Emerging Technologies in Healthcare and Medicine, Vol. 116, 2023, 246–253
https://doi.org/10.54941/ahfe1004378

Incident Response Exercises and Methodologies to Guide Best Practices for Incident Response in Healthcare Institutions

Kenta Nakayama[1,2] 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

Cyber-attacks on healthcare institutions have been increasing in recent years, and organizational security measures are urgently needed. However, healthcare institutions face challenges such as limited IT investment and a lack of specialists. In order to enhance organizational resilience with limited IT investment and human resources, this paper proposes an incident response exercise drawing insights from previous research and actual security incident cases within healthcare institutions. Furthermore, this study endeavors to create comprehensive incident response manuals and formulate condensed incident response matrices. These endeavors have the potential to unearth optimal practices for addressing incidents within healthcare institutions.

Keywords: Cyber-security, Non-technical countermeasures, BCP, Human-centric perspective

INTRODUCTION

The threat of cyber-attacks has been on the rise in recent years, exposing a wide variety of institutions to attacks. Check Point, a U.S. security vendor, reported that the number of cyber-attacks against organizations per week increased by approximately 38% from 2021 to 2022 (Check Point Research Team, 2023). Figure 1 shows the number of cyber-attacks on organizations by industry, followed by Education/Research, Government/Military, and Healthcare. Among these, cyber-attacks on healthcare increased the most (74%) from 2021 to 2022. This is because the systems of healthcare organizations are likely to be relatively more vulnerable than those of organizations with sensitive information, such as Education/Research and Government/Military, despite healthcare-related information containing sensitive information, such as personal disease information. In fact, IT investment in healthcare organizations has been limited. In addition, IT investment in healthcare organizations is limited, and cyber-security measures are inadequate (Kruse, 2017). As a result, old, unsupported operating systems remain, and their critical vulnerabilities increase the risk of security incidents. However, since the threat of cyber-attacks is increasing every year, organizations

need to accept a certain level of risk with their limited IT investments, while maintaining resilience to enable rapid recovery in the event of a security incident.This paper develops exercises to increase resilience in the event of those incidents and makes recommendations for a series of PDCA cycles.

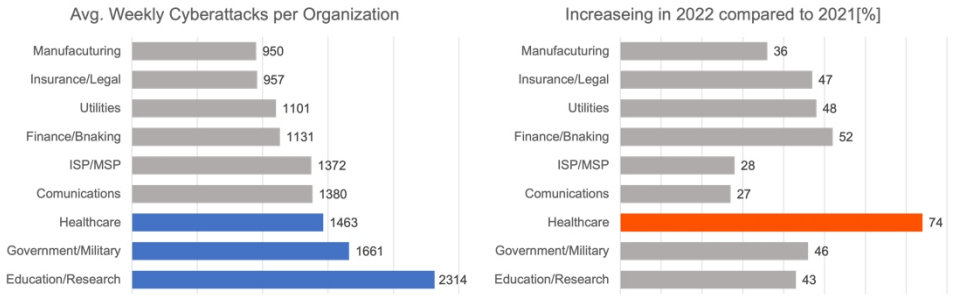

Figure 1: Avg. weekly cyber attacks per organization (left figure) and increasing rate in 2022 compared to 2021 per organization (right figure) (check point research team, 2023).

Method

In a previous study, an exercise using about 40 action cards to discuss what information is necessary for information coordination and decision-making against cyber-attacks was recommended, and employees of a critical infrastructure company actually participated in the exercise (Davaadorj, 2018. Figure 2). A questionnaire survey of the exercise participants revealed positive comments such as satisfaction with the exercise and a reaffirmation of the importance of communication within the organization. Although the exercise was conducted for critical infrastructure companies, it was actually designed to simulate cyber-attacks on a plant for a manufacturing company with a plant. This paper examines incident response exercises for healthcare institutions in the following steps.

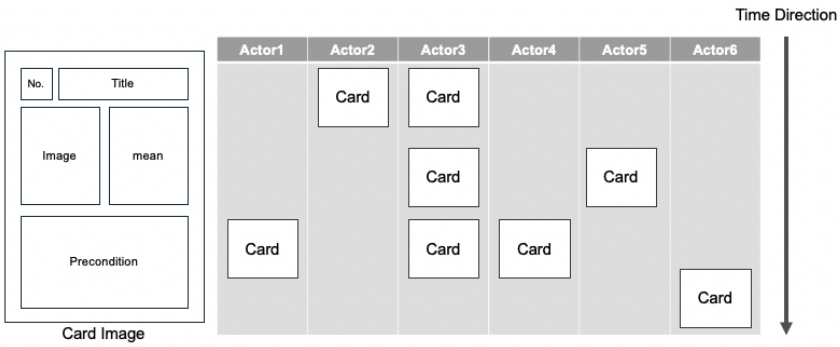

Figure 2: Card and placement board images (Davaadorj, 2018).

(1) Examine exercise scenarios based on security incident cases
- Analyze system failures based on cyber-attacks from cases of system failures at healthcare institutions that occurred and were reported in Japan from 2021 to 2022, and study exercise scenarios.

(2) Define a network configuration diagram
- Define a hypothetical healthcare institution network for the exercise based on the information listed in (1).

(3) Definition of stakeholders of healthcare institutions (exercise participants)
- Organize and define healthcare institution personnel and external parties based on NIST SP800-61.

(4) Examine response contents and scripts
- Define responses in the anticipation, emergency, and recovery phases.

RESULTS

This chapter describes the results of the study according to the four steps introduced in Method.

(1) Examine exercise scenarios based on security incident cases

Table 1 lists the system failures of Japanese healthcare institutions reported in 2021-2022. There were a total of 11 cases, 7 of which were caused by unauthorized access and 6 by ransomware infection. Further reading of the 7 cases of unauthorized access reveals that 3 of the cases were caused by intrusion into the organization's system through a VPN vulnerability. Although detailed investigation results for the other four cases of unauthorized access have not been made public, it can be inferred from the number of cases and times that the unauthorized access may have been carried out via a VPN vulnerability that was similarly disclosed on the Internet. Therefore, the incident response exercise recommended in this paper is based on the scenario of a ransomware incident in which an organization's system is infiltrated via an external public VPN, and system information is subsequently encrypted.

(2) Define a network configuration diagram

Ransomware incidents caused system failures, mainly due to the encryption of the electronic medical record system (EMR), which resulted in the suspension of medical services. The VPN device that served as the intrusion route was used to maintain the hospital information system (HIS), and such a configuration is considered a typical HIS configuration. Based on these examples, a diagram of the healthcare institution network configuration used in the exercise is shown in Figure 3. HIS network can be maintained via VPN from an external vendor and is logically separated from the adjacent IT network. The HIS network has a Picture Archiving and Communication System (PACS) that stores electronic medical records (EMR) and radiographs, and is characterized by a configuration different from that of IT networks.

(3) Definition of stakeholders of healthcare institutions (exercise participants)

The parties involved in incident response are organized in Table 2 based on incident cases, reports, and NIST SP 800–61 (Paul, 2012).

Table 1. System failures of healthcare institutions reported in Japan in 2021-2022.

No.	Date	Institution	Detail	Factor
1	April 6, 2021	KAISEI Hospital, Kagawa	System failure (Tsukasa, 2021)	Unravel
2	May 31, 2021	Higashiosaka City Medical Center, Osaka	System failure (Masahiko, 2021)	Unauthorized Access
3	October 1, 2021	Fuji Hospital, Shizuoka	System failure (Norio, 2021)	Unauthorized Access
4	October 31, 2021	Handa Hospital, Tokushima	Ransomware - Lockbit2.0 (Yasuhi, 2021)	Unauthorized Access (via VPN vulnerability)
5	January 14, 2022	Nihon University School of Dentistry Dental Hospital, Tokyo	System failure (Nikkei, 2022)	Virus
6	January 12, 2022	Kasugai Rehabilitation Hospital, Aichi	Ransomware (Masako, 2022)	Unauthorized Access
7	April 23, 2022	Aoyama Hospital, Osaka	Ransomware (Kota, 2022)	Unauthorized Access
8	June 19, 2022	Naruto Yamakami Hospital, Tokushima	Ransomware - Lockbit2.0 (Naruto Yamakami Hospital, 2022)	Unauthorized Access (via VPN vulnerability)
9	October 27, 2022	Tazawa Iin, Shizuoka	Ransomware (Tazawa Iin, 2022)	Unravel
10	October 31, 2022	Osaka General Medical Center, Osaka	Ransomware - Phobos variants (Takeshi, 2022)	Unauthorized Access (via VPN vulnerability)
11	December 3, 2022	Kanazawa Nishi Hospital, Ishikawa	System failure (Yuri, 2022)	Unravel

Two of the most unique healthcare institutions are the medical department and other healthcare institutions in the same region. What each considers when an incident occurs is as follows.

Medical Department

This department includes everything from weekday diagnostics and surgery to emergency outpatient services. When an incident occurs, it is necessary to consider suspending medical treatment, postponing surgery, or transferring the patient to other healthcare institutions.

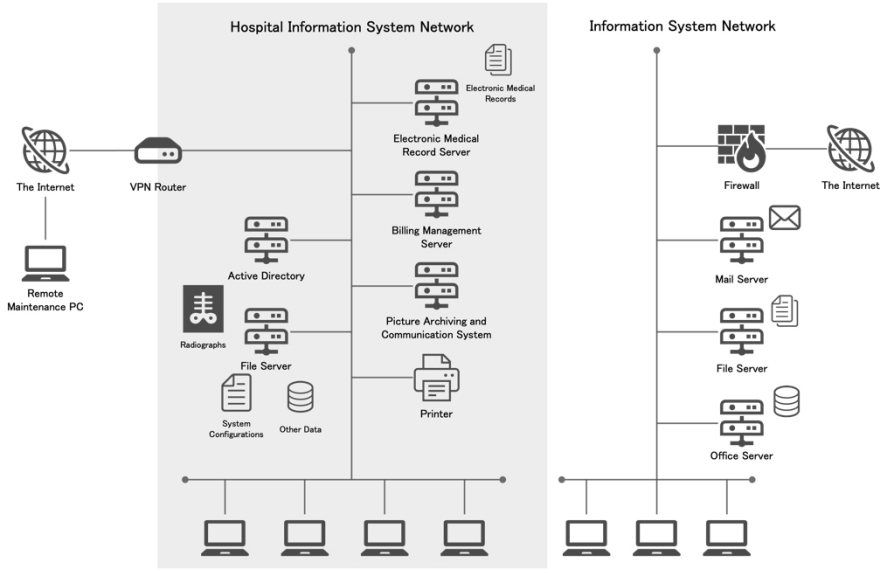

Figure 3: System network configuration for exercise.

Table 2. Stakeholders of incident response (bold letters are specific in healthcare institutions).

Dependencies within Organizations	Outside Parties
• Management (Board of Directors) • IT Department • Administrative Department • **Medical Department** • Legal Department • Public relations Department	• The Media • Low Enforcement • Incident Reporting Organizations e.g. ISACs, other healthcare institutions • Others e.g. ISP, Software Vendors

Other Healthcare Institutions

Need to collaborate with other healthcare institutions in order to transfer patients who require emergency diagnosis or surgery, or to request an ambulance to be dispatched to the hospital. In a city with only a limited number of hospitals, it is necessary to take into account coordination in the event of an incident from the perspective of regional medical BCPs (Business Continuity Plan).

(4) Examine response contents and scripts

Response items in the exercise were organized according to the system network configuration defined in Figure 3, based on previous research and incident case studies that have been published in detail (Davaadorj, 2018. Yasuhi, 2021. Takeshi, 2022). In addition, the scripts in the exercise were exercise stories (ISO, 2013) to help the participants understand how the

events unfolded during the exercise, and these were examined in the anticipation, emergency, and recovery phases. The scripts for each phase are as follows, and the corresponding items are shown in Figure 4, along with an image of the exercise board.

Predictive Phase

-Terminal operation of the HIS system deteriorates.
-Time-consuming access to the file system on the IT system side.
-EMR server freezes.

Emergency Phase

-Ransomware threats are found on the printer.
-EMR personal information is encrypted.

Recovery Phase

-System could be restored using backups.
-EMR is restored to normal operation.

Phase	Management	Medical Dep.	···	Actor X
Anticipation				
Emergency				
Recovery				

Exercise Bord

1	Information Sharing	21	Decision to Resume General Medical Services
2	Dissemination of Information across the entire organization	22	Temporary Suspension of Surgeries
3	Verification of the EMR System	23	Resumption of Surgeries
4	Verification of the PACS	24	Decision to Temporary Suspend Surgeries
5	Verification of the Billing Management System	25	Decision to Resume Surgeries
6	Verification of the Appointment Management System	26	Temporary Suspension of Ambulance Acceptance
7	Verification of the Patient Portal	27	Resumption of Ambulance Acceptance
8	Isolation of the EMR System	28	Decision to Suspend Ambulance Acceptance
9	Isolation of the PACS	29	Decision to Resume Ambulance Acceptance
10	Isolation of the Billing Management System	30	Collection of Vulnerability Information
11	Isolation of the Appointment Management System	31	Collection of Threat Information
12	Isolation of the Patient Portal	32	Response to New Patients
13	Confirmation of Logs from the EMR System	33	Support for Existing Patients
14	Verification of Logs from the PACS	34	Initiation of Operations with Paper Medical Records
15	Verification of Logs from the Billing Management System	35	Termination of Paper Medical Record Operations
16	Verification of Logs from the Appointment Management System	36	Interruption of Communication between IT and HIS Network
17	Verification of Logs from the Patient Portal	37	Restart of Communication between IT and HIS Network
18	Temporary Suspension of General Medical Services	38	Forensic Examination of Medical Devices
19	Resumption of General Medical Services	39	Verification of Unmanaged Devices Connected to HIS Network
20	Decision to Temporarily Suspend General Medical Services	40	Inspection of Suspicious Logs in IT Network

Response Contents (Card Items)

Figure 4: Exercise bord (left) and response contents (right).

There is no specification of who is in charge of the items to be handled, and the exercise participants choose the items to be handled and place the cards on the exercise board according to the scripts that are introduced sequentially. By discussing in the exercise who will be in charge of the items on the cards, the participants aim to gain an awareness of the current status of the incident response system in their own organizations as well as the roles and functions that are lacking. These exercises are expected to improve the security awareness of participants.

Discussion & Challenge

Cycling through the planning, execution, and improvement phases are essential for exercises (ISO, 2013), but this paper is still on the planning stage. The

next steps are to conduct exercises in healthcare institutions and incorporate feedback to enhance the exercises. In this exercise, response actions for the anticipation, emergency, and recovery phases are allocated to respective individuals. As these details become refined, the exercise board itself could serve as a quick reference manual. Regarding documentation, as decision-making processes are crucial, a chronological record of discussions during the exercise is required. Quantitative measurements, such as who gave what instructions and when, and the time taken for certain decisions during the exercise would identify bottlenecks in incident response.

In the future, building upon a refined exercise board or manual, abstracting the content, and organizing it into a matrix of tasks for each phase and individual could lead to identifying best practices for incident response in healthcare institutions.

CONCLUSION

This paper proposes an incident response exercise based on system failures in healthcare institutions in Japan from 2021 to 2022. The exercise flow should encompass planning, implementation, and subsequent improvement of the exercise itself. However, it is currently stalled in the planning stage. Next work aims to execute this exercise within healthcare institutions and enhance its overall effectiveness.

In the future, creating incident response manuals through exercises, or developing abstracted incident response matrices, could help in identifying best practices for incident response in healthcare institutions.

REFERENCES

Check Point Research Team. (January 5, 2023) Check Point Research Reports a 38% Increase in 2022 Global Cyberattacks. Check Point Website: https://blog.checkpoint.com/2023/01/05/38-increase-in-2022-global-cyberattacks/.

Davaadorj, Nyambayar. (2018) Fundamental Study on Security Management Framework for Critical Infrastructures based on Safety-II. Ph.D. thesis. Nagoya Institute of Technology.

International Organization for Standardization [ISO]. (2013) ISO22398:2013 Societal security — Guidelines for exercises, Switzerland: ISO.

Kaur, H., Alam, M. A., Jameel, R. (2018). A Proposed Solution and Future Direction for Blockchain-Based Heterogeneous Medicare Data in Cloud Environment. Journal of Medical Systems, 42(8).

Kota, Kawano. (April 28, 2022) Unauthorized access to a hospital in Osaka, Japan. The Asahi Shimbun Website: https://www.asahi.com/articles/ASQ4W71RWQ4WPTIL00J.html.

Kruse, C. S., Frederick, B., Jacobson, T., & Monticone, D. K. (2017). Cybersecurity in healthcare: A systematic review of modern threats and trends. Technological Health Care, 25(1), pp. 1–10. doi: 10.3233/THC-161263

Masahiko, Tsutsui. (June 22, 2021) Downing of the Medical Image Reference System Server (2nd Report). Higashiosaka City Medical Center Website: https://www.higashiosaka-mc.jp/news/notice/20210622_notice.html.

Masako, Fukui. (June 19, 2022) Notice of System Failure due to (Suspected) Unauthorized Access. Kasugai Rehabilitation Hospital Website: https://www.kreh.or.jp/2022/01/19/3837/.

Naruto Yamakami Hosipital. (June 20, 2022) Damage Caused by Cyber Attacks (1st Report). Naruto Yamakami Hospital Website: https://kyujinkai-mc.or.jp/info/20220620/.

Nikkei. (June 19, 2022) Nihon University School of Dentistry Dental Hospital Server infection Temporary suspension of acceptance. NIKKEI Website: https://www.nikkei.com/article/DGXZQOUE196B20Z10C22A1000000/.

Norio, Sonoda. (November 4, 2021) Apology and Notice Regarding System Failure. Fuji Hospital Website: http://www.yuurinkouseikai.or.jp/info/20211104.asp.

Paul, C. Thomas, M. Tim, G. (2012) NIST SP 800–61 Rev.2 Computer Security Incident Handling Guide, U. S.: National Institute of Standards and Technology.

Takeshi, Shimazu. (May 23, 2023) Information Security Incident Investigation Committee Report. Osaka General Medical Center Website: https://www.gh.opho.jp/important/785.html.

Tazawa Iin. (November 1, 2022) Problems with Electronic Medical Records. Tazawa Iin Website: http://shinyoukai.or.jp/tazawa-clinic/news/20221101.html.

Tsukasa, Fukuya. (April 14, 2021) Inability to view electronic medical records KAISEI Hospital, Kagawa, Japan. The Asahi Shimbun Website: https://www.asahi.com/articles/ASP4G3DMZP4FPTLC00F.html.

Yasushi, Sudo. (June 7, 2022) Computer Incident Report. Handa Hospital Website: https://www.handa-hospital.jp/topics/2022/0616/index.html.

Yuri, Atsumi. (December 8, 2022) Kanazawa Nishi Hospital announces damage from unauthorized access; some electronic medical records cannot be viewed. Nikkei Business Publications, Inc. Website: https://xtech.nikkei.com/atcl/nxt/news/18/14283/?i_cid=nbpnxt_sied_blogcard