Strengthening Cybersecurity of Fuji Electric

UMEZAKI, Kazuya* YOSHIDA, Satoshi‡

ABSTRACT

Fuji Electric aims to contribute to the promotion of customer's DX by offering products and services that use IoT and digital technologies. To achieve this goal, it is the foremost importance to ensure that our products and services are secure. To strengthen our security as a vendor, we have revised our security policy and reinforced the defense system to improve our ability to defend against and detect new attacks, as well as took security measures for our development processes and our manufacturing sites. In addition, we are developing technologies that enhance the security of our products and services themselves.

1. Introduction

Since around 2010, the use of digital technologies such as the Internet of Things (IoT), artificial intelligence (AI), and cloud services has been expanding, and there has been a growing trend to establish competitive advantages by transforming products, services, and business models based on the needs of customers and society, as well as by transforming business operations, organizations, processes, and corporate cultures. Furthermore, since the end of 2019, COVID-19 has been accelerating the use of digital technologies in "new normal" environments, where remote work is encouraged under the restriction of going out.

At the same time, the rapid expansion of digital technologies is also causing an increase in cybersecurity risks due to a surge in cyberattacks.

Therefore, in order to promote digital transformation (DX), it has become necessary to strengthen cybersecurity measures as well.

This paper describes the cybersecurity risks associated with the progress of digitalization, the trends of countermeasures in Japan and overseas, and Fuji Electric's cybersecurity efforts based on these trends.

2. Cybersecurity Trends

2.1 Trends in cyberattacks

In recent years, there has been an increase in ransomware attacks that target organizations, such as universities and businesses. For example, computer viruses can be transmitted by attaching malicious files to emails, by directing users to phishing Web sites, or by exploiting vulnerabilities in operating systems. A ransomware attack uses a computer virus to encrypt files on a PC or server, renders the files unusable, and then demands money in exchange for recovering the files and sometimes threatens to release the information to the public if the money is not paid. Ransomware has caused major damage, including the shutdown of factory production systems and oil pipelines.

In the case of information leaks, there are an increasing number of incidents that exploit expanding supply chains by targeting organizations with weak security measures (contractors, overseas subsidiaries, etc.) as footholds. Therefore, it is necessary to take security measures not only for one's own organization, but also for the entire supply chain, including suppliers, contractors, and affiliated companies.

The increase in remote work due to COVID-19 has resulted in the rapid expansion of the use of virtual private networks (VPNs), cloud computing, and web conferencing, as well as an increase in attacks on these technologies.

2.2 Trends in cybersecurity measures

In light of such cyberattacks, governments and standardization organizations have been formulating regulations, standards, and guidelines for cybersecurity measures.

Cybersecurity measures can be divided into strategic risk management at the organizational level and system-level risk management for security threats in information systems (see Fig. 1).

At the organizational level, the Cybersecurity Framework (CSF) of the National Institute of Standards and Technology (NIST) is being used as a new framework that focuses on cyberattack countermeasures more than conventional information security management system (ISMS).

* Corporate R&D Headquarters, Fuji Electric Co., Ltd.

‡ Corporate Management Planning Headquarters, Fuji Electric Co., Ltd.

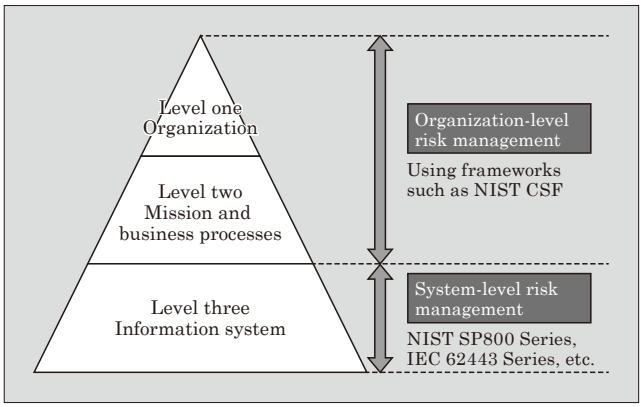

Fig.1 Risk management approaches for cybersecurity measures [1]

The CSF specifies security measures that organizations should implement according to five security functions (i.e., identification, protection, detection, response, and recovery). It aims at enabling organizations to properly manage security risks. Identifying information assets that need to be protected and their corresponding risks, an organization establishes security countermeasure goals (for protection, detection, response, and recovery) based on business requirements and risk tolerance, while also making systematic improvements. The CSF includes the following features:[2]

(1) Increased emphasis on detection, response, and recovery, rather than protection

Cyberattacks are becoming more sophisticated. Since it is difficult to completely protect against them, cybersecurity is now focusing on how to quickly detect them, minimize damage, and recover normal operations.

(2) Supply chain risk management

The goal is to identify, evaluate, and control products and services that may contain exploitable weaknesses due to low-quality manufacturing and development in the supply chain.

In regard to system level security, the NIST SP800 Series is being developed for information systems. To counter information leaks in the supply chain, NIST SP800-171 has been issued as a guideline that provides standards for countermeasures that should be taken by companies that do business with federal government organizations.[3] In addition, it is expected that standards such as IEC 62443 will be increasingly applied in control systems.

There are moves to create guidelines for each domain, including transportation systems such as automobiles, railroads, and ships, as well as electric power and petrochemicals. Regulations and guidelines that require specific security measures for IoT devices have been established in various countries. Furthermore, there are moves to require compliance with these regulations, standards, and guidelines through laws and regulations, and initiatives to establish certification mechanisms. In addition to the security of products and systems themselves, there are also requirements that target vendor development and manufacturing processes.

Vendors are being increasingly required to comply with these regulations, standards, and guidelines. Moreover, in addition to organizational security measures, vendors are also being required to ensure the security of their development and manufacturing environments and to apply appropriate security measures for their products and services.

3. Fuji Electric's Initiatives

In light of the increasing demand for vendor security measures described in Chapter 2, Fuji Electric has been taking steps to enhance the security of not only its existing internal information technology (IT) systems, but also operational technology (OT) systems in factories and other facilities and our products and services (see Fig. 2). For products and services, in addition to strengthening the security of development processes, we are also developing technologies to strengthen the security of products themselves.

3.1 Organizational initiatives

(1) Strengthening of our information security policy

In response to the increasing sophistication and complexity of cyberattacks, Fuji Electric formulated a new mid-term IT plan in 2019 and has designated the strengthening of cybersecurity as one of its priority measures.

Since it is difficult to completely prevent the latest attacks using conventional defensive security measures, we decided to adopt a new policy. Based on the assumption that intrusion will occur, we are prepared to detect intrusion early, speed up the response to the

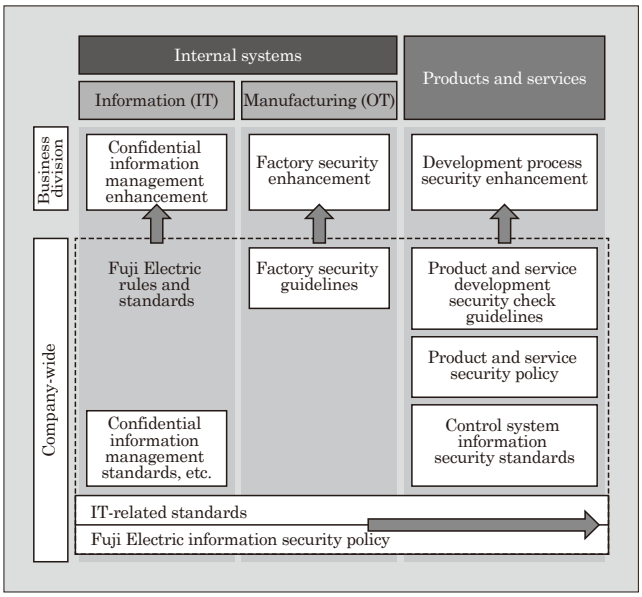

Fig.2 Fuji Electric's initiatives to strengthen security

attack, and strengthen the resilience of business while enhancing the protection system against new attack methods.

Accordingly, we have revised our information security policy and related rules and standards in accordance with the requirements of the NIST CSF and NIST SP800-171, and have made the following enhancements:

(a) Identification and protection
  (i) Revision of confidential information management methods and thorough management of such information
  (ii) Thorough security assessment, vulnerability countermeasures, operating management, and monitoring of cloud services and information systems
  (iii) Enhancement of protection and monitoring capabilities for systems and client devices, enabling zero-trust security
(b) Detection
  (i) Enhanced monitoring of unknown attacks and abnormal behavior in networks, systems, servers, and devices
  (ii) Strengthening of monitoring operations using a security operation center (SOC)
(c) Response
  (i) Development of a crisis management system for cyber incidents that includes management-level involvement to ensure immediate initial response in the event of an emergency
  (ii) Strengthening of cyber-incident response through Fe-CSIRT (Fuji Electric Computer Security Incident Response Team) and our information security management system
  (iii) Establishment of a system in cooperation with external specialists to outsource technical support such as forensics (investigation of evidence left on computers to determine the cause of a security incident, such as a cyberattack, or accident) in preparation for initial response, as well as legal and public relations support
  (iv) Automation of the collection of cyber risk and threat information, and thorough alerting of system administrators and users
(d) Recovery and business continuity
  (i) Adding recovery plans and procedures in preparation for cyberattacks to the IT business continuity management (BCM) that has conventionally presuming natural disasters
  (ii) Implementation of response training to enhance the effectiveness of recovery plans

(2) Strengthening of manufacturing security

In the past, Fuji Electric's factories operated manufacturing equipment using a manufacturing network that was isolated from the Internet and internal information networks. This meant that the cybersecurity risk was small, and protection could be achieved by paying attention to opportunities that enable data to be transferred to and from the contact point of information systems, for example, by reducing the possibility of indirect malware infection via USB memory or maintenance PCs.

However, in recent years, as the IoT of factories and the digitalization of manufacturing have progressed, the need for communications between manufacturing and information networks has increased, and the possibility of cyberattacks similar to those on information systems has increased, thus necessitating countermeasures. In the past, cybersecurity risks were low in manufacturing sites, where cybersecurity awareness was not high and there was a lack of security engineers.

Therefore, in addition to understanding the need for security and corresponding measures, we established a system that enables the IT department to be involved in the manufacturing system measures.

It is difficult to stop manufacturing equipment to apply software patches or anti-malware software, and applying the software while the equipment is in operation can cause abnormal operations. Therefore, technical measures need to be taken differently from those of information systems. However, in addition to applying the same countermeasures as those of information systems to the extent possible, we have also enabled our control devices, which have limited applications and communications features, to implement defensive measures to reduce the risk of cyberattacks by minimizing software operation and communication cybersecurity risks.

Except for technical measures, many measures are basically the same as those for information systems. We thoroughly utilize the framework of conventional information security initiatives to implement organizational measures, such as security systems, and physical measures, such as controlling access to and from the factory and its security zones, as well as education and awareness activities. Expanding and horizontally sharing measures taken for our information systems, we are enhancing our detection and response to cyberattacks.

Along with the cyberattack scenarios of IT-BCM, recovery procedure is incorporated into the BCM framework of our factories.

(3) Security measures for products and services

In order to respond to the increased security risks that was accompanied the introduction of IoT, Fuji Electric published a security policy for its IoT products and services as an internal standard in April 2018 and has since been strengthening its security measures.[4] In June 2021, we published a revised version that reflects the security requirements strengthened by CSF and IoT-related guidelines.

In order to ensure the security of products and services, it is necessary to implement security mea-

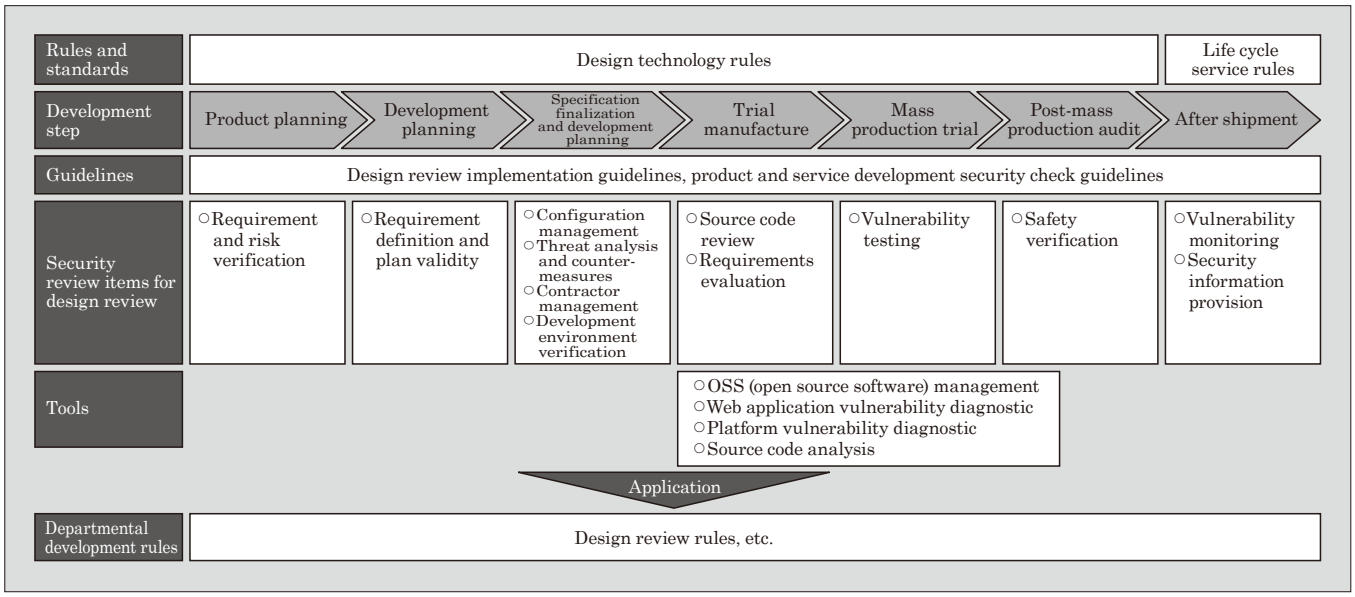

Fig.3 Security measures in product and service design reviews

sures at each stage of the product life cycle (from the planning stage to development, manufacturing, testing, usage, and disposal). Therefore, we established guidelines as internal standards that define security measures that should be implemented at each development step of products and services, as well as security review items that should be confirmed in design review (DR) (see Fig. 3).

These internal standards require the appropriate identification of security requirements that need to be addressed without omission. At the product planning stage, we have to confirm the applicable procurement requirements, laws, regulations, and risks. According to those conditions, at the development planning stage, we have to confirm the validity of the requirements definition and development plan. At the specification finalization and development planning stages and beyond, in order to comply with security requirements, it is necessary to implement specific security measures based on threat analysis, prevent vulnerabilities in design and implementation, and ensure security in the development environment. Supply chain security measures require the management of contractors, as well as the establishment of systems and processes for monitoring vulnerabilities and providing security information after products are shipped.

These measures are reflected in the DR processes of each business division and factory to strengthen security measures for all Fuji Electric products and services.

3.2 Security technology development

Table 1 shows some of the technological developments to improve the security of products and services. Besides technologies for protection, we are developing technologies for detection, response, and recovery based on the assumption of cyberattack intrusion. We are also developing the technical means of security measures that are required at each stage of product and service development.

Table 1 Product security technology development

Technology	Description	Protection	Detection	Response	Recovery
Secure runtime environment	Secure boot, runtime data protection	✓	—	—	—
User authentication and authorization	Multi-factor authentication on web servers, etc.	✓	—	—	—
Log monitoring	Detection and analysis of signs of cyberattacks and damage caused to equipment and systems	—	✓	✓	—
Secure coding	Prevention of vulnerabilities during software development	✓	—	—	—
Web server vulnerability verification	Web application and platform vulnerability detection	—	✓	✓	—
OSS (open source software) management	Detection of OSS vulnerabilities and licensing issues that software depends on	—	✓	✓	—
Incident management	Labor savings and automation of incident detection, impact analysis, and recovery	—	✓	✓	✓

(1) Secure runtime environment

Devices that are connected to external environments such as the Internet are at risk of security incidents, such as being remotely controlled through unauthorized access or causing information leaks due to

computer viruses.

We have developed a technology that enables secure boot (software verification at startup) and runtime data protection. This technology is based on microcomputers with built-in security functions, but customized to reduce its memory usage and processing time to meet constrained specifications of our embedded products.

(2) User authentication and authorization

There has been an increasing number of incidents of information leakage due to unauthorized logins to web servers.

We are developing technology to enable existing web servers (ID and password based user authentication) to support multi-factor authentication. This authentication method will make it possible to add authentication using client certificates and other means, without making major changes to existing websites.

(3) Log monitoring

Cyberattacks that seek to gain unauthorized access and steal information are becoming increasingly sophisticated and often take a long time to detect. Therefore, it is important to take measures to detect damage and signs of cyberattacks as quickly as possible. To achieve this, we are developing systems to collect and manage various logs from IoT systems and other sources to enable efficient monitoring and analysis.

By using these systems to collect and analyze access and operation logs, it will be possible to quickly detect potential cyberattacks such as authentication failures.

(4) Secure coding

Vulnerabilities in a product's software increase the likelihood that it will be exploited by cyberattacks. Therefore, it is necessary to prevent vulnerabilities during the software development stage.

To achieve this, we developed application procedures and document templates that facilitate the application of CERT C secure coding rules, and check compliance to the source code rules using diagnostic tools and compliance reports. We apply this approach to C language firmware development, as well as to other programming languages.

(5) Web server vulnerability verification

There has been an increasing number of incidents of information leakage caused by unauthorized access that exploits vulnerabilities in web servers.

We are evaluating and selecting standardized tools for vulnerability assessment of web applications and platforms.

4. Postscript

In this paper, we described Fuji Electric's cybersecurity efforts. In recent years, cyberattacks have become more sophisticated and complex, and security threats have been increasing due to growing use of digitalization. Fuji Electric has revised its information security policy to strengthen security measures not only for information but also for factories. In order to provide more secure products and services, we have formulated a security policy for our products and services and established systems and processes for implementing security measures from the development stage while working on the development of security technologies.

Since cyberattacks are advancing day by day, it is essential that security measures be taken on an ongoing basis. Moving forward, we will continue to contribute to the promotion of customer DX through efforts that improve the security of Fuji Electric and its products and services.

References

(1) Risk Management Framework for Information Systems and Organizations: A System Life Cycle Approach for Security and Privacy, Revision 2, NIST, SP800-37, 2018-12. https://www.nist.gov/publications/risk-management-framework-information-systems-and-organizations-system-life-cycle.

(2) Framework for Improving Critical Infrastructure Cybersecurity, Version 1.1, NIST, 2018-04. https://nvlpubs.nist.gov/nistpubs/cswp/nist.cswp.04162018.pdf, (accessed 2021-07-28).

(3) Protecting Controlled Unclassified Information in Nonfederal Systems and Organization, Revision 2, NIST, SP800-171, 2020-02. https://csrc.nist.gov/publications/detail/sp/800-171/rev-2/final, (accessed 2021-07-28).

(4) Umezaki, K. IoT System Security. FUJI ELECTRIC REVIEW. 2018, vol.64, no.3, p.154-157.

Fuji Electric

Innovating Energy Technology