Human-Centered Design and User Experience, Vol. 114, 2023, 331–337
https://doi.org/10.54941/ahfe1004251

Analysis of Cybersecurity Risk for Factory Systems

Hiroshi Sasaki[1,2], Kenji Watanabe[1], and Ichiro Koshijima[2]

[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

As the digitization of factory systems progresses and the number of digital connections between factories increases, cybersecurity risks throughout the supply chain also increase. In fact, there have been many cases where factories have stopped due to damage from ransomware. For large enterprises, it is possible to secure the budget and personnel for cybersecurity, including outsourcing. However, almost all small and mediums enterprises (SMEs) are facing with the difficulties to secure them. In this paper, we used a web diagnostic tool for simple risk assessment of factory systems using the checklist for understanding the rough risk posture in the appendix of "The Cyber/Physical Security Framework for Factory Systems" formulated by the Ministry of Economy, Trade and Industry in November 2022. After analysing the survey results from 225 factory sites and interviews from some respondents, we elicited the common challenges for promoting security measures for the factory systems.

Keywords: Operational technology (OT) security, Risk analysis of cybersecurity for factory system, Risk assessment tool for factory system

INTRODUCTION

As the digitization of operational technology (OT) in factories has caused more susceptible to cyberattacks in recent years. Have been increasing the cases where cyberattacks targeting information systems affected factories. Especially in the last few years, several factories shut down due to malware infection of information systems related to production. For example, a cyberattack on an automotive parts supplier in Japan caused that major automobile manufacturer relying on the supplier shut down all the domestic factories for a day. It is a symbolic example showing a supply chain with strengthened digital connections induces that a cyberattack on a member of the chain can affect not only the company itself but also its business partner.

In response to the situation, the importance of cybersecurity measures has recently come to be recognized even in factories. However, the organization responsible for cybersecurity measures at factories is not clear, and there are no personnel with knowledge.

In addition, an increasing demand for carbon-neutral business happens globally, and factories are moving to visualize CO_2 emissions in production and share it in the supply chain. As the number of data connections

between factories increases in this way, factory cybersecurity measures become an "etiquette" for business participation. This is because the presence of vulnerable players in the supply chain will cause damage to other businesses.

Despite the increasing importance of cyber security in factory systems, many companies continue to be unable to say that their measures are sufficient. The reason for this is that the degree of risk of the factory system is not known and it is not possible to judge how much investment should be made.

This research aims to take the first step in promoting cybersecurity measures for factory systems by visualizing the security risks associated with the current state of factory systems and presenting a simple risk assessment method that can be used to secure budgets and human resources. purpose. In this paper, based on the information collected by the web diagnostic tool using this risk assessment method, common issues in cybersecurity measures for factory systems were derived.

PRIOR RESEARCH

The following standard and framework are known as prior research on cybersecurity risk assessment for factory systems.

The most well-known international standards are ISA/IEC 62443 series, mainly focused on the security of industrial control systems. IEC 62443-2-1 is used for cybersecurity management system for Industrial Automation and Control System (IACS) (IEC 2008). IEC 62443-3-3 which has 128 Items is often used by the requirement of OT system procurement along its security level in plant automation industry (IEC 2013). Many prior efforts are known for utilizing the standard (Weiss, 2015) (Wylie et al., 2015).

The NIST Cybersecurity Framework (CSF) is also a very popular and voluntary framework to help organizations manage and reduce cybersecurity risk (NIST, 2014). The framework provides a set of guidelines and best practices (108 items) that organizations can use to assess their current cybersecurity posture, identify gaps and weaknesses, and develop a plan for improving cybersecurity. Many prior efforts on NIST CSF were known (Barnes et al., 2014) (Lightman et al., 2014).

The Cybersecurity Evaluation Tool (CSET) is a software tool to help organizations assess and improve their cybersecurity posture (CISA 2023). CSET is specifically designed for industrial control systems, used in CI sectors. It provides recommendations for improving the organization's cybersecurity program, based on industry best practices and standards such as NIST CSF and ISA/IEC 62443.

CSET is designed to be flexible and customizable. It can be used by organizations of all sizes and types. The tool is free to download and use and is regularly updated to reflect changes in cybersecurity threats and best practices. some prior efforts on CSET were known (Mumm, 2012) (Chipley et al., 2014).

These previous studies are already very useful for organizations that have established management system and secure budgets in factory systems. However, it is too time consuming and difficult for SMEs to utilize them because

these guidelines have over 100 requirements and need specialized people who understand both cybersecurity and industrial control systems well.

METHOD

In this study, we utilized the checklist for posture assessment of the appendix E of the "The Cyber/Physical Security Framework for Factory Systems (draft) Version 1.0" as the basic tool (Table 1) (METI, 2022). The reason is that the burden of implementing 32 items is relatively low. In addition to the easy-to-understand three basic classifications of "people", "processes", and "technology". In addition, it also mentions the recent security issue of "supply chain management of factory assets (FA SCM)". The four categories make it easy to use to visualize risks rather than the previous works.

For the 32 items in this checklist, we can input 6 options (Table 2) shown in the guidelines and score the risks (20% to 100%) of 4 categories and overall results. Developed web diagnostic tool. This tool is designed to visualize the high-level risk posture of factory systems by scoring (20% to 100%) the degree of achievement of each requirement. A risk-scoring methodology is presented in the other paper (under peer review).

By releasing the web tool on the public, we obtained the input results from 225 sites (the number of factory bases to be diagnosed) from June 2022 to July 2023. The results are aggregated and utilized for risk analysis of the factory system. In addition, for several factory sites, detailed interviews were conducted regarding the input content. We have identified common challenges and issues in the four categories.

Table 2. Selection items for checklist (METI, 2022).

Selection Item
Not applicable
Not Implemented
Partially Implemented
Implemented
Implemented, control procedures are documented and automated, and measures are periodically reviewed'
Implemented, control procedures are documented and automated, and reviewed as needed

RESULT

As a web tool survey result, more than 80% of factory sites found it inadequate to mitigate cybersecurity risks. To see more details of the situation, the survey result for 225 sites obtained is shown (Fig. 1). Firstly, more than 50% of the responses for all items other than physical security item (3-4) were "Not implemented" or "Partially implemented", indicating that overall measures are inadequate.

From the follow-up interviews of over 10 factory sites, we summarized some common results in each category below:

Table 1. Selection item for checklist (METI, 2022).

Category	No	Item
People	1-1	The decision maker (factory manager, company manager, etc.) or management is aware of the need for security of factory systems, is in a position to obtain cooperation in terms of sufficient budget and personnel allocation.
	1-2	Cooperation and linkage arrangements are in place between the information system division, production related divisions, and other relevant divisions and departments to ensure the security of factory systems.
	1-3	The factory system security review organization and the person in charge are prepared, and the responsibilities and business contents are clarified.
	1-4	A person in charge in the event of a factory security accident is prepared, and responsibilities and business contents are clarified, accident is prepared, and responsibilities and business contents are clarified.
	1-5	Provide on-site training such as receiving regular information and holding study sessions on trends in threats related to factory security.
Process	2-1	The risks to the business in the event of a system breach or outage are considered.
	2-2	Dedicated security policies in the factory system are specified and recognized.
	2-3	E-mail and Internet access from the factory system is prohibited by the policy.
	2-4	Responsible person's response to the occurrence of security anomalies in the factory system is clarified.
	2-5	On-site workers understand and are trained on how to respond to security anomalies in factory systems.
	2-6	A ledger of devices (servers, client terminals, network equipment, facilities, etc.) connected to the factory network is created, including the use of information asset detection tools, and a system configuration diagram is created.
	2-7	A wireless LAN is installed in the factory, a system is in place to create a ledger of devices authorized to connect to the network and reject unauthorized devices.
	2-8	Periodic vulnerability assessments and penetration tests are conducted to identify attack methods and vulnerabilities that can be used to successfully infiltrate the system.
	2-9	Restrictions on the use and bringing of external storage media (USB memory sticks, flash cards) and portal media into the plant.
	2-10	There are password rules for systems in the factory, including password strength and expiration dates. (Excluding terminals such as display units that require emergency response related to safety).
	2-11	Old accounts (e.g., retirees, transferees, etc.) that are not in use with access rights to systems in the plant are deleted.
	2-12	For connected devices in the factory network, there is a procedure to verify in advance that they are not infected with viruses.
	2-13	Backups are made with the assumption of complete restoration of system functions, and tests of restoration from backup data are conducted periodically. In addition, the procedure is clarified.
Technology	3-1	Anti-virus software or application white lists are installed on terminals where anti-virus measures can be installed, and some alternative measures (e.g., USB-type anti-virus) are installed on terminals where installation is not possible.
	3-2	Security patches are applied to the application/operating system (OS). Or alternative measures are in place.
	3-3	Services and applications using the control terminal operating system are kept to the minimum necessary, and unused services and ports are stopped or disabled.
	3-4	Sufficient measures, such as level classification, are taken for physical access to important factory equipment. Or alternative operational measures are in place such as access control and escort of relevant personnel to outside visitors.
	3-5	Within the factory network, network segment management is conducted according to security level (e.g., VLANs).
	3-6	Protective measures such as authentication (e.g., twofactor authentication) and network intrusion protection are taken when external Internet access is possible for the purpose of remote maintenance of factory systems, etc
	3-7	A network detection/protection system is in place to identify suspicious communications on the factory network (including the boundary with the information system)
	3-8	Event logs of logins, operation histories, etc. of the factory's internal systems are being collected. Those logs are periodically analyzed or stored for the required number of days.
Supply chain risk management for factory asset	4-1	A liaison and coordination system has been established with control system vendors and construction companies to respond to security incidents in factory systems.
	4-2	Conducting security training for subcontractors involved in factory system maintenance, etc.
	4-3	A system for communication and coordination with control system vendors/builders is in place to ensure that information is shared promptly when security vulnerabilities related to delivered factory systems are discovered.
	4-4	Aware of threats to factory systems in the supply chain (subcontractors, production subsidiaries, etc.), the degree of impact, and the status of response (e.g., implementation of audits, etc.)
	4-5	Has a process to determine whether the factory system equipment to be delivered meets certain security standards, and an acceptance inspection.
	4-6	Security requirements are clarified in the design specification requirements for new system implementation.

"People": No awareness of executives, stakeholders, no governance and organization, no collaboration between IT and factory organizations, no educational contents for mitigating the risk in the factory.

"Process": No risk assessment, no assets management for factory systems, no security policy and rule, no procedure and back up asset for incident response.

"Technology": Some countermeasures are installed such as firewall, endpoint security solutions, but not managed well, no network segmentation, no log management, well done for physical security.

"FA SCM": No management for system integrators and asset vendors, no procedures for mitigating the cybersecurity risk for procurement of factory assets.

CHALLENGE AND DISCUSSION

From the survey results and interviews, we found out "People" factor is the root obstacle because no dedicated people for cybersecurity in a factory organization causes the insufficient risk mitigation of the other three categories. If a factory site needs the people in charge of cybersecurity, it is essential for the executives to commit the investment for human resources.

Table 3. Checklist items by subcategory.

Category	Subcategory	Checklist Item
People	Governance	1-1, 1-2, 1-3, 1-4
	Operator Awareness	1-5
Process	Periodic Assessment	2-1, 2-8
	Incident Response	2-4, 2-5, 2-13
	Asset Management	2-6, 2-7
	Rule Making/Update	2-2, 2-3, 2-9, 2-10, 2-11, 2-12
Technology	Endpoint Protection	3-1, 3-2, 3-3
	Physical Security	3-4
	Network security	3-5, 3-6, 3-7
	Log Management	3-8
Supply chain risk management for factory asset	Supplier Management	4-1, 4-2, 4-3, 4-4
	Procurement Process Management	4-5, 4-6

To analyse the results more deeply, we grouped the items and organized them into 12 subcategories (Table 3). For example, the "Governance" subcategory is a collection of items related to the organizational structure and division of roles indicated by checklist items 1-1, 1-2, 1-3, and 1-4. For each subcategory, we calculated the ratio of "insufficient measures" ("Not implemented" + "Partially implemented") (Table 4). As a result, "Periodic assessment", "Incident response", "Supplier management", and "Procurement Process Management" exceed 70%, and it is considered that these measures have not progressed. All of four subcategories require cross-organizational activities, and it is considered that measures tend to be delayed due to the insufficient resources of the cybersecurity organization on the factory site.

Table 4. Ratio of insufficient measures of each subcategory.

Category	Subcategory	"Not Implemented" + "Partially Implemented" (%)
People	Governance	62.3
	Operator Awareness	64.0
Processs	Periodic Assessment	75.6
	Incident Response	71.9
	Asset Management	56.0
	Rule Making/Update	59.3
Technology	Endpoint Protection	62.2
	Physical Security	46.7
	Network Security	61.2
	Log Management	69.3
Supply chain risk management for factory asset	Supplier Management	71.9
	Procurement Process Management	74.2

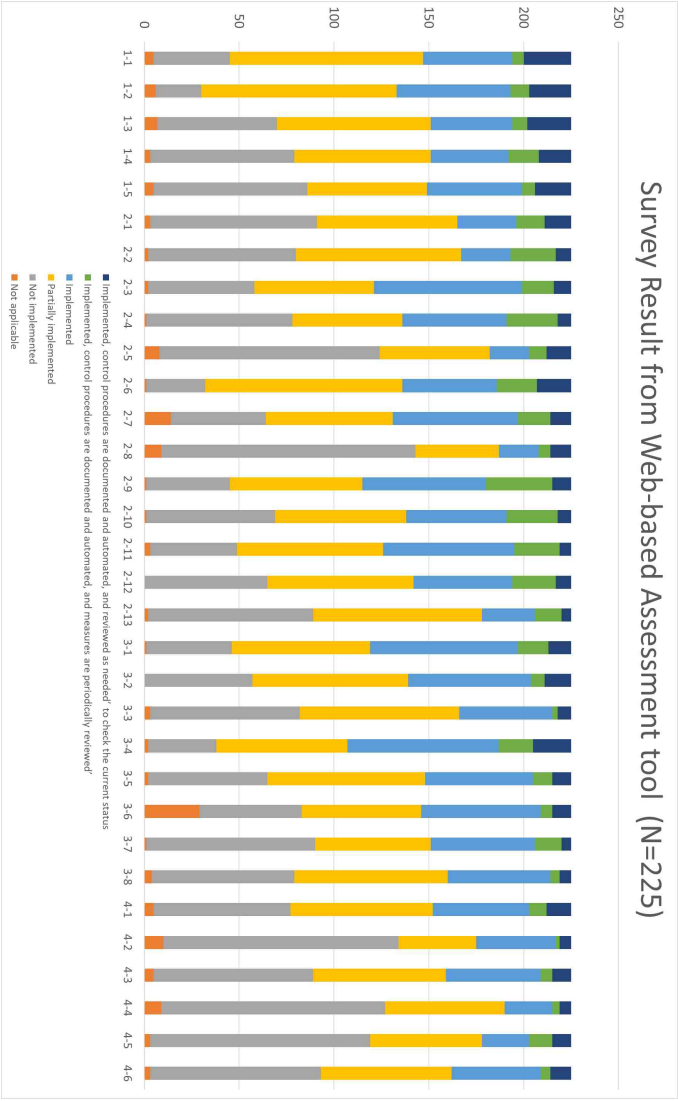

Figure 1: Survey result from web-based assessment tool.

CONCLUSION

In this study, to understand the current state of security risks in factory systems, we used the checklist of Japanese government guidelines and conducted a web survey of factory systems from 225 factory sites. We found out more than 50% of the responses for all items other than physical security item are insufficient, indicating that overall measures are inadequate. Some common results derived from the follow-up interviews shows the "People" factor is the root obstacle of the insufficient measures. It is reinforced by the deeper analysis which shows top four insufficient subcategories (over 70%) need cross-organizational activities.

As future research topics, we will examine methods to easily proceed with risk assessment and develop a standard approach and specific measures for each subcategory to reduce security risks in factory systems.

ACKNOWLEDGEMENTS

This research was supported by Fortinet Japan G.K. to co-work web-based survey and respondent interviews. Authors would like to thank the peer reviewers for their valuable comments for improving the quality of the manuscript.

REFERENCES

Barnes, J. H., Nichols, E. (2014). NIST Cybersecurity Framework: A Tool for Critical Infrastructure Protection. National Institute of Standards and Technology.

Chipley, M., Ogle, S. (2014). Assessing Cybersecurity Risks in Industrial Control Systems: The Cybersecurity Evaluation Tool. INL/EXT-14-32936.

CISA. (2023). The Cybersecurity Evaluation Tool (CSET) v11.5: https://www.cisa.gov/downloading-and-installing-cset https://github.com/cisagov/cset

IEC. (2009). Security for industrial automation and control systems - Part 2-1: Security Program Requirements for IACS asset owner (IEC/ISA 62443-2-1:2009). Geneva, Switzerland: International Electrotechnical Commission.

IEC. (2013). Security for industrial automation and control systems - Part 3-3: System security requirements and security levels (IEC/ISA 62443-3-3:2013). Geneva, Switzerland: International Electrotechnical Commission.

Lightman, S., Healey, J. (2014). The NIST Cybersecurity Framework: A Primer for Critical Infrastructure Owners and Operators. Atlantic Council.

Mumm, K. L., Roxey, T. (2012). Cyber Security Evaluation Tool for Control Systems. Idaho National Laboratory.

NIST. (2014). Framework for improving critical infrastructure cybersecurity (NIST CSF). Gaithersburg, MD: National Institute of Standards and Technology.

METI., Study Group for Industrial Cybersecurity Working Group 1 (Systems, Technologies and Standardization) Factory sub-working group. (2022). The Cyber/Physical Security Framework for Factory Systems (draft) Version 1.0: https://public-comment.e-gov.go.jp/servlet/PcmFileDownload?seqNo =0000236565

Weiss, J. (2015). A Framework for ICS Cybersecurity: ISA/IEC 62443. Control Engineering Practice, 46, 82–93.

Wylie, D. O'Brien, L. (2015). A Comprehensive Approach to Industrial Control Systems Cybersecurity: ISA/IEC 62443. Journal of Cyber Security and Mobility, 3(3), 213–237.