Human Factors in Cybersecurity, Vol. 127, 2024, 105–114
https://doi.org/10.54941/ahfe1004770

Analyzing Important Factors in Cybersecurity Incidents Using Table-Top Exercise

Kenta Nakayama[1,2], Ichiro Koshijima[2], and Kenji Watanabe[1]

[1]Nagoya Institute of Technology, Gokiso-cho, Showa, Nagoya, Japan
[2]Manufacturing and Innovation DX Laboratory, Nagoya Institute of Technology, Gokiso-cho, Showa, Nagoya, Japan

ABSTRACT

In recent years, the threat of cyber-attacks has been increasing yearly. Various organizations should take countermeasures for it. In the face of increasing threats, organizations need to take not only technical measures but also human countermeasures. However, cyber-attacks themselves are becoming more sophisticated, so organizations need to prepare countermeasures and organizational structures based on the assumption that incidents due to cyber-attacks will occur. Moreover, organizations are required to minimize the damage caused by cyber-attack incidents and continue their business operations. This study focused on human countermeasures, especially organizational structures, designed an incident response exercise, and conducted it with approximately 60 members of a critical infrastructure company in Japan. Based on the exercise records and the post-exercise questionnaire results, these results examine organizational and human barriers that organizations may face in incident response and the organizational structure that minimizes the damage from incidents. The questionnaire survey was conducted after the exercise, and the exercise itself received a high evaluation, with an average score of 4 or higher out of 5. In addition, information on important items in incident response, including changes before and after the exercise, was collected through free-text statements. Context-based evaluation and analysis of the collected results revealed what members of the Japanese critical infrastructure community consider important in incident response.

Keywords: Cybersecurity, Incident response, Human factor countermeasures, Resilience, Table top exercise

INTRODUCTION

In recent years, the increase in cyber-attacks has made it imperative to secure not only technical measures but also human resources. However, cyber security personnel are in short supply, and in a survey of Japanese companies, approximately 88% said they lack cyber security personnel (KPMG, 2023). Therefore, cyber security training and exercises are being conducted for personnel involved in IT systems and control systems (NISC, 2023). In light of these current conditions, cyber security exercises are one of the important security measures, and it is also important to review the organizational structure and process improvement cycle based on the exercise results. Existing studies have proposed card game exercises with specific actions for any

given incident scenario (Mizuno 2019, Nakayama 2023). These can simulate many incidents repeatedly to strengthen incident response capabilities. However, because the actions are specified, it is difficult for participants to think of their actions and put them into practice during the exercise. In addition, there is no system in place for review after the exercise or for post-incident response. In this study, a method in which participants assume specific roles and conduct exercises based on their ideas was considered. In addition, chronology, which is also used at disaster sites, was adopted as a recording method so that participants could look back on the content of the incident response. In addition, a simple incident response manual was prepared to assist participants, and they were encouraged to review the manual as necessary during the exercise. After the exercise, participants were asked to review the recorded chronology and revise the incident response manual to include the post-incident response phase. In addition, the recorded chronology revised manual, and post-exercise questionnaire were analyzed using text mining techniques. Through these analyses, we attempted to extract important elements in incident response and barrier elements that hinder the incident response. The extracted items will also provide insight into the nature of the organization and the transfer of authority.

METHODS

In conducting the exercise, a virtual company is set up so that participants can have a common understanding of the exercise. The virtual company is a company that has a control system and two plants from which it provides services. The services to be provided can be configured arbitrarily, but for this exercise, a service to supply heat sources to neighboring facilities was defined. As a prerequisite, a plant shutdown directly affects the business of the hypothetical company. In addition, if the control system in the plant becomes uncontrollable, human lives may be endangered. Figure 1 shows a network diagram of the virtual company. The participants in the exercise will work while looking at the network configuration diagram in Figure 1.

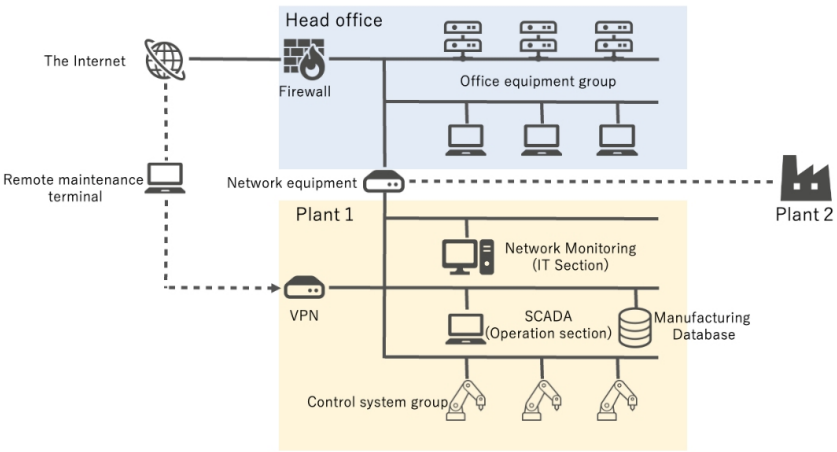

Figure 1: Network diagram of the virtual company.

In addition, participants are assigned roles in the virtual company shown in Table 1. Participants will engage in the exercise while considering their assigned role. Rather than having everyone participate in a discussion about incident response, participants are assigned specific roles, and by considering the priorities of each role, they cannot only resolve the incident, but also, if they are in management, consider the impact of the incident on the business, and if they are in the plant, to consider the impact of the incident on the plant operations and lifesaving. For plant personnel, the objective is to broaden their perspectives from multiple perspectives, including plant operations and lifesaving, and to gain an understanding and awareness of the different elements and ways of thinking that are important in incident response as an organization.

Table 1. Characters and their roles in the virtual company.

Loc.	Role	Role Details
Head office	Management	Make management-related decisions Represent the organization, including accountability
	Sales Div.	Performs operations for customers
	CSIRT	Performs system security duties Has a role in planning, implementation, response, etc.
	Back Office Div.	Perform tasks related to public relations, general affairs, accounting, and human resources
	IT Div.	Performs construction, operation, and maintenance of internal information systems and infrastructure
	Manufacturing Div.	Operate and maintain the plant to provide services
Plant1	Plant Manager	Oversee plant operations
	Operation Section (Boardman)	Performs duties related to the operation • Monitors and operates SCADA screens
	Operation Section (Fieldman)	Performs duties related to the operation • Checks and operates on-site equipment
	Instrumentation/ Equipment Section	Manage maintenance of plant instrumentation and equipment
	Safety Management Section	Design accident prevention for process safety, occupational safety, etc.
	IT Section	Management and operation of the network in the plant
Others	Others	*Set up as necessary in the exercise

Incident response exercises are conducted in the form of scenarios in which events occur over time, and each person in charge coordinates information and decides on a response policy. As shown in Table 2, the scenario of the incident response exercise is divided into three major phases: Predictive, Emergency, and Recovery. The total duration of the exercise is expected to be

70 minutes. The discussion during the exercise was conducted using chronology, which is also used in disaster response so that the discussion can be reviewed in chronological order. At a disaster site, information is organized in chronological order on a whiteboard, but for this exercise, chronology using Excel was adopted due to the need to tally the information. The chronology summarizes the content of discussions in chronological order and also records who contacted whom to clarify the information network at the time of incident response.

Table 2. Incident response exercise scenario.

Phase	Events	Discussion Points
Predictive (10 min)	The customer informs sales that the service is not working.	• What are the possible causes at this point? • Where is an internal inquiry considered appropriate?
	Fieldman told us the plant's safety valve was open. *Meaning that some kind of abnormality has occurred in the actual equipment of the plant.	• What are the possible causes at this point? • Where is an internal inquiry considered appropriate?
Emergency (30 min)	Threats are found on office terminals in Back Office Div. *Threatening letter Pay 50 BTC within 3 days or we will shut down the system	• To what extent and how to report incidents that have occurred • What are the possible business consequences? • How do we decide whether or not to pay the ransom?
	Threats are found on SCADA terminals in Plant 1 *Threatening letter Pay 50 BTC within 3 days or we will shut down the system	• To what extent and how to report incidents that have occurred • What are the possible business consequences? • How do we decide whether or not to pay the ransom? • What is considered to be the extent of ransomware infection?
Recovery (30 min)	SCADA terminal will no longer be able to control the plant *For the sake of the exercise scenario, let's assume that no ransom was paid	• To what extent and how to report incidents that have occurred • How do you consider the impact on business continuity? • How do we decide to shut down the plant or operate it manually?

For this incident response exercise, a simplified manual was prepared by the JPCERT/CC incident response flow. During the exercise, participants

were asked to respond flexibly according to the situation while referring to this manual. After the exercise, participants practiced improving the manual and simulated post-incident response. The manual summarizes the general framework of incident response in a virtual company in the following five items.

Contents of the Incident Response Manual (JPCERT, 2021)

1. incident detection and reporting
2. initial response to the incident
3. notification of the incident
4. incident containment and recovery
5. post-incident response

Table 3. Content of post-exercise questionnaire.

No.	Question	Answer Format
1	What was your most recent assignment? CSIRT, SOC, Information System Div., Manufacturing Div., Vendor/SIer, Others (Free text)	Multiple choice
2	How many years of work experience do you have for Q1?	Free text
3	Please indicate any work experience other than Q1	Free text
4	Overall satisfaction with the incident response exercise (Small: 1 - Large: 5)	5-point rating
5	Please tell us the reason for the above	Free text
6	Please rate your efforts during the exercise (Bad:1 - Good:5)	5-point rating
7	Will chronology be useful in the incident response? (1: Not useful at all - 5: Very useful)	5-point rating
8	Please tell us about any difficulties you had in conducting the exercise.	Free text
9	What items in the incident response manual would speed up the incident response process?	Free text
10	Please tell us what you thought was important in incident response "before" this exercise.	Free text
11	Please tell us what, if any, changes you have made to your thoughts on Q10 "after" this exercise.	Free text
12	Please tell us what you learned and realized through this exercise.	Free text
13	Please tell us what could be improved for the exercise (e.g., what was difficult to understand)	Free text

After the exercise, a questionnaire was administered to measure the effectiveness of the exercise. The content and format of the questionnaire are shown in Table 3. The background of the participants, their satisfaction with the exercise, their attitudes toward incident response before and after the exercise, and how they have changed since the exercise will be confirmed. In addition, the effectiveness of the chronology used in the exercise during incident response will also be investigated. The text mining tool, User Local AI

Text Mining (https://textmining.userlocal.jp/), will be used for the free text responses.

RESULTS

The exercise lasted for three days and was attended by 63 participants (14 teams). The survey responses were collected for all teams, but the chronology of the exercise was corrupted for one team, so the results of 13 teams were used for the relevant analysis. Table 4 shows the number of participants and their level of satisfaction with the exercise for each day.

Table 4. Exercise participants and satisfaction with each schedule.

No.	Date	Participants	Teams	Evaluation Point Avg.	Evaluation Point SD.
1	October 4, 2023	20	4	4.20	0.62
2	November 8, 2023	22	5	4.14	0.56
3	December 18, 2023	21	5	4.24	0.70

Satisfaction With the Exercise

Each session scored an average of 4 or higher, proving that each session provided an exercise of equal quality with a high degree of satisfaction. This allows us to assume that the quality of the exercises will have a low impact on the results of the analysis in subsequent results, which will reflect the background and thinking of each participant. The backgrounds of the participants and the number of participants in each session are shown in Table 5.

Table 5. Background information on participants and number of participants per date.

No.	Role (Background)	No. 1	No. 2	No. 3	Total
A	CSIRT	2	5	6	13
B	SOC	1	3	2	6
C	Information System Div.	9	4	4	17
D	Manufacturing Div.	4	0	3	7
E	Vendor/SIer	3	5	5	13
F	Others	1	5	1	7

Evaluations of the Chronology in the Incident Response Exercise

The validity of the chronology used in the exercise was also verified in questions 7 and 8 of the questionnaire. The results show that only No. 1's evaluation of chronology during the exercise exceeded 4 points on average, while the average score for No. 2 and 3 was about 3.5 points. The standard deviation also appears to be greater than 0.9 compared to No. 1. The backgrounds of the participants in each session were different, and they were

not evenly distributed as shown in Table 5. Therefore, the validity of the chronology was evaluated for each participant's background, as shown in Table 6.

Table 6. Evaluation of the use of chronology during incident response for each background.

No.	Role (Background)	Evaluation Point Avg.	Evaluation Point SD.
A	CSIRT	3.38	1.04
B	SOC	3.50	1.05
C	Information System Div.	3.82	0.95
D	Manufacturing Div.	3.86	0.69
E	Vendor/SIer	3.92	0.76
F	Others	3.71	0.76

From these results, it can be seen that the CSIRT and SOC gave chronology a score of 3.5 or less, with a standard deviation of more than 1, indicating that the effectiveness of chronology is not well evaluated. The standard deviation for the Information System Division was 0.95, which is relatively close to the standard deviation for CSIRT and SOC. The common points among the three divisions are daily IT-related work, monitoring and operations, and actual cyber security incidents. The commonality among the three is that they are engaged in IT-related operations, monitoring, and operations daily, as well as in responding to actual cybersecurity incidents. Some of the comments in the questionnaire included, "I think it would be difficult to describe in the chronology when an actual incident occurs," and it can be inferred that it would be difficult to describe in the chronology using Excel this time when an actual incident occurs. However, since the average evaluation out of 5 points was above the median, a certain effectiveness of the chronology was demonstrated in incident response exercises such as this one.

Important Factors in Incident Response

The important items in incident response were identified in Q10 of the questionnaire items, and changes in their thinking were checked in Q11 after the exercise. It was confirmed that 59% (37 respondents) of the total respondents changed their thinking or came up with additional ideas before and after the exercise and that more than half of the respondents brought about changes or new insights into their thinking about incident response before and after the exercise. The top five most frequently occurring nouns in the survey responses are shown in Table 7. The responses of those whose thinking did not change before and after the exercise were retained in the table. In both questions, "information" appeared frequently after "response," indicating the importance of information in incident response. In addition, "speed" was ranked third before the exercise (Q3), but was ranked lower than fifth after the exercise (Q11). In Q10, "communication" and "manual" were also in the top five, but in Q11, "decision" was more frequent. This can be inferred as a result of the importance of decision-making in each role in the incident response exercises, as some roles require decision-making. The "response,"

"manual," and "incident," which were also ranked in the same category, were incident response exercises that used some of the manuals. For further discussion, the results of Q11 were analyzed using a co-occurrence network shown in Figure 2. The co-occurrence network has been traditionally used in content analysis to statistically express the data (Osgood 1959, Danowski 1993).

Table 7. Ranking of frequently appearing words in survey questions 10 and 11.

No.	Before(Q10)		After(Q11)	
1	response	14	response	16
2	information	13	information	12
3	speed	9	incident	10
4	communication	8	manual, communication, decision	8
5	manual	7	-	-

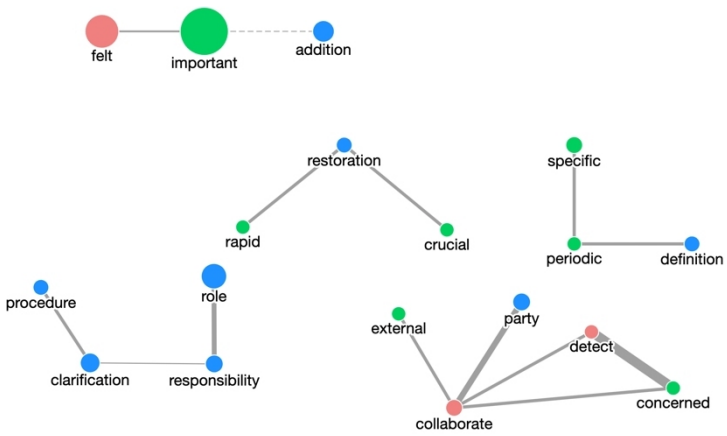

Figure 2: Co-occurrence network created from responses to survey Q11 (extract only items with 3 or more nodes).

Figure 2 shows that there is a network of roles and responsibilities and that these roles and responsibilities are linked to a network of clarification and procedures. In addition, the word "collaboration" is used as a starting point for considering and identifying external and other departments. Based on the results, it is considered important to clarify the roles and responsibilities of each person in incident response, and for the person in charge to make appropriate decisions based on these procedures. In addition, information is important to support these roles, and accurate information must be provided to the appropriate personnel during the incident response process. Therefore, it is important to show the roles, authorities, and procedures, including the organization structure, in advance of the incident response.

To examine the organizational structure, the contact source and contact person recorded in chronology during the exercise were analyzed, and the average percentage of appearances of these roles during the exercise was calculated and each is shown in Figure 3. CSIRT plays a central role in incident

response, followed by the plant manager, who is involved in the core of coordination during incident response. In the scenario of the incident exercise, the plant manager was entrusted with the final decision in many cases because the incident involved plant operations. In other words, the head of the site, who is involved in the core of the business when an incident occurs, is required to make appropriate judgments at the time of the incident. Therefore, it is necessary for the organization to define a central organization for incident response, such as a CSIRT, and a role for on-site management in the event of an impact on the company's business, and to transfer the necessary authority to this organization.

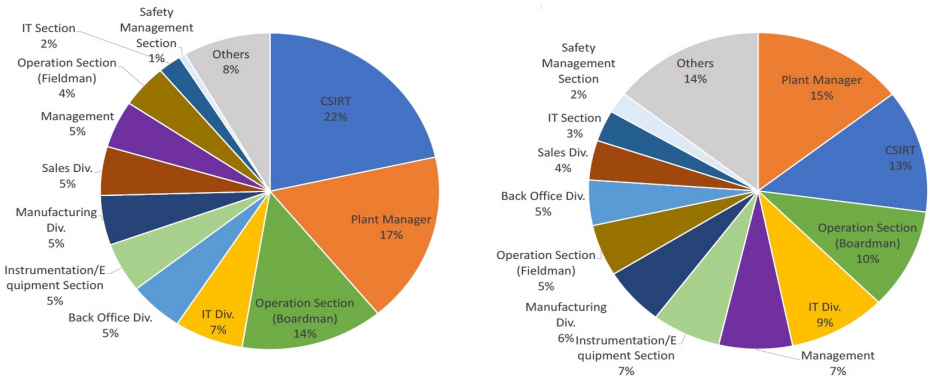

Figure 3: Percentage of contact source (left) and person (right) listed on chronology.

CONCLUSION

In this study, an incident response exercise was conducted and the contents of the questionnaire and contact information recorded on the chronology were analyzed. The exercise was highly satisfactory overall, and more than half of the participants found it useful in changing their thinking about incident response and providing new insights after the exercise. In addition, analysis of the questionnaire and chronology confirmed the importance of clarifying information and the roles and authority of each person in charge of incident response and establishing procedures in advance. In the future, we aim to create a mechanism for information coordination in incident response by analyzing the details of the roles that serve as a place for information collection and the contents of the manual improvement exercise conducted after the exercise.

ACKNOWLEDGMENT

I would like to acknowledge the IPA Industrial Cyber Security Center Trainees who participated in this exercise, as well as Prof. Koshijima and Prof. Hashimoto for their support in conducting the exercise.

REFERENCES

Danowski, J. A. (1993). Network Analysis of Message Content. In W. D. Richards Jr. & G. A. Barnett (Eds.), Progress in Communication Sciences IV (pp. 197–221). Norwood, NJ: Ablex.

JPCERT Coordination Center., (2021) Creation of Incident Response Manual. https://www.jpcert.or.jp/csirt_material/files/13_incident_response_manual_20211130.pdf

KPMG. (2024). Cyber security Survey 2023. https://assets.kpmg.com/content/dam/kpmg/jp/pdf/2024/jp-cyber-security-survey2023.pdf

Mizuno, E., et al. (2021). Cyber Incident Response Tabletop Exercise to Raise Ownership. https://doi.org/10.11511/jacc.64.0_1152

Nakayama, K., Watanabe, K. (2023). Incident response exercises and methodologies to guide best practices for incident response in healthcare institutions. AHFE (2023) International Conference. AHFE Open Access, vol. 116. AHFE International, USA. http://doi.org/10.54941/ahfe1004378

NISC. (2023). Targeting 14 areas of critical infrastructure Cyber Exercise to Verify Disaster Response System-FY2023 "Cross-cutting Exercise" - https://www.nisc.go.jp/pdf/policy/infra/NISC_enshu_20231208.pdf

Osgood, C. E. (1959). The Representational Model and Relevant Research Methods. In I. d. S. Pool (Ed.), Trends in Content Analysis (pp. 33–88). Urbana, IL: University of Illinois Press.