Supply Chain Security Measures Using Outcome-based Approach

● Yuki Fukuda ● Isamu Kawamura ● Yoshihiro Kubota ● Yoshiro Wataguchi

In recent years, cyber attacks targeting companies and organizations without sufficient supply chain security measures have increased and security standards across many countries have fragmented. As a result, the burden of security measures on companies and organizations have increased. In response, Fujitsu believes it can contribute to reduce the burden of supply chain security measures by making use of an outcome-based approach that is increasingly being used by some regulators and standardization organizations on security. In this approach, only the results to be accomplished by security measures are specified as requirements, and the selection of the specific security measures is left up to those taking the security measures. Benefits will include a reduction of the burdens on both purchasers and suppliers in supply chains. This paper describes how to deploy this approach and the benefits of such an approach.

1. Introduction

The expansion of digital businesses based on technologies such as the IoT and AI has created a "connected society" where all kinds of objects and services are connected to the network. A new age has arrived in which various types of data can be exchanged and services can be enjoyed with no regard to borders.

A consequence of these trends has been the development of security standards, rules, and guidelines (hereafter, security standards) in many different countries to deal with heightened security risks and privacy violations. However, this situation has led to the fragmentation of security standards across the world, causing confusion in many different areas.

The area that is greatly affected is the supply chain. Supply chains are spread across the globe, which means they must comply with many different security standards, and this increases the burden on companies.

In response to these challenges, Fujitsu has been studying how an outcome-based approach can be used to improve security measures for supply chains. The aim of the outcome-based approach is to reduce the burden of complying with these security standards that are growing on a global scale. The use of such an approach is increasing at some regulators and standardization organizations on security.

This paper first describes the issues facing supply chains and the issues of conventional security measures. Then, it describes how to deploy the outcome-based approach proposed by Fujitsu and the benefits of the approach.

2. Issues facing supply chains in Japan and internationally

This section describes the issues facing supply chains.

2.1 Security risks for companies involved in supply chains

Large corporations in Japan are already investing in security measures against malware and other cyber attacks. However, small- and medium-sized businesses tend to only invest small amounts in security.[1)]

Some small- and medium-sized suppliers in the supply chain have not implemented adequate security measures. Therefore, incidents have increased where attackers use these suppliers as a gateway for attacks on purchasers. Actual cases have occurred where the purchaser's product design data, personal information, and confidential business information have been leaked via suppliers in the supply chain. Such cases reveal issues that could affect any company in the supply

chain, regardless of its business type, configuration, or size. Any company could become either a victim or a victimizer (inadvertently contribute to the damage).

2.2 Fragmented security standards in each country

Security standards are currently being developed in the U.S., Europe, Japan, and other Asian countries. For example, in the U.S., the National Institute of Standards and Technology (NIST) publishes the Special Publication (SP) series,[2] and the Federal Risk and Authorization Management Program (FedRAMP) security standard system[3] is used for the procurement of cloud services that are used by U.S. federal agencies.

European standards include the U.K.'s PSN certification (Apply for a Public Services Network connection compliance certificate)[4] and Germany's BSI-Standards (Bundesamt für Sicherheit in der Informationstechnik-Standard).[5]

In Japan, bodies such as the National Center of Incident Readiness and Strategy for Cybersecurity (NISC)[6] and the Information-technology Promotion Agency (IPA)[7] have issued various security standards that are used by companies and organizations.

Most of these security standards were created in each country independently. Even security requirements comprised of roughly the same objectives and results after implementation are specified using different methods and approaches in different countries. As a result, implementation work must be duplicated to comply with multiple security standards, and this compliance takes a long time and leads to increased costs.

For example, when assessing security standards compliance, the methods of evaluating security measures and the evidence to be confirmed vary by country. The specified evaluator also varies by country, with some countries requiring a governmental body, while in others, a private organization or company is sufficient. Therefore, even when the security requirements themselves have been satisfied, each standard may generate its own extra work to deal with assessing compliance or third-party certification.

3. Issues in performing security measures at purchasers and suppliers

As described in the previous section, there are two main issues when dealing with the security of supply chains. Currently, the most common methods for enforcing security in supply chains are "contract and procedure-based measures."

ISO/IEC 27036 (a standard providing guidelines on information security risk management when procuring products or services from suppliers)[8),9)] specifies the guidelines for control that should be implemented in each phase such as selection of suppliers, contracting, and contract fulfillment management and assurance, as information security measures related to procurement. In Japan, the Ministry of Economy, Trade and Industry (METI) published its "Cybersecurity Management Guidelines"[10] in 2015. In the same year, NISC specified information security measures related to procurement in its "Guide for Creating Specification Documents for Responding to Supply Chain Risks Related to Supplier Information Security in Outsourcing."[11]

The key points of these guidelines for reducing the risk of cyber attacks on purchasers in the supply chain are described below.

- Check the security level when selecting suppliers
- Clarify the demarcation points of security responsibilities in contracts
- Clarify how to respond to incident occurrence
- Check the security management system periodically, such as by assessment
- Manage subcontractors

The guidelines, however, describe just the aspects to be managed and not how to manage them. Then, actual requirements to be implemented by the suppliers are up to the purchaser. As a result, the following two issues come up when requesting the supplier to perform security measures (**Figure 1**).

1) Impairs flexibility of security measures at suppliers

Purchasers often instruct suppliers to use the security measures implemented at the purchaser's own company. This is because managing security requirements individually for each supplier increases the work burden at the purchaser and makes operations less efficient. The end result is that compliance costs at suppliers increase and the flexibility of their security measures is impaired.

For example, a purchaser requested the automation of log collection as a security requirement, but the supplier could not deploy such an automation tool because its budget was insufficient. In this case, even if the supplier implemented an alternative measure

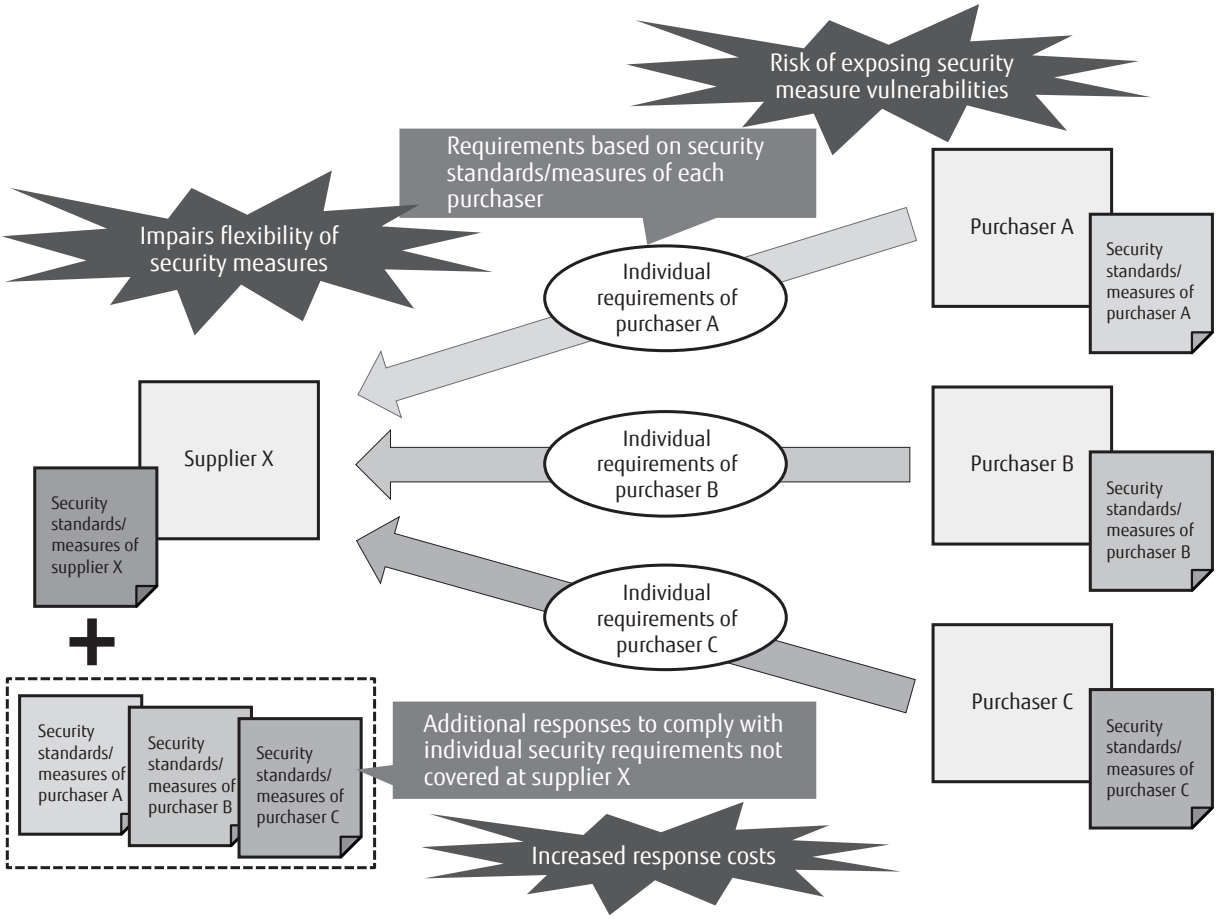

Figure 1
Security requirement problems for suppliers and purchasers.

such as manual collection that ensured security to an equivalent level, it would be judged as not meeting the security requirement. Flexibility impairment is the excessive restriction of the security measures of the supplier by the requirements of the purchaser. Even important suppliers in the supply chain may fail their security qualification, which unnecessarily narrows the options for selecting suppliers.

2) Risk of exposing security measure vulnerabilities of purchaser

When a purchaser requests the supplier to perform security measures based on those for the purchaser's own products and services, the purchaser inadvertently reveals its own security measures and implementation level to other companies. Even signing a non-disclosure agreement (NDA) does not completely eliminate the risk of this information being used to identify the security vulnerabilities of the purchaser. For example, the purchaser requests that the supplier adopts the security monitoring periods of the purchaser as a security requirement. The result may be that the purchaser has revealed to the supplier that malicious operations cannot be detected between the monitoring periods.

4. Outcome-based approach proposed by Fujitsu

In response to the current situation of supply chains and security measure issues described above, Fujitsu studied the potential of adopting an outcome-based approach. In this approach, only the results that should be accomplished by the security measures are described as requirements. The specific controls and methods for achieving the requirements can be selected by the suppliers. This lightens the burdens on both purchasers and suppliers.

4.1 Overview of outcome-based approach

This approach started to be used by some regulators and standardization organizations from the middle of the 2000s to address the issues described in subsection 2.2, and its use has been expanding steadily. An example of a standard that incorporates this approach is NIST SP800-171.[12] This is a security measure guideline for handling Controlled Unclassified Information (CUI), and is one of the standards in the SP series of NIST. Although CUI is not designated as classified information, it includes important information that needs to be managed correctly. Examples include credit card information or medical data, or information for developing weapons systems.

An example of a requirement in NIST SP800-171 is "3.6.1 Establish an operational incident-handling capability for organizational systems that includes adequate preparation, detection, analysis, containment, recovery, and user response activities." This description indicates that the security standard is based on this approach.

The Cybersecurity Framework (CSF)[13] created and published by NIST is also a cybersecurity standard that incorporates this approach. The framework core of CSF defines five functions: Identify, Protect, Detect, Respond, and Recover. Security requirements based on these functions are described by following this approach.

CSF has also been adopted for ISO/IEC TR 27103 (guidance for utilization of standards such as ISO/IEC 27001 from the perspective of cybersecurity),[14] for which discussions are currently proceeding. Adoption of CSF is likely to grow in other areas as well, as this approach is used or referenced in the security standards of many countries, including Japan.

4.2 Procedure for deploying outcome-based approach

Fujitsu seeks to overcome the previously described issues by positioning a security standard based on this approach between the security standards actually implemented by the purchaser and supplier. Specifically, a security standard based on this approach is positioned as an intermediate language between the security measures of the purchaser and supplier, as shown in **Figure 2**. The purchaser evaluates the supplier's accomplishment of security protection via this intermediate language. This lessens the burden on the supplier for complying with individual security requirements from different purchasers, and provides greater flexibility when selecting security measures. This also reduces the burden on the purchaser when selecting and evaluating suppliers, and enables the purchaser's own detailed security measures to be kept secret.

The following describes the procedure for deploying this approach at one's own organization or at a supplier in the supply chain.

1) Adoption of security standards

This is the setting of the intermediate language by the purchaser. If the compliant security standard is that based on this approach, the required items can be, then, selected from the security requirements described as outcome-based in the security standard, and they can be used as the intermediate language. When the current practice is not based on an outcome-based standard, a security standard based on this approach will be newly adopted as the intermediate language, and the current security measures will be mapped to this.

In a notable development, it became mandatory for all companies in supply chains related to the US defense industry to comply with NIST SP800-171 from December 2017. In addition, this standard is also highly likely to be adopted for the procurement of defense equipment and in important infrastructure fields in Japan, and its use as an intermediate language for supply chain security measures is encouraged. As CSF has also started to be widely used for a common language for cybersecurity, this may also be used as an intermediate language.

2) Evaluation of security measures at suppliers

The purchaser will evaluate security measures at the supplier according to the security standards based on this approach that are used as an intermediate language. Specifically, the supplier will map its security measures based on a different standard from the one adopted by the purchaser to the purchaser's security requirements described in an outcome-based manner, and the supplier will report the mapping results and achievement level. The purchaser will evaluate the status of the security measures based on the details of the report.

5. Benefits of outcome-based approach

This section describes the specific benefits of

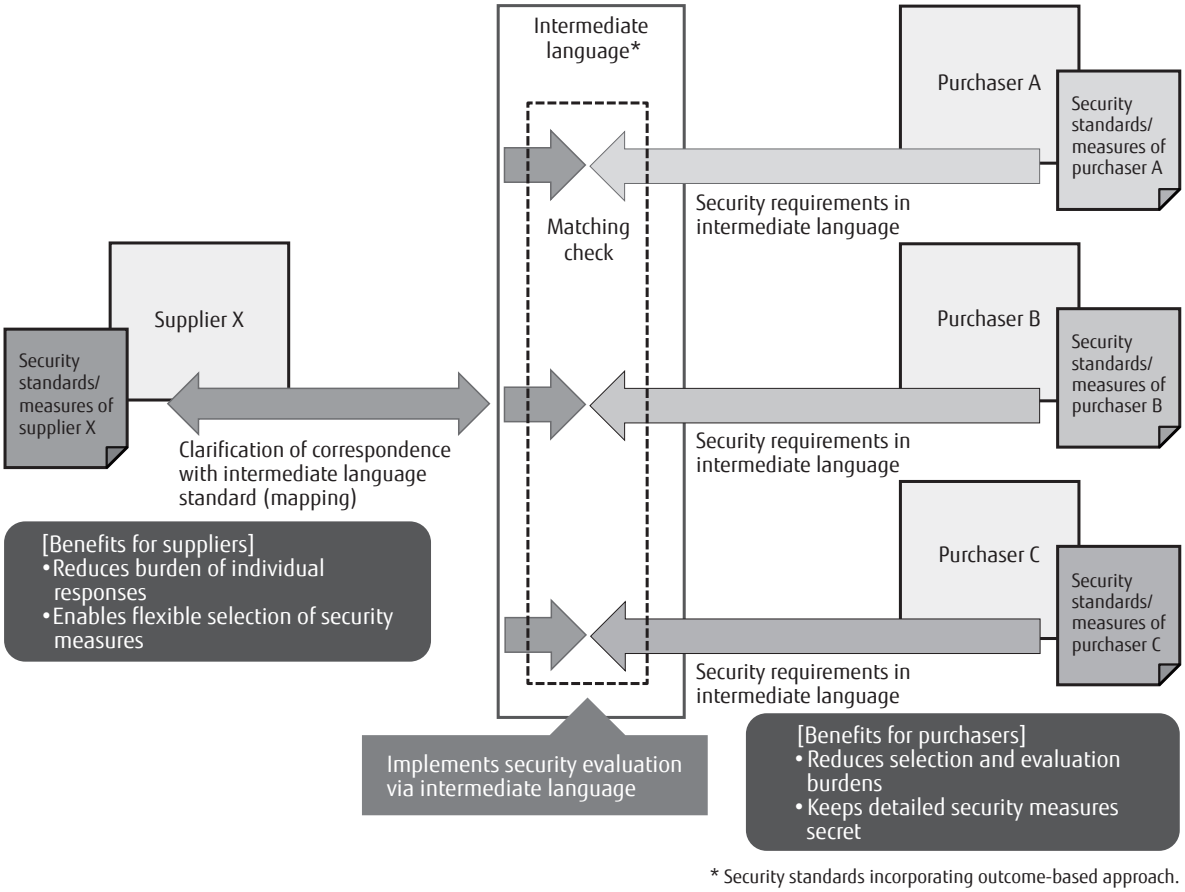

Figure 2
Structure of security requirements using outcome-based approach.

incorporating this approach into the security measures of supply chains.

1) Benefits for suppliers who implement security requirements

This approach helps resolve the issue whereby different procedures or approaches have to be implemented by each supplier for multiple security requirements from multiple purchasers, even when the achieved results are the same. This enables security measure costs to be reduced by suppliers.

This approach also increases implementation flexibility by enabling the supplier to freely select the security measures. As described in section 3. 1), if a company that has not implemented an automated tool for a certain security requirement can use an alternative method such as manual operation or enhancing an existing monitoring method, the target (e.g. outcome) is, then, achieved as long as the level of the security measure outcome is the same as the requirement. This widens the selection range of suppliers for the purchaser.

2) Benefits for purchasers who specify security requirements

When the purchaser specifies security requirements for the supplier by using this approach, it is possible for the supplier to take actions for only the corrective measures for security requirements that the supplier has not yet achieved. Therefore, the process for complying with the security standards does not need to be started from the beginning again, which prevents increased procurement costs and schedule delays.

Current security implementation methods and future milestones can be evaluated at the purchaser as well, which has the benefit of enabling flexible selection and evaluation of suppliers that are important for providing the company's own products and services.

Further, this approach enables the purchaser to specify security requirements for the supplier via the security standards used as the intermediate language. As a result, the detailed security measures (and specific implementation methods) of the purchaser do not need to be revealed to the supplier, which avoids the risk of identifying security vulnerabilities.

6. Conclusion

This paper first described the issues facing supply chains in Japan and internationally, and those of purchasers and suppliers. Then it described measures using an outcome-based approach that helps resolve these issues. Concern regarding security threats to supply chains is growing around the world. As a sign of this, threats to the supply chain was ranked 4th in the Organization section of the 10 Major Security Threats 2019[15] released in February 2019. Fujitsu has been following these trends and studying the application of security evaluations that use this approach to its own supplier evaluation system. In the future, Fujitsu will use this approach while confirming its own results to enable both purchasers and suppliers to strengthen their supply chain security measures, and widely expand the scope of these activities to enable the safe and secure promotion of business.

References

1) IPA: Current Status of Information Security Measures at Small- and Medium-sized Businesses in 2016 – Research Report –. pp. 70–75 (in Japanese).
https://www.ipa.go.jp/files/000058502.pdf
2) Computer Security Resource Center (CSRC): All SP (Special Pubs) series.
https://csrc.nist.gov/publications/sp
3) FedRAMP.
https://www.fedramp.gov/
4) U.K. Government: Apply for a Public Services Network (PSN) connection compliance certificate.
https://www.gov.uk/guidance/apply-for-a-public-services-network-psn-connection-compliance-certificate
5) Federal Office for Information Security, Germany: BSI -- IT-Grundschutz-Standards.
https://www.bsi.bund.de/EN/Publications/BSIStandards/BSIStandards_node.html
6) NISC.
https://www.nisc.go.jp/eng/
7) IPA.
https://www.ipa.go.jp/index-e.html
8) International Organization for Standardization (ISO): ISO/IEC 27036-1:2014, Information Technology -- Security Techniques -- Information Security for Supplier Relationships -- Part 1: Overview and Concepts.
https://www.iso.org/standard/59648.html
9) ISO: ISO/IEC 27036-3:2013, Information Technology -- Security Techniques -- Information Security for Supplier Relationships -- Part 3: Guidelines for Information and Communication Technology Supply Chain Security.
https://www.iso.org/standard/59688.html
10) METI, IPA: Cybersecurity Management Guidelines Ver 1.1.
https://www.meti.go.jp/policy/netsecurity/downloadfiles/CSM_Guidelines_v1.1_en.pdf
11) NISC: Guide for Creating Specification Documents for Responding to Supply Chain Risks Related to Supplier Information Security in Outsourcing (in Japanese).
https://www.nisc.go.jp/active/general/pdf/risktaiou28.pdf
12) NIST: NIST Special Publication 800-171, Protecting Controlled Unclassified Information in Nonfederal Systems and Organizations.
https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-171r1.pdf
13) NIST: Framework for Improving Critical Infrastructure Cybersecurity Version 1.1.
https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.04162018.pdf
14) ISO: ISO/IEC TR 27103:2018, Information Technology -- Security Techniques -- Cybersecurity and ISO and IEC Standards.
https://www.iso.org/standard/72437.html
15) IPA: 10 Major Security Threats 2019.
https://www.ipa.go.jp/files/000076989.pdf

Yuki Fukuda
Fujitsu Ltd.
Mr. Fukuda is currently engaged in research and development for global security quality assurance.

Isamu Kawamura
Fujitsu Ltd.
Mr. Kawamura is currently engaged in research and development for global security quality assurance.

Yoshihiro Kubota
Fujitsu Ltd.
Mr. Kubota is currently engaged in research and responses to international standardization trends related to cybersecurity.

Yoshiro Wataguchi
Fujitsu Ltd.
Mr. Wataguchi is currently engaged in internal application of enterprise system security.