Developing a Cyber Incident Communication Management Exercise for CI Stakeholders

Tomomi Aoyama(✉), Kenji Watanabe, Ichiro Koshijima, and Yoshihiro Hashimoto

Department of Architecture, Civil Engineering and Industrial Management Engineering, Nagoya Institute of Technology, Showaku, Gokiso, Nagoya, Aichi 4668555, Japan
{aoyama.tomomi,watanabe.kenji,koshijima.ichiro, hashimoto.yoshihiro}@nitech.ac.jp
http://shakai.web.nitech.ac.jp

Abstract. Existing cyber security training programs for Critical Infrastructures (CI) place much emphasis on technical aspects, often related to a specific sector/expertise, overlooking the importance of communication (i.e. the ability of a stakeholder to gather and provide relevant information). We hypothesise that the achievement of a secure and resilient society requires a shared protocol among CI stakeholders, that would facilitate communication and cooperation. In order to validate our hypothesis and explore effective communication structures while facing a cyber incident and during recovery, we developed a discussion-based exercise using an Industrial Control System (ICS) incident scenario, and implemented it in pilot workshops where a total of 91 experts participated. Results suggest there are three possible incident communication structures centered around the IT department, the production department, and management, respectively. In future, these structures can be used as the framework to build an ICS-Security Incident Response Team (ICS-SIRT), which would strengthen cooperation among CI stakeholders.

Keywords: CIP exercise · Cyber incident management · ICS security Communication management · Business continuity management

1 Introduction

1.1 Background

Cyber security training is a common measure to enhance the security capability of an organization. Numerous security *awareness training* programs are available for every type of expertise. Most of these training programs aim at educating basic knowledge about cyber protection and teaching how vulnerable a participant or an organization can be to cyber threats. Awareness training is important as a foundation of organizations' security capability, but it may not be enough. This is because they often focus only on the prevention of an incident,

G. Havarneanu et al. (Eds.): CRITIS 2016, LNCS 10242, pp. 13–24, 2017.
https://doi.org/10.1007/978-3-319-71368-7_2

and leave out cyber incident response. Therefore, the need for cyber security training *beyond awareness* is growing in the industry, and several key centres are providing training for cyber incident response. Training programs, such as the well-known *beyond awareness* adversarial Red team - Blue team Exercise, include classroom lectures and exercises to maximize the learning of technical skills with respect to cyber crisis management.

However, awareness and beyond awareness training programs focus on technical aspects and overlook the importance of soft skills in the management of a cyber incident. Indeed, in their annual cyber security awareness report, the SANS Institute claims that security personnel lacks soft skills [1], and that communication skills are among the most critical ones. In this context, communication skills are regarded as the ability to describe a critical situation effectively, to collect information relevant to an incident from other stakeholders, and to fit in an adaptive communication structure within the dynamics of a cyber attack. Based on on-site observation of the Red-Blue teams exercise, we found that many skillful engineers struggled to negotiate with others in an unorganized communication structure, or paid no attention to cooperation. This corroborates the hypothesis that lack of communication skills is a major issue in cyber incident management, and that the achievement of a secure and resilient society requires a shared protocol among CI stakeholders.

This paper especially focuses on cyber security training programs meant for those CI sectors that make use of ICS. However, given the generality of the proposed exercise, we believe the whole CI protection (CIP) community may benefit from it.

The next paragraph reviews the merits and demerits of the Red-Blue teams exercise. In the following section, a discussion-based exercise that aims at both enhancing communication skills and promoting cooperation among CI stakeholders is proposed, and its implementation is described in detail. The last section reviews the results of the implemented pilot exercises, and discuss their impact on the CIP community.

1.2 Case Study: Red Team - Blue Team Exercise

One of the leading cyber security incident response training in the field of ICS security is the ICS-CERT's 5 days training which includes a Red-team/Blue-team exercise. In this exercise, participants play the role of either the attacking (Red) or the defending (Blue) teams [2]. Similar adversarial exercises are provided by other key centres in the world, such as Queensland Institute of Technology in Australia [3,4], and European Network for Cyber Security (ENCS) in the Netherlands. The entire exercise is set up in a secure environment [5] for participants to experience how an organization can be compromised by a cyber attack. It should be noted that the exercise focuses on the impact of a cyber attack on a single organization, rather than on the whole CI stakeholder community. However, we believe that it represents one of the most recognized exercises in the field of ICS security. Therefore, we devote this subsection to the description of its characteristics.

Branlat et al. [6,7] studied the exercise operated by ICS-CERT, and pointed out that the realistic timeline of the exercise allows participants to simulate the complexity of incident handling. Encouraged by their work, we have been studying the dynamic adaptation of organizations' decision-making structures, by monitoring the training of ENCS [8,9]. Our on-site observation confirmed that the environment of the exercise provides valuable lessons regarding cyber incident management. Indeed, the reproducibility and the realistic timeline of the exercise allow participants to have an authentic experience. Moreover, it is a rare opportunity to establish technical skill-sets required in cyber defense, and to see how certain skills can impact the target system within the dynamics of a cyber attack. Arguably, one of the most noticeable strengths of the exercise is the heterogeneous background and expertise of the participants and facilitators. In fact, team-working among these professionals provides a new perspective to their mental model and enhances the impact of the training.

However, considering the technicality and the intensive nature of the exercise—even though it portrays the realistic speed of a cyber attack—, participants focus on their immediate task leaving little time for communication with each other, let alone for sharing ideas towards better incident management. As a result, the exercise does not explicitly provide a structured framework to learn about the importance of communication and cooperation among the different departments of an organization or across organization boundaries. Participants are not guided in understanding how an effective communication of their technical knowledge could influence the decision-making. Moreover, they are not taught to see the bigger picture, making it difficult for them to comprehend how dynamically the organization's communication structure should adapt to the timeline of a cyber attack.

2 Communication Management Exercise for ICS Security (CME-ICS)

Based on the realisation that soft skills are as important as hard skills in cyber incident management, we developed a discussion based ICS security exercise for improving communication management and creating a shared protocol in the community of CI stakeholders.

2.1 Peculiarity of Existing Japanese CIP Training

In Japan, there have been discussions about whether the Red-Blue teams exercise is necessary, and so far this format has not been adopted for domestic CI stakeholders. Conversely, there are several ICS security training programs that consist of class-room lectures and drills, which do not include active discussion among participants.

More importantly, participation to these training programs is restricted to certain expertise profiles or CI sectors (e.g. banking, chemical). However, large-scale cyber incident can cause an impact beyond boundaries of CI sectors in a

highly inter-connected society. In case of such an event, the cooperation of CI sectors and other stakeholders (e.g. government agencies) is essential [10]. Nevertheless, the current training system is isolated by sectors, and does not include stakeholders outside the organization. The results of such limited diversification of expertise are that the participants' perspective on cyber security issues is narrowed down, and that knowledge transfer across sectors is not facilitated.

2.2 Discussion-Based Exercise

Considering the sectorized nature of the existing Japanese CIP training programs, our aim is to develop an exercise that is open for any CI stakeholder, and that enables knowledge transfer among participants. This motivated the adoption of a *discussion-based* table-top exercise style, since it stimulates the discussion among participants with a large variety of backgrounds, allowing them to compare their views on an issue [11]. In addition, it is often used to develop new plans and procedures, focusing on strategic issues [12]. For all these reasons, it provides new perspectives to each participant's conceptual knowledge structure, and helps to build a shared mental model among them.

2.3 Theme of the Exercise: Communication Management

As previously mentioned, the lack of communication skills is a major issue in cyber incident management. Therefore, the exercise has the major objective of highlighting the importance of communication and cooperation among CI stakeholders. Specifically, the scenario represents a cyber incident within a simplified organization structure, where participants discuss and strategize countermeasures with a bird's-eye-view, that is without playing a specific role. This helps them understand the importance of effective communication among stakeholders, rather than focus excessively on technical aspects.

2.4 Scenario

The scenario of the exercise is based on our CI testbed (Fig. 1), that was originally built for the purpose of gaining public security awareness, as well as testing and developing security solutions for ICS [13]. The testbed consists of two plant systems, a controlling network for each plant, and a corporate network connecting the two control networks. Each plant is a closed hot water circulation system consisting of two tanks: water in the lower tank is heated by a heater, then circulated to the upper tank by a pump. With respect to the exercise, the testbed models a community heating/cooling facility of a fictitious company that provides services to two different areas [14]. Safety violations, such as spilling water or heating an empty tank, could not only damage the equipment and harm the personnel, but may cause the discontinuation of the plant.

The phases of the scenario follow the time line of incident handling proposed by Sheffi et al. [15]. They suggested that any significant disruption has a typical

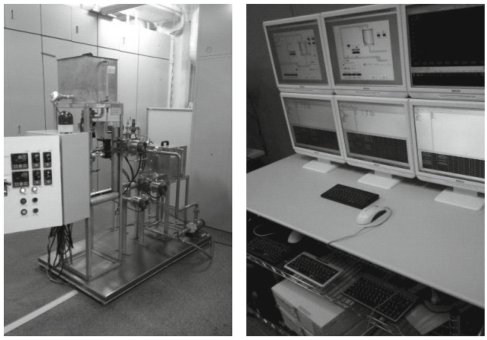

Fig. 1. The plant side (left) and the operator side (right) of the testbed. Testbed visitors can operate the system during the demonstration.

profile in terms of its effect on company performance. Moreover, the nature of the disruption and the dynamics of the company's response can be characterized by eight phases (Fig. 2). From the originally proposed, three phases were adopted in the exercise: first response to an disruptive event, preparation for recovery, and recovery. In the following paragraphs, the phases are described in detail, under the convention that *italicized* text represents the actual scenario descriptions provided to the participants.

Disruptive Event/First Response. The exercise starts when *an anomaly in network traffic is detected by the monitoring room* and *control room operators in Plant No. 2 notice unexpected value declaration in a level sensor.*

The goal of this phase is to determine that the incident is caused by a cyber attack, and that is not the result of either equipment or sensor failure. The participants discuss how to implement a cyber incident response for a transition

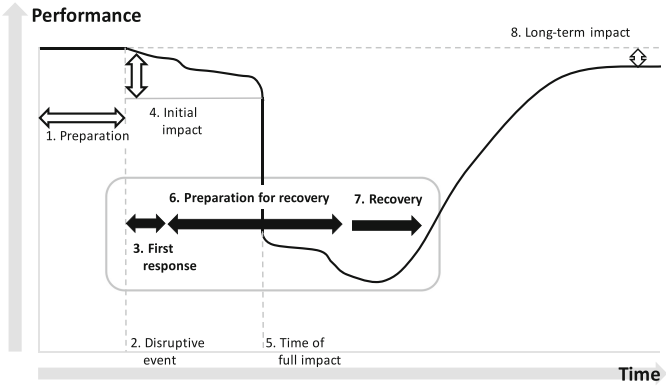

Fig. 2. Stages of disruption proposed by Sheffi [15], recreated by the authors.

to safe manual operation of the plant, and how IT and other departments can support the plant system to achieve safety.

Preparation for Recovery. The preconditions of this phase are that proofs of a cyber attack are confirmed (i.e. *no equipment/sensor malfunction detected*, *the configuration file of an OPC server in Plant No. 2 has been changed in an unauthorized manner*) and that *Plant No. 2 is operated manually*. The key decision-making in this phase is whether operation in Plant No. 2 should be shut down. Moreover, in case the plant is kept in manual operation, what measure should be taken to ensure safety. The participants discuss what kind of information is required to make a decision, if such information is available, and who has the authority to make a decision in this circumstance. They will conceive how to conduct business continuity management, in order to mitigate the further impact on business performance by the disruption. For example, what action should be taken at Plant No. 1 which is connected to Plant No. 2 through the corporate network, and what roles do the sales and public relations (PR) departments play.

Recovery. This phase assumes that the following conditions are met: *Plant No. 2 has been shut down* and *Plant No. 1 is operating without network connection (limited productivity)*. The task in this phase is to plan the efficient and safe plant reactivation based on the start up procedure manual. Additionally, participants review the past phases and discuss the measures to prevent a recurring failure.

As for the third and final phase of the exercise, the goal is to reexamine the balance of technical, management, and external cooperation capability to achieve high resiliency in the organization.

2.5 Exercise Steps

The exercise is composed of five steps: briefing, scene description, group work, discussion and debriefing. As mentioned in the previous section, the scenario is divided into three scenes (i.e. disruptive event/first response, preparation for recovery, and recovery). Therefore, scene description, group work and discussion are repeated as one cycle for each scene.

Briefing. At the beginning of the exercise, participants are divided into groups consisting of four to six members with different backgrounds. A facilitator introduces the group task and the general scenario. If needed, some ice breaker activities may be carried out to motivate all participants to become actively involved in the group work. Most importantly, the purpose of the exercise is shared with participants, so that they can all understand the significance of the activity.

Scene Description. As for the opening of each scene, the status of the plant and IT network system are revealed along with the (fictitious) organization's understanding of the situation. The scene is reenacted in a short video, which is used as visual aid.

Group Work. The group task is to create a work flow of actions that would solve the given situation. Each group is provided with a printed A0-sized worksheet, colored sticky-notes, and markers. On the worksheet, the columns of actors (e.g. IT dept., manufacturing dept., maintenance dept.) and the initial scenario injections are printed (Fig. 3). The list of actor names provided in the worksheet is not comprehensive, therefore participants are recommended to add/remove actor columns. At the beginning of each cycle, new worksheets including the scenario injections matching the current scene are distributed. The types of activity such as actor-system interaction (action) and actor-actor interaction (command) are color coded. In order to add an activity to the worksheet, a sticky-note of the matching color is used. In this way, the worksheet visualizes the flow of actors' actions and the organization's communication structure.

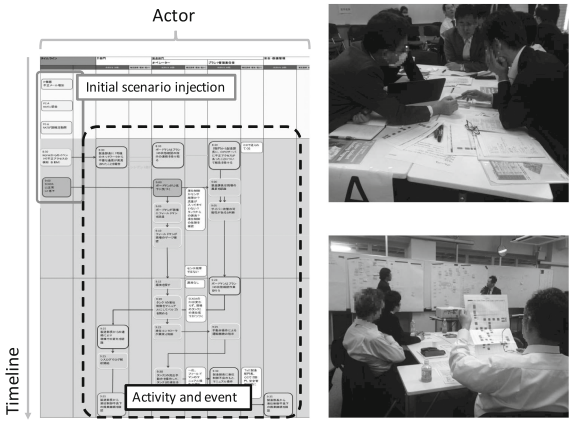

Fig. 3. The example of the worksheet (left) and pictures from the exercise (right) where participants engage in group work (top right) and present their group work at discussion time (bottom right). Participants' faces are blurred out for their privacy.

Discussion. The former process helps participants to create shared mental models within their group. On the other hand, discussion and debriefing are activities that create a shared mental model among all participants. Discussion is the final step of one cycle. Each group gives a short presentation of their work flow while displaying the worksheet to everyone. The members of other groups may raise some questions. In this way, participants compare their worksheets to discover similarities and differences among their subjective perspectives regarding the many degrees-of-freedom of the scenario (e.g. likelihood of an event, consequence of an action).

Debriefing. To conclude, the goals of the exercise are revisited, and participants share results and lessons learned. This activity helps the organizers to evaluate if the exercise method was appropriate, and more importantly, if the intended learning outcomes are achieved.

2.6 Administration Staff

The size and complexity of the exercise required a large number of personnel for assisting the exercise facilitation. For a smooth administration, the role were divided as follows: facilitator, adviser, and replier.

Facilitator. The facilitator guides participants through the exercise. He/she explains the exercise at briefing, and describes the scene at each cycle. During the group work, the facilitator pays attention to each group's progress, while keeping track of time. He/she also supervises the discussion and debriefing. In debriefing, he/she helps participants to summarize results and lessons learned.

Adviser. During group work, the adviser walks among tables and gives suggestions to each group based on his/her expertise. He/she also asks questions that trigger more actions and discussion. Therefore, the role requires knowledge and experience in the field. During discussion, the adviser provides positive feedback and comments for each group. We invited IT security specialists, ICS security researchers, and experts from ICS security agencies as advisers. These experts also helped during the process of scenario development.

Replier. The role of the replier is to reply the emails from each group as a (fictitious) "company employee" and to supplement the scenario. Participants cannot touch the system by themselves, given the nature of the table-top exercise. Therefore, some of the participants' emails are requests for additional information, while others are requests for taking action.

2.7 Pilot Exercises

Pilot exercises were conducted at the campus of Nagoya Institute of Technology as a part of two days ICS security workshop in August 2015 and March 2016.

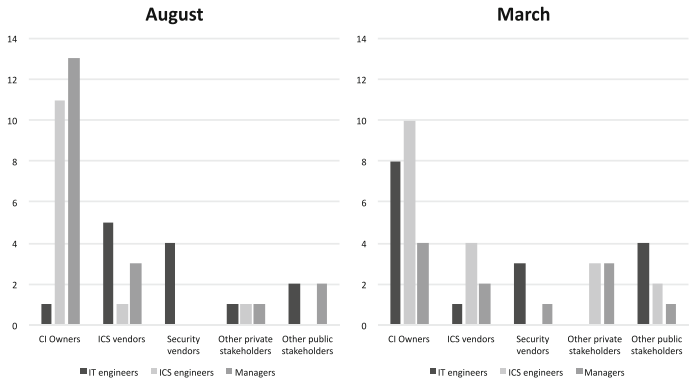

Fig. 4. Participant's profile distribution.

The number of participants was 45 and 46 respectively, and their expertise was heterogeneous. The distribution of participants' profiles at each workshop is shown in Fig. 4, where participants are classified by their organization types and occupational category. The sectors of CI owners included chemical, energy, gas, and telecommunication. In both exercises, participants were divided into six groups—totalling twelve groups—in order to facilitate the discussion. Since the exercise aims at stimulating the discussion and expand the participants' perspective, groups were carefully composed in order to maximise intra-group heterogeneity of expertise, background and position.

3 Results and Discussion

3.1 Variation of Incident Management Structure

The groups' worksheets were analyzed at discussion and debriefing time, by comparing the structure of their actions and commands. As a result, the following three types of incident management structures were found: IT department centered, production department centered, and management centered.

IT Department Centered. The IT department plays the leading role during the incident management. Specifically, it investigates the incident, and gives directions to the production department. Additionally, it provides updates about the situation to the management and to other departments who may be affected by the incident (e.g. sales, PR). In a real life situation, this structure may be applicable to an organization with a strong IT capability. Moreover, for the IT department to successfully lead the cyber incident response, it should have knowledge of the plant systems and a full understanding of the incident's impact on the business.

Production Department Centered. The production department leads the response, cooperates with the IT and other departments in charge of maintaining the production (e.g. the maintenance department), and gathers information related to the investigation and to the situation of the damage. This structure may be suitable for a large plant system where the production department has a strong leadership and authority. However, if the production department is unprepared to handle a cyber incident, the investigation may take longer than necessary, and potentially cause a bigger impact. Therefore, a thorough cyber security training of the production department personnel is necessary for this structure.

Management Centered. The management department leads the operation, by keeping an exclusive communication with the IT and the production departments, which don't directly exchange information with each other. One group even suggested to set up a crisis management headquarter, where all department

and management heads would cooperate. This structure is similar to the incident command system adopted for natural disasters [16], where plans and objectives are decided at the top of the hierarchy, while activities at the lower levels are a consequence of those decisions. In reality, this structure may be applicable to an organization with a highly centralized management system, or to a situation that requires the involvement of top management (e.g. large scale disaster, the critical service is not substitutable).

3.2 Results of the Survey

A survey was conducted after each pilot exercise. The results show that 94.7% (in August) and 90.9% (in March) of the participants were satisfied with the exercise, and that 83.0% (in August) and 90.6% (in March) would recommend the exercise to other CI stakeholders. In fact, some of the August workshop participants participated in the March workshop as well, and some extended the invitation to their colleagues.

3.3 Discussion

The proposed exercise aimed at training communication management skills of CI stakeholders and strengthen the cooperation capability of the CIP community, by engaging participants in discussion. We could observe that participants were stimulated by the exercise to express their point of view, acknowledge variety, and achieve a mutual understanding of an issue, regardless of their background. It can be said that the exercise encourages CI stakeholders to cultivate a shared mental model, which may positively influence performance [17]. Moreover, the exercise was general enough to stimulate the participants who did not belong strictly to the ICS security community (i.e. telecommunication sector), who in turn were satisfied by the acquisition of new knowledge. In conclusion, the unique experience of the exercise was appreciated by the CIP community.

As to the limitations of the current study, the evaluation of the pilot exercise was based on a subjective analysis. However, the overlap ('sharedness') of mental models can be explored using network analysis [18]. In future studies, the employment of objective evaluation techniques will be taken into consideration.

3.4 Future Work: "ICS-SIRT" Exercise

Based on consultation with the exercise participants, we realised that most organizations in the ICS field are not endowed with a tailored cyber incident procedure yet, and current incident management systems in the industry often miss coordinating capabilities. On the other hand, IT security organizations have adopted the Cyber Security Incident Response Team (CSIRT) as a common measure against cyber attacks. CSIRT is a team of IT security experts whose main duty is to mitigate, prevent, and respond to computer security incidents [19]. With the same philosophy, we believe that an ICS Security Incident Response

Team (ICS-SIRT), a team of ICS security experts, should be devised. In this context, the incident management structures proposed by the exercise participants reflect the possible communication structure of ICS-SIRT. Indeed, they are independent from the specific characteristics of CI sectors, which makes them suitable for any type of organization. Each organization would establish its own ICS-SIRT, which has a consistent communication structure across sectors and is connected with ICS-SIRTs of other organizations, strengthening the horizontal cooperation among CI stakeholders.

Future studies will explore the possibility of expanding the proposed exercise towards the development ICS-SIRT inside the organizations affiliated with Nagoya Institute of Technology.

Acknowledgements. This research is partially supported by the Ministry of Education, Science, Sports and Culture, Grant-in-Aid for Scientific Research (A), No. 16H01837 (2016); however, all remaining errors are attributable to the authors.

References

1. SANS Institute: 2016 Security Awareness Report. SANS Institute (2016). http://securingthehuman.sans.org/resources/security-awareness-report
2. Department of Homeland Security: Training available through ICS-CERT. https://ics-cert.us-cert.gov/Training-Available-Through-ICS-CERT#workshop
3. Sitnikova, E., Foo, E., Vaughn, R.B.: The power of hands-on exercises in SCADA cyber security education. In: Dodge, R.C., Futcher, L. (eds.) WISE 2009. IAICT, vol. 406, pp. 83–94. Springer, Heidelberg (2013). https://doi.org/10.1007/978-3-642-39377-8_9
4. Foo, E., Branagan, M., Morris, T.: A proposed Australian industrial control system security curriculum. In: 2013 46th Hawaii International Conference on System Sciences (HICSS), pp. 1754–1762. IEEE (2013)
5. European Network for Cyber Security: E.ON teams get trained on ICS and smart grid cyber security during the ENCS red team blue team course—ENCS. https://www.encs.eu/2015/11/10/
6. Branlat, M.: Challenges to adversarial interplay under high uncertainty: staged-world study of a cyber security event. Ph.D. thesis, The Ohio State University (2011)
7. Branlat, M., Morison, A., Finco, G., Gertman, D., Le Blanc, K., Woods, D.: A study of adversarial interplay in a cybersecurity event. In: Proceedings of the 10th International Conference on Naturalistic Decision Making (NDM 2011), 31 May–3 June 2011
8. Aoyama, T., Naruoka, H., Koshijima, I., Watanabe, K.: How management goes wrong? The human factor lessons learned from a cyber incident handling exercise. Procedia Manuf. **3**, 1082–1087 (2015). 6th International Conference on Applied Human Factors and Ergonomics (AHFE 2015) and the Affiliated Conferences, AHFE 2015. http://www.sciencedirect.com/science/article/pii/S2351978915001791
9. Aoyama, T., Naruoka, H., Koshijima, I., Machii, W., Seki, K.: Studying resilient cyber incident management from large-scale cyber security training. In: 2015 10th Asian Control Conference (ASCC), pp. 1–4. IEEE (2015)

10. Watanabe, K.: Developing public-private partnership based business continuity management for increased community resilience. J. Bus. Contin. Emerg. Plann. **3**(4), 335–344 (2009)
11. Borell, J., Eriksson, K.: Learning effectiveness of discussion-based crisis management exercises. Int. J. Disaster Risk Reduct. **5**, 28–37 (2013). http://www.sciencedirect.com/science/article/pii/S2212420913000332
12. US Department of Homeland Security and United States of America: Homeland security exercise and evaluation program (HSEEP) volume I: HSEEP overview and exercise program management (2007)
13. Aoyama, T., Koike, M., Koshijima, I., Hashimoto, Y.: A unified framework for safety and security assessment in critical infrastructures. In: Safety and Security Engineering V. Witpress Ltd., September 2013. http://dx.doi.org/10.2495/SAFE130071
14. Takagi, H., Morita, T., Matta, M., Moritani, H., Hamaguchi, T., Jing, S., Koshijima, I., Hashimoto, Y.: Strategic security protection for industrial control systems. In: 2015 54th Annual Conference of the Society of Instrument and Control Engineers of Japan (SICE), pp. 986–992. IEEE (2015)
15. Sheffi, Y., Rice Jr., J.B.: A supply chain view of the resilient enterprise. MIT Sloan Manag. Rev. **47**(1), 41 (2005)
16. Bigley, G.A., Roberts, K.H.: The incident command system: high-reliability organizing for complex and volatile task environments. Acad. Manag. J. **44**(6), 1281–1299 (2001)
17. Converse, S.: Shared mental models in expert team decision making. In: Castellan, N.J. (ed.) Individual and Group Decision Making: Current Issues, p. 221. Lawrence Erlbaum, Hillsdale (1993)
18. Mathieu, J.E., Heffner, T.S., Goodwin, G.F., Salas, E., Cannon-Bowers, J.A.: The influence of shared mental models on team process and performance. J. Appl. Psychol. **85**(2), 273 (2000)
19. Bronk, H., Thorbruegge, M., Hakkaja, M.: A step-by-step approach on how to set up a CSIRT (2006)

http://www.springer.com/978-3-319-71367-0

Critical Information Infrastructures Security
11th International Conference, CRITIS 2016, Paris, France, October 10–12, 2016, Revised Selected Papers
Havarneanu, G.; Setola, R.; Nassopoulos, H.; Wolthusen, S. (Eds.)

2017, XI, 348 p. 103 illus., Softcover
ISBN: 978-3-319-71367-0