need, but this ignores the perils of relying on the tacit knowledge of a few key individuals. Increasing incident frequency or unplanned absences can require sudden adding of emergency manpower, which will not work well if there is no documentation.

7 Conclusion

The interviews reveal a lack of systematic approaches to information security incident management. They also show that there is not a close cooperation between ICT staff and power automation staff, but rather quite clear definitions of responsibilities, although some respondents from the same DSO have given quite opposite opinions on this matter.

Even though the interviews portray a current practice that seems to work in a satisfactory manner, we advise against relying on this for the future, also because most of the respondents see future challenges for information security incident management in smart grid (and, by extension, industrial control system) environments. They confirm our initial concerns regarding the need for much closer cooperation between ICT staff and power automation staff, and the challenges related to this cooperation.

[4] http://www.first.org/

[5] https://www.kraftcert.no/

[6] http://www.securityincidents.org/

8 Further work

In general, there is a need for additional empirical research in the area of incident response management [5, 11]. Although we get the impression that the informants describe current practice, not only an ideal picture, we would like to do some further investigations on this matter. One way to approach this would be to run a retrospective group interview after a DSO has experienced an ICT security incident, i.e., a meeting with the persons and/or parties involved in solving the incident, where the complete course of events would be analyzed in order to understand how the organization responded to that specific incident. Interesting aspects for further exploration include how the incident was detected, reported and resolved, in which ways they followed their plans, and if not, how and why the plans were abandoned, and so on. This could be done as part of the organization's own evaluation process, if such exists.

There are usually quite a few differences between theory and practice. Observations are therefore also important. While the interviews give much insight in how incident management is planned and performed, observing the work in practice will give invaluable additional knowledge. Having knowledge of both theory and practice will make it possible to compare theory and practice, suggest realistic improvements, and hence actually make a contribution to the industry. Ideally, researchers should be present during a certain period of time in locations where incidents are detected and responded to. Observing meetings and other interactions, and having informal talks with the involved personnel by the coffee machine can also be important sources of information. The intersection between ICT and power automation competence, culture, language, incidents, and tools will be especially interesting to observe.

Regular emergency preparedness exercises have long been required in many critical infrastructure sectors, but these have until recently not considered cyber security a necessary component. There is a need to perform more empirical research on how preparedness exercises can incorporate cyber security, and to evaluate how this contributes to better cyber security for an organization [11].

Acknowledgments. The authors would like to thank the distribution system operators who have contributed with informants for our interviews. This research has been supported by the Norwegian Research Council through the projects DeVID and Flexnett.

References

1. Line, M.B.: A Case Study: Preparing for the Smart Grids - Identifying Current Practice for Information Security Incident Management in the Power Industry. IT Security Incident Management and IT Forensics (IMF), 2013 Seventh International Conference on, pp. 26-32 (2013)

2. Line, M.B., Tøndel, I.A., Jaatun, M.G.: Information Security Incident Management: Planning for Failure. Proceedings of the 2014 Eighth International Conference on IT Security Incident Management & IT Forensics, pp. 47-61. IEEE Computer Society (2014)
3. Line, M.B., Tøndel, I.A., Jaatun, M.G.: Current practices and challenges in industrial control organizations regarding information security incident management - Does size matter? Information security incident management in large and small industrial control organizations. Int. J. Crit. Infrastruct. Prot. 12, 12-26 (2016)
4. ISO/IEC 27035:2011 Information technology - Security techniques - Information security incident management. ISO/IEC (2011)
5. Tøndel, I.A., Line, M.B., Jaatun, M.G.: Information security incident management: Current practice as reported in the literature. Comput. Secur. 45, 42-57 (2014)
6. Wei, D., Lu, Y., Jafari, M., Skare, P.M., Rohde, K.: Protecting Smart Grid Automation Systems Against Cyberattacks. IEEE Transactions on Smart Grid 2, 782-795 (2011)
7. Jaatun, M.G., Albrechtsen, E., Line, M.B., Tøndel, I.A., Longva, O.H.: A framework for incident response management in the petroleum industry. International Journal of Critical Infrastructure Protection 2, 26-37 (2009)
8. Werlinger, R., Muldner, K., Hawkey, K., Beznosov, K.: Preparation, detection, and analysis: the diagnostic work of IT security incident response. Information Management & Computer Security 18, 26 - 42 (2010)
9. Ahmad, A., Hadgkiss, J., Ruighaver, A.B.: Incident response teams – Challenges in supporting the organisational security function. Computers & Security 31, 643-652 (2012)
10. Line, M.B.: Understanding information security incident management practices: A case study in the electric power industry. PhD Thesis, NTNU (2015)
11. Bartnes, M., Moe, N.B., Heegaard, P.E.: The future of information security incident management training: A case study of electrical power companies. Computers & Security (2016)