Human Factors in Cybersecurity, Vol. 127, 2024, 219–224
https://doi.org/10.54941/ahfe1004781

Development of Approach for Improving Cybersecurity Governance 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 digitization of factory systems progresses, with mutual digital connections among them, cybersecurity risks throughout the supply chain also increase. In fact, there have been many cyber incidents where factories have stopped due to damage from ransomware. While large companies can allocate budget and personnel for cybersecurity, including outsourcing, almost all small and medium enterprises (SMEs) face difficulties in securing themselves. In this paper, we focus on improving cybersecurity governance for factory systems because our previous research revealed that it is the most critical challenge for SMEs in reducing cybersecurity risk. We propose an easy approach to address this challenge. The first step involves conducting a workshop to analyze the cybersecurity risk of factory systems, following the Consequence-driven, Cyber-informed, Engineering (CCE) framework (Bochman, 2021). To mitigate risks identified during the workshop, the next step is to develop a reference governance architecture based on the COBIT 5 concept for factory cybersecurity, tailored to roles in both normal and emergency states. This approach enhances insufficient cybersecurity governance for factory systems in SMEs and serves as a crucial initial step in mitigating the overall cybersecurity risk of factory systems.

Keywords: Operational technology (OT) security, Cybersecurity governance for factory systems, COBIT 5, Consequence-driven, Cyber-informed engineering (CCE)

INTRODUCTION

As the digitization of operational technology (OT) in factories has increased susceptibility to cyberattacks in recent years, there have been numerous cyber incidents where factories stopped due to damage from ransomware. Notably, in the last few years, several factories shut down due to ransomware infections in information systems related to production. For instance, a cyberattack on an automotive parts supplier in Japan led to the major automobile manufacturer relying on that supplier shutting down all domestic factories for a day. This symbolic example highlights how a supply chain with strengthened digital connections can be affected by a cyberattack on any member, impacting not only the company itself but also its business partners.

In response to this situation, the importance of cybersecurity measures has recently been recognized even in factories. However, the organization

responsible for cybersecurity measures within factories remains unclear, and there is a lack of personnel with the necessary knowledge. Despite the increasing importance of cybersecurity in factory systems, many companies believe their current measures are sufficient. The challenge lies in assessing the degree of risk associated with factory systems and determining the appropriate level of investment.

This research aims to improve the cybersecurity governance for factory systems in SMEs because our previous research identified the "People" factor as the root cause of insufficient readiness.

PREVIOUS WORK

In previous work, we developed an easier risk assessment tool consisting of only 32 items (GitHub, 2023). This tool is based on Japanese government guidelines for factory systems (METI, 2022). According to the results of a web tool survey conducted across 225 factory sites, more than 80% of SMBs found it inadequate for mitigating cybersecurity risks (Sasaki et al., 2023). We categorized these cybersecurity risks into four factors: "People," "Process," "Technology," and supply chain management of assets in the factory automation system (FA SCM). Follow-up interviews revealed that the "People" factor, which includes governance and awareness, is the root obstacle to implementing sufficient measures. Consequently, we aim to clarify how to improve the "People" factor for SMEs. To achieve this, we must address two common challenges identified during our interviews, as outlined in the subcategories below (Table 1):

1. Periodic Assessment: Lack of risk assessment in factory systems, hindering a common understanding of the risk posture among stakeholders (including executives, IT personnel, and factory staff).
2. Governance: Absence of a clear governance organizational structure."

Table 1. Checklist items by subcategory (Sasaki et al., 2023).

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

This research aims to enhance the cybersecurity governance of factory systems in SMEs, addressing the critical issue of insufficient readiness.

BASIC CONCEPT OF APPROACH

To improve the cybersecurity governance of factory systems, we need to raise awareness among factory personnel. The typical approach involves IT professionals disseminating common cybersecurity guidelines and rules to all factory staff at each site. However, factory workers often disregard these measures because they don't fully understand the necessity behind actions like managing USB memory drives or patching outdated terminals. Our approach aims to address this gap. We have initiated a mindset shift among factory employees by creating cybersecurity incident scenarios to enhance risk awareness.

In pursuit of this goal, we developed an "OT risk workshop" specifically for this purpose. For its development, we drew inspiration from the CCE concept. CCE is a methodology focused on securing critical infrastructure systems at the national level. Originating from the Idaho National Laboratory, CCE operates under the assumption that if a skilled and determined adversary targets a critical infrastructure system, that network will be penetrated. The "think like the adversary" approach provides critical infrastructure owners and operators with a four-phase process to safeguard their essential operations. The following graphic illustrate each of the four phases of the CCE Methodology (Fig. 1). Our primary focus lies on "Phase 1: Consequence Prioritization" within these four phases. This phase is particularly accessible for factory personnel with limited cybersecurity awareness because it directly aligns with their business objectives, including production continuity, safety, quality, environmental considerations, cost management, and timely delivery.

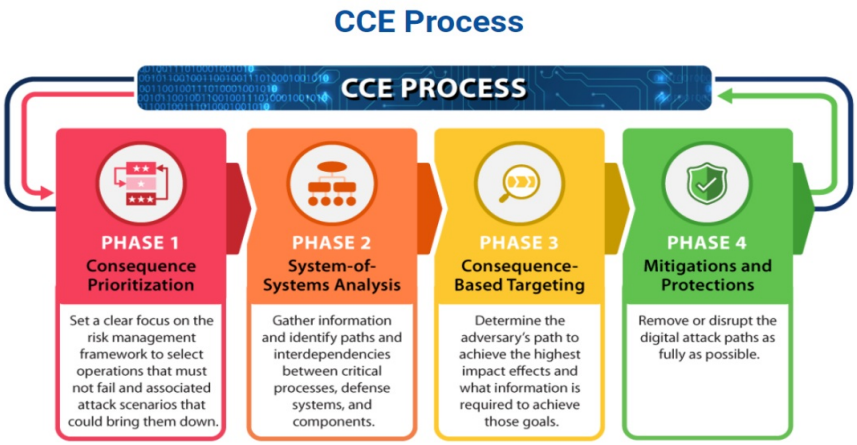


Figure 1: CCE process (INL, 2023).

To address the second challenge, which pertains to the lack of a governance organizational structure, we applied the COBIT5 governance framework for enterprise IT (ISACA, 2012) to the management system of factory systems. One of the notable features of COBIT5 is its clear separation between governance and management. We adapted this concept to the context of factory systems and established a reference architecture for organizing roles in both normal and emergency states.

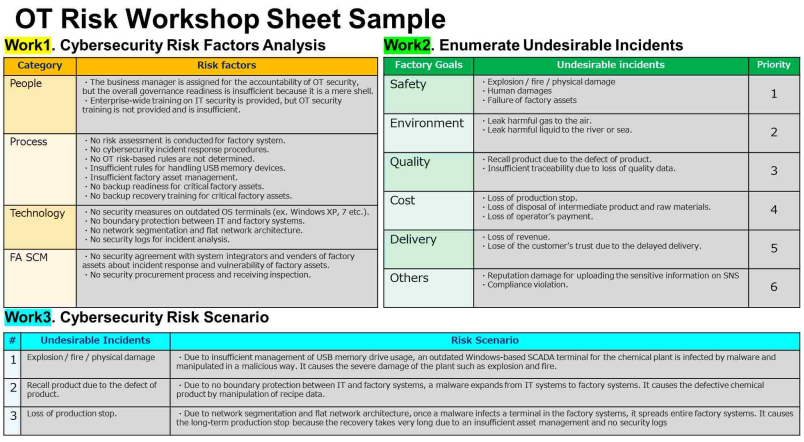
OT RISK WORKSHOP

We developed an OT risk workshop that provides factory personnel with the opportunity to recognize the connection between cybersecurity and operational technology (OT) risks, as well as their business goals. Organizing this workshop is essential, and IT professionals should take the lead due to their cybersecurity expertise. Ideally, more than 10 factory employees from production management, production engineering, and the factory IT team should participate in managing the factory network. We conducted this workshop at several factory sites to refine our approach.

The workshop comprises three group activities, each lasting 30 minutes for group discussions. During these sessions, the group leader shares the results for 10 minutes. Here's an overview of the workshop components:

1. **Cybersecurity Risk Factors Analysis:** In the first activity, participants analyze cybersecurity risk factors across four categories based on the Japanese guidelines' checklists. Referring to the comprehensive checklist of 32 items is recommended.
2. **Enumerating Undesirable Incidents:** The second activity involves enumerating undesirable incidents related to factory goals, such as safety, environment, quality, cost, and delivery. Importantly, participants should not consider cybersecurity during this step. Often, factory personnel tend to focus on cybersecurity incidents without fully understanding how they relate to undesirable outcomes. Therefore, they should purely consider the undesirable incidents.
3. **Cybersecurity Risk Scenario:** Finally, participants consider the top three cybersecurity risk scenarios, prioritizing incidents. They combine the results from the first and second activities to build these scenarios. IT professionals can assist in creating them, as specialized knowledge of cybersecurity may be necessary.

This workshop aims to enhance awareness and preparedness for cybersecurity risks in factory systems. The sample result is shown for the reference (Fig. 2).



OT Risk Workshop Sheet Sample

Work1. Cybersecurity Risk Factors Analysis

Category	Risk factors
People	· The business manager is assigned for the accountability of OT security, but the overall governance readiness is insufficient because it is a mere shell. · Enterprise-wide training on IT security is provided, but OT security training is not provided and is insufficient.
Process	· No risk assessment is conducted for factory system. · No cybersecurity incident response procedures. · No OT risk-based rules are not determined. · Insufficient rules for handling USB memory devices. · Insufficient factory asset management. · No backup readiness for critical factory assets. · No backup recovery training for critical factory assets.
Technology	· No security measures on outdated OS terminals (ex. Windows XP, 7 etc.). · No boundary protection between IT and factory systems. · No network segmentation and flat network architecture. · No security logs for incident analysis.
FA SCM	· No security agreement with system integrators and venders of factory assets about incident response and vulnerability of factory assets. · No security procurement process and receiving inspection.

Work2. Enumerate Undesirable Incidents

Factory Goals	Undesirable incidents	Priority
Safety	· Explosion / fire / physical damage · Human damages · Failure of factory assets	1
Environment	· Leak harmful gas to the air. · Leak harmful liquid to the river or sea.	2
Quality	· Recall product due to the defect of product. · Insufficient traceability due to loss of quality data.	3
Cost	· Loss of production stop. · Loss of disposal of intermediate product and raw materials. · Loss of operator's payment.	4
Delivery	· Loss of revenue. · Lose of the customer's trust due to the delayed delivery.	5
Others	· Reputation damage for uploading the sensitive information on SNS · Compliance violation.	6

Work3. Cybersecurity Risk Scenario

#	Undesirable Incidents	Risk Scenario
1	Explosion / fire / physical damage	· Due to insufficient management of USB memory drive usage, an outdated Windows-based SCADA terminal for the chemical plant is infected by malware and manipulated in a malicious way. It causes the severe damage of the plant such as explosion and fire.
2	Recall product due to the defect of product.	· Due to no boundary protection between IT and factory systems, a malware expands from IT systems to factory systems. It causes the defective chemical product by manipulation of recipe data.
3	Loss of production stop.	· Due to network segmentation and flat network architecture, once a malware infects a terminal in the factory systems, it spreads entire factory systems. It causes the long-term production stop because the recovery takes very long due to an insufficient asset management and no security logs

Figure 2: Sample result of OT risk workshop.

REFERENCE MODEL OF GOVERNANCE

After the workshop, factory personnel need to maintain the momentum of mindset transformation. They should promptly establish a cybersecurity governance organization for factory systems. The typical approach involves IT professionals determining the roles of factory cybersecurity for the factory staff. However, this often results in governance becoming a mere shell because the factory personnel do not fully grasp the underlying purpose. To enhance the situation, we must keep the concept of productivity resilience in mind (Fig. 3).

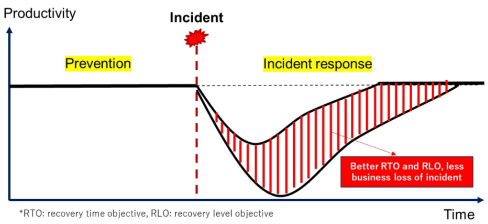
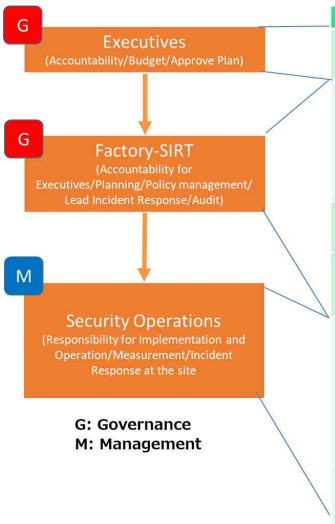


Figure 3: Productivity resilience concept.

The purpose of cybersecurity measures is not merely their installation; it is business risk mitigation. In IT systems, this typically involves protecting information. However, in factory systems, the primary goal is production continuity. Therefore, quick incident response and recovery are as crucial as prevention because they mitigate business losses when incidents occur. We have developed a reference model for governance in factory systems, aligned with COBIT5, which delineates roles in both prevention and incident response (Fig. 4). This transition is seamless after the workshop, as factory personnel are already aware of the risks that need mitigation.



Job Title	Role (Prevention)	Role (Incident Response)
Factory Manager	・Accountability of factory security management to the head office. ・Approval of security planning.	・Accountability for making decisions in a factory security incident.
Director of IT Team	・Budget planning based on OT risk assessment ・Personnel evaluation of security management personnel (building career path). ・Approval of factory security policies for asset management, vulnerability management, risk assessment, monitoring, incident response. ・Auditing factory security policy compliance. ・External organization point of contact.	・Making decisions from the viewpoint of cybersecurity in a security incident at factory. ・Coordination of stakeholders in a security incident at factory. ・Warning and punishment for security policy violators.
Director of Production Management	・Accountability for awareness and training of members.	・Making decisions from the viewpoint of production management in a security incident at factory.
Director of Production Engineer	・Accountability for awareness and training of members. ・Accountability for secure design and maintenance of members.	・Making decisions from the viewpoint of production engineering in a security incident at factory.
IT Team Members	・Collect information on factory system security risks ・Factory asset management. ・Regular update and patching operation. ・Vulnerability management (vendors, system integrators management). ・Regular implementation of factory system security risk assessment. ・Implementation of security countermeasures. ・Factory security monitoring ・Awareness and training	・Mitigation and investigation in a security incident at factory.
Production Engineers	・Factory asset management. ・Security by design for factory systems. ・Secure procurement (RFP and receiving test) ・Awareness and training	・Mitigation and investigation in a security incident at factory.

Figure 4: Governance reference model for factory systems.

At factory sites, executives who are usually factory managers handle accountability, budget approval, and plan endorsement. The Factory-SIRT, which serves as the core governance team for factory cybersecurity, is responsible for executives, planning, policy management, and leading incident response. When a cybersecurity incident occurs, the Director of the IT team coordinates stakeholders and oversees the incident response from a cybersecurity perspective. The Director of Production Management determines whether production should be halted. The Director of Production Engineering assesses OT risks stemming from the incident. Finally, the Security Operations team is responsible for implementation, operation, measurement, and incident response at the site. Once factory personnel define the roles of factory cybersecurity based on the reference model, establishing cybersecurity governance for factory systems becomes straightforward, enhancing readiness to mitigate the OT risks identified during the workshop.

CONCLUSION

In conclusion, we have developed an effective approach to enhance cybersecurity governance for factory systems in SMEs. This approach is rooted in the understanding that the original purpose of cybersecurity is to mitigate business risks, rather than merely installing cybersecurity countermeasures according to guidelines. The OT risk workshop facilitates a better comprehension of OT risks for all stakeholders. Following the workshop, factory personnel can easily establish factory cybersecurity governance using our developed reference organizational model. Our tools will soon be available on GitHub after the paper is published. Additionally, we plan to continue exploring how SMEs can enhance their cybersecurity readiness based on the 32 items outlined in the Japanese guidelines.

ACKNOWLEDGMENT

This research was supported by Fortinet Japan G.K. for collaborative work during the workshop. The authors extend their gratitude to the peer reviewers for their valuable feedback, which contributed to improving the quality of this manuscript.

REFERENCES

Bochman, A. A., & Freeman, S. (2021). Countering cyber sabotage: introducing consequence-driven, cyber-informed engineering (CCE). CRC Press.

GitHub (2023), OT Security Simple Assessment https://github.com/OTSec-Hiroshi-Sasaki/en-ot-security-simple-assessment. Last accessed 7 Jan 2024.

INL (2023). Consequence-Driven Cyber-Informed Engineering https://inl.gov/cie/

ISACA, 2012. COBIT 5: A Business Framework for the Governance and Management of Enterprise IT, Isaca.

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

Sasaki, H., Watanabe, K., & Koshijima, I. (2023). Analysis of Cybersecurity Risk for Factory Systems. *Human-Centered Design and User Experience*, *114*(114).