Human Interaction and Emerging Technologies (IHIET-AI 2024), Vol. 120, 2024, 497–502
https://doi.org/10.54941/ahfe1004602

Recommendations for the Use of Resilience Matrix 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

With cyber-attacks against healthcare institutions on the rise, urgent organizational and technical security measures are required. However, healthcare institutions are currently lagging in their security measures due to their limited budgets for security investment. Therefore, it is important to respond with limited resources and to improve organizational resilience when an incident occurs. This paper would like to identify issues of security measures in healthcare institutions based on reports of actual incidents and provide points for reviewing the status of security measures in your organization. Also, it will discuss the response process for each role when an incident occurs, which should help improve the resilience of the organization and the incident response policy.

Keywords: Cybersecurity, Non-technical countermeasures, BCP, Humancentric perspective, Resilience

INTRODUCTION

According to the annual report of U.S. security vendor Check Point, cyber-attacks worldwide increased by 38% in 2022 compared to 2021. In particular, cyber-attacks targeting healthcare institutions have been on the rise recently, with an average of 1,410 cyber-attacks per organization per week occurring at healthcare institutions in the U.S. alone, an 86% increase from the previous year of 2021 (Figure 1) (Check Point, 2023). It is believed that the reason why cybercriminals attack healthcare institutions is that personal healthcare information is 20 to 50 times more valuable than personal financial information (Kruse, 2017). They may be one factor that makes healthcare institutions targets of cyber-attacks.

Therefore, it is essential to promote security measures in healthcare institutions, but they have been slow in taking organizational and technical countermeasures for cybersecurity due to their history of integration into networks from previously independent systems and small budgets for security in IT capital investment (Kruse, 2017). Thus, organizations need to secure appropriate budgets for IT investments and at the same time take measures against cyber-attacks that can be implemented within a limited budget. In addition, the report stated that they are hesitant to disclose some of the findings of security incidents involving vulnerabilities that have occurred at healthcare institutions because they reveal vulnerabilities within the industry and suggest the possibility of further cyber-attacks (Conn, 2016).

However, NIST SP800-61, which is also a guideline for computer incident response, states that it is important to prepare for the next security incident by learning lessons from past security incidents. In this paper, after organizing the issues of security incidents that have occurred in the past in healthcare institutions in terms of PPT (People, Process, and Technology), deepen the discussion in terms of Process, which is believed to be addressed with existing resources.

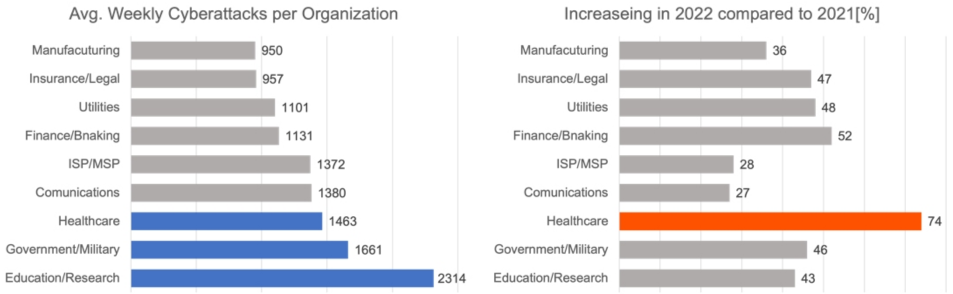


Figure 1: Avg. weekly cyber attacks per organization (left figure) and increasing rate in 2022 compared to 2021 per organization (right figure) (Check Point, 2023).

Method

The PPT (People, Process, Technology) framework, also known as the Golden Triangle, is used to examine security measures and represents three elements that inevitably interact (Caramancion, 2020). The reports of ransomware attacks on healthcare institutions in Japan in 2021 and 2022 will organize the responses to incidents in each role of healthcare institutions and recommend ways to improve them. The following two hospitals are examples of incidents to be referred to.

Case A: Handa Hospital (2021) (Morii, 2022)

- In the early hours of October 31, 2021, the hospital system was infected with Lockbit2.0 ransomware
- The vulnerability of VPN equipment was exploited to gain entry
- BCP for earthquake disasters was activated and the incident was treated as a disaster from the beginning
- During this time, the hospital stopped accepting new patients
- On January 4, 2022, normal healthcare services were resumed after the system was restored.

Case B: Osaka General Medical Center (2022) (Inomata, 2023)

- In the early morning of October 31, 2022, the hospital system was infected by Elbie ransomware

- The intrusion occurred through a VPN device of a food service vendor adjacent to the hospital
- The BCP task force established to discuss restoration
- Complete restoration, including surgical operations, was completed on January 16, 2023.

RESULTS

In both cases A and B, when an incident occurred, BCP (Business Continuity Plan) for a large-scale natural disaster was used to ensure business continuity and recovery. In each report, these causes are summarized in Table 1 from the perspective of PPT. After that, I would like to discuss each of the issues in cases A and B in more detail.

Table 1. Security incident issues with the PPT framework.

PPT	Security incident issues
People	• Insufficient security personnel and knowledge (A, B) • Lack of security awareness, knowledge, experience, and preparation for incident response at IT system vendors (A, B)
Process	• Password policy is not in place (A, B) • Insufficient information collection system for vulnerability information, etc (A, B) • Policies and rules for external connections were not in place (A) • The boundary of responsibility at the time of contract was unclear (A, B)
Technology	• Weak passwords (A, B) • Vulnerabilities in equipment and systems were not addressed (A, B) • Anti-virus products have not been installed (A) • Standard port (3389) is allowed for RDP communication at all times (B)

ISSUES AND RECOMMENDATIONS IN PEOPLE

It is emphasized that no matter how technology is considered human-independent, individuals will ultimately come into contact with technology at various points (Furnell, 2012). In both cases, a lack of security personnel was positioned as the cause of the incidents, but in healthcare institutions, the priority is to serve patients, and it is difficult to secure personnel for IT personnel as well as security, even for economic reasons (Kruse, 2017). In addition, while the security incidents were due to technical vulnerabilities, there are also security incidents based on human factors (phishing emails, social engineering) (Pollini, 2022). While it is important to secure human resources, it is also important for healthcare institutions to provide security education to personnel such as doctors and nurses, which is reported to be effective to a certain extent (Nifakos, 2021).

ISSUES AND RECOMMENDATIONS IN THE PROCESS

The reasons for the vulnerability were the lack of an information collection system and patch application process for urgent vulnerabilities, as well as the lack of a password policy and its weaknesses. In particular, vulnerability responses are often not covered by the maintenance contracts with IT system vendors, which do not cover the provision of vulnerability information or version upgrades. Therefore, it is important to establish a policy for contracts with IT system vendors and the division of roles. In the latter part, Challenge & Discussion section will further discuss what kind of response process is required before and after an incident for each role of the person in charge by applying the existing framework.

ISSUES AND RECOMMENDATIONS IN THE TECHNOLOGY

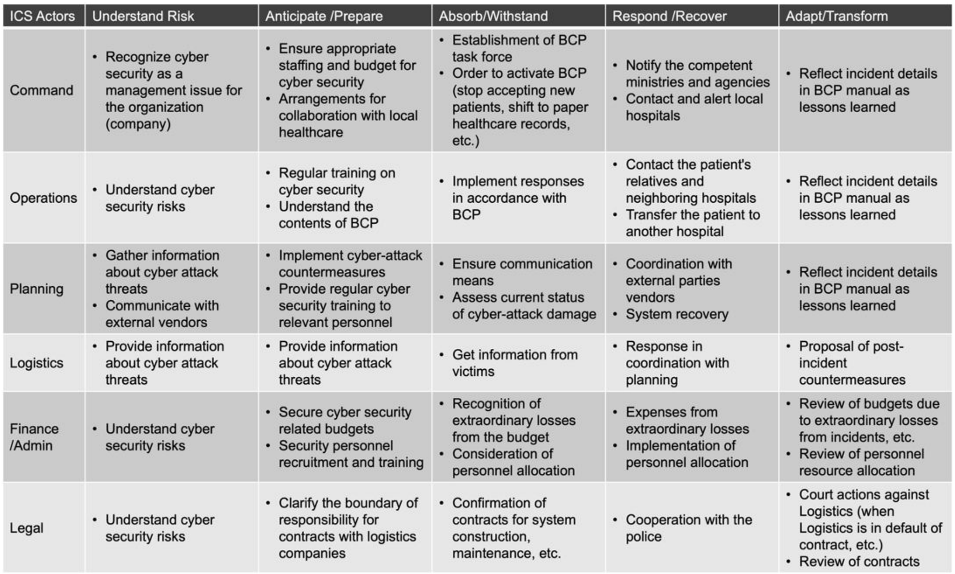
There were issues of equipment and system vulnerabilities that had not been addressed and anti-virus systems that had not yet been put into operation. In the case of general corporate IT systems, OS updates, and anti-virus installations would be performed, but in both cases, it was not possible to update equipment or run anti-virus due to the compatibility of the electronic healthcare record system.

Although the entire system would need to be modified to maintain system compatibility, budgetary and other issues may prevent such modifications from taking place. This response to the emphasis on system availability can be seen as similar in some respects to Operational Technology (OT) in the manufacturing industry (Uchenna, 2017). If the availability of legacy systems is to be emphasized as in factories, it would be useful as a countermeasure to consider permission list-type endpoint security measures that only allow application operation for specific purposes, rather than those that stop operation such as anti-virus.

CHALLENGE & DISCUSSION

In both cases, BCP for natural disasters was useful. It is also obvious that cybersecurity has caused as much damage as disasters in recent years, and BCP is considered to have had a certain level of effectiveness, especially in the healthcare field where human lives are at stake.

To consider the process of triggering BCP, the roles of actors in the incident response phase are summarized using the Incident Command System (ICS) used in firefighting and other fields. In a normal ICS, the five actors are Command, Operations, Planning, Logistics, Finance, and Administration (Broder, 2012). By the way, the lack of a system for communication and maintenance by the IT system vendor regarding vulnerability information that is commonly disclosed in both cases A and B is also mentioned as a cause of security incidents. There are many legal elements regarding contracts, and it is also important to confirm appropriate contracts at the time of IT system implementation through legal documents. As for case B, there was also an intrusion from the network from a food service vendor, and it is necessary to pay attention to the security of the supply chain again. For this reason, this study will focus on clarifying the boundary of responsibility in the event of a security incident involving the supply chain. Therefore, the role of legal affairs will be added to the ICS actors, and the resilience matrix proposed in Horizon 2020 (SmartResilience, 2019) will be used to organize the response of each ICS actor in normal times and emergencies. Although the original matrix is organized within a broad framework of systems, organizations, and information, it does not organize the response that is incorporated into each organization's role. Then incorporating the actions of each response phase into the roles of each organization is believed to provide a more concrete indicator for incident response. Figure 2 shows an incident matrix that organizes the processes that the 5 actors of ICS and the legal should respond to during each incident phase based on cases A and B. Also, logistics in this matrix for healthcare institutions can be replaced with IT system vendors for a better understanding.



ICS Actors	Understand Risk	Anticipate /Prepare	Absorb/Withstand	Respond /Recover	Adapt/Transform
Command	• Recognize cyber security as a management issue for the organization (company)	• Ensure appropriate staffing and budget for cyber security • Arrangements for collaboration with local healthcare	• Establishment of BCP task force • Order to activate BCP (stop accepting new patients, shift to paper healthcare records, etc.)	• Notify the competent ministries and agencies • Contact and alert local hospitals	• Reflect incident details in BCP manual as lessons learned
Operations	• Understand cyber security risks	• Regular training on cyber security • Understand the contents of BCP	• Implement responses in accordance with BCP	• Contact the patient's relatives and neighboring hospitals • Transfer the patient to another hospital	• Reflect incident details in BCP manual as lessons learned
Planning	• Gather information about cyber attack threats • Communicate with external vendors	• Implement cyber-attack countermeasures • Provide regular cyber security training to relevant personnel	• Ensure communication means • Assess current status of cyber-attack damage	• Coordination with external parties vendors • System recovery	• Reflect incident details in BCP manual as lessons learned
Logistics	• Provide information about cyber attack threats	• Provide information about cyber attack threats	• Get information from victims	• Response in coordination with planning	• Proposal of post-incident countermeasures
Finance /Admin	• Understand cyber security risks	• Secure cyber security related budgets • Security personnel recruitment and training	• Recognition of extraordinary losses from the budget • Consideration of personnel allocation	• Expenses from extraordinary losses • Implementation of personnel allocation	• Review of budgets due to extraordinary losses from incidents, etc. • Review of personnel resource allocation
Legal	• Understand cyber security risks	• Clarify the boundary of responsibility for contracts with logistics companies	• Confirmation of contracts for system construction, maintenance, etc.	• Cooperation with the police	• Court actions against Logistics (when Logistics is in default of contract, etc.) • Review of contracts

Figure 2: Incident matrix with ICS actors and legal.

The response process for all parties involved was organized based on the ICS and Horizon 2020 resilience matrix. Of special note for healthcare institutions is crisis communication, such as the transfer of patients to and from local healthcare institutions at the time of an incident. It is important to ensure that these communication systems and means are in place in advance of an incident during the preparation phase. In addition, these processes need to be reviewed through the PDCA cycle to ensure that there are no omissions in the response through incident response training. Moreover, it is important to utilize the OODA loop (Observe, Orient, Decide, Act) instead of the usual PDCA cycle during emergencies.

In the future, training and demonstration experiments will improve the incident matrix and deepen the consideration of triggers for following the OODA loop during incident response.

CONCLUSION

This paper reviewed incident cases of Japanese healthcare institutions from the perspective of PPT and provided recommendations for each issue. This paper tried to apply existing frameworks to the response to incidents, particularly in process, and makes recommendations for enhancing organizational resilience, depending on the role of the person in charge of the field. As noted earlier, it is important to learn from the lessons of security incidents that do occur. This research expects that the lessons learned from the incidents that occurred and the resilience matrix discussed will serve as an indicator for improving the resilience of each organization. In addition, the resilience matrix should be improved by creating training based on it and then implementing the training. The creation of applicable training and improvement of the resilience matrix will be a future issue.

REFERENCES

Broder, J. F., & Tucker, E. (2012). "Emergency Management – A Brief Introduction." In J. F. Broder & E. Tucker (Eds.), Risk Analysis and the Security Survey (Fourth Edition). pp. 101–112. Butterworth-Heinemann. ISBN 9780123822338. https://doi.org/10.1016/B978-0-12-382233-8.00012-1.

Caramancion, K. M. (2020). An Exploration of Disinformation as a Cybersecurity Threat. 440–444. 10.1109/ICICT50521.2020.00076.

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/

Conn, Joseph. (April 16, 2016). Federal task force takes on healthcare cybersecurity. Modern Healthcare Website: https://www.modernhealthcare.com/article/20160416/MAGAZINE/304169890/federal-task-force-takes-on-healthcare-cybersecurity

Furnell, S., Clarke, N. (2012). Power to the people? The evolving recognition of human aspects of security. Computers & Security. Volume 31, Issue 8, pp. 983–988. https://doi.org/10.1016/j.cose.2012.08.004.

Inomata, Atsuo. (May 23, 2023). Information Security Incident Investigation Committee Report. Osaka General Medical Center Website: https://www.gh.opho.jp/pdf/report_v01.pdf

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.

Morii, Masakatsu. (Jun 7, 2022). Computer Incident Report. Handa Hospital Website: https://www.handa-hospital.jp/topics/2022/0616/report_01.pdf

Nifakos, S., Chandramouli, K., Nikolaou, C. K., Papachristou, P., Koch, S., Panaousis, E., & Bonacina, S. (2021). "Influence of Human Factors on Cyber Security within Healthcare Organisations: A Systematic Review." Sensors, 21(15), 5119. https://doi.org/10.3390/s21155119.

Pollini, A., Callari, T. C., Tedeschi, A., et al. (2022). "Leveraging human factors in cybersecurity: an integrated methodological approach." Cognitive Technology Work, 24, 371–390. https://doi.org/10.1007/s10111-021-00683-y.

SmartResilience. (2019). Smart Resilience Indicators for Smart Critical Infrastructures. CORDIS Website: https://cordis.europa.eu/project/id/700621

Uchenna, P., Ani, D., He, H. (Mary), & Tiwari, A. (2017). "Review of cybersecurity issues in industrial critical infrastructure: manufacturing in perspective." Journal of Cyber Security Technology, 1(1), 32–74. DOI: 10.1080/23742917.2016.1252211.