Yokogawa's Approach to Enhancing Security of its Products and Handling of their Vulnerability

Hirotaka Tsuji [*1]

These days, the risk of a cyber-attack is recognized on not only information systems but also industrial control systems, and for Yokogawa's business, security has become an important requirement for our customers. Customer satisfaction is inherent in Yokogawa's corporate philosophy and to achieve it Yokogawa needs to work harder, through its products and services, to ensure the security of customers' environments. In 2014, Yokogawa disclosed vulnerability in the CENTUM CS 3000 integrated production control system. This is the first time that Yokogawa disclosed a vulnerability to people other than users, and several problems were found while responding to these. Taking this opportunity, Yokogawa Point of Contact (YPOC) revised the vulnerability handling standards and system with a view to issuing them as rules for the entire Yokogawa Group. This paper describes these standards and system.

INTRODUCTION

In the past, control systems were independent ones based on original architecture and protocols with no connection to business networks. For this reason, security for control systems was not considered seriously. These days, the technology that changed to Commodity, through development of information technology and the reduction in costs, came to be adopted for control systems. In addition, for convenience and for linkage with other information such as management information, control systems are connected to business networks. As a result, security threats that information systems have been exposed to are beginning to be seen in control systems, and thus, the concern for security measures of control systems is increasing.

NECESSITY OF PRODUCT SECURITY

Control System Security at Present

As described below, the conditions surrounding the security of control systems has been rapidly changing since the appearance in 2010 of Stuxnet [(1)], which is known as the first malware targeting control systems.

1) Diversifying cyber-attacks

Recent cyber-attacks such as phishing by criminal groups for money, DoS attacks by parties wanting to assert a certain ideology, and stealing information by military organizations have appeared in many ways. New attacking techniques like interactive and watering-hole attacks have appeared.

2) Easiness of cyber-attacks

Tools and information for cyber-attacks can be easily obtained on the Internet, and the cost for cyber-attacks is decreasing. In other words, the technical and financial barriers to cyber-attacks are lowering.

3) Openness of control systems

Control systems use general-purpose technologies and are connected to business networks more than before.

4) Study on control system security

Studies and surveys on control system security are being conducted, and vulnerability reports about the software products and devices comprising control systems are disclosed to the public at events or on web sites. The disclosed information sometimes includes attack tools as verification tools.

5) Responsibility of product vendors

Product vendors must not only make efforts to offer secure products but also provide users with information regarding the vulnerabilities of their own products including information on the countermeasures against those vulnerabilities. Such understanding is required of control system vendors as well as IT product vendors.

*1 IA Platform Business Headquarters Common Technology Development Center Technology Promotion Dept.

In this way, the conditions surrounding the security of control systems have been changing significantly. However, the availability of control systems is still a high priority. Once a control system starts operation, it cannot be suspended easily. Moreover, control systems are used for a long time, generally several decades. As a result, there are many cases where countermeasures against diverse cyber-attacks cannot be implemented in a timely manner or the latest security measures cannot be applied to control systems. Thus, the risks in customers' environments are increasing year by year.

Yokogawa's Approach to Enhancing the Security of Its Products and Services

Yokogawa has been making efforts to enhance the security of its products and services by actively performing quality improvement activities for its products and services, and risk management through confidential information management and crisis management. Figure 1 shows conceptually Yokogawa's approach to enhancing the security of its products and services.

The product quality improved by quality improvement activities will reduce vulnerabilities of the products and improve their security quality. Proper management of design information and vulnerability information of products through confidential information management will eliminate the possibility of an attacker easily obtaining information usable for attacking. If an incident involving serious losses or affecting human lives is caused by cyber-attacks to Yokogawa's products, it is in the scope of Yokogawa's crisis management and must be treated following its crisis management rules. However, Yokogawa's efforts for quality improvement, confidential information management, and crisis management are not enough for ensuring and improving the security of customers' environments. Furthermore, cyber-threats must be tackled. Efforts for providing secure products and dealing with vulnerabilities are more crucial than ever.

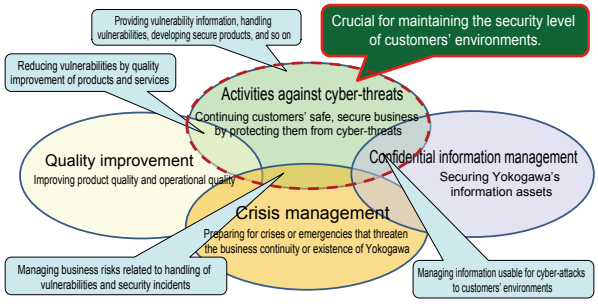

Figure 1 Yokogawa's approach to enhancing the security of its products and services

Until 2013, there were no products of the YOKOGAWA Group for which vulnerability information was open to the public. Yokogawa disclosed the vulnerability information on the CENTUM CS 3000 integrated production control system in March 2014, according to a trigger by a report from a security vendor to the Computer Emergency Response Team/Coordination Center (CERT/CC), a US organization for coordinating vulnerability information. When disclosing the vulnerability information on the CENTUM CS 3000, a cross-organizational response was required and then the needs for unified standards and procedures were recognized by Yokogawa. Under the corporate philosophy of customer satisfaction, Yokogawa has been making efforts to enhance the security of its products and services through quality improvement activities and confidential information management. In addition to that, to respond to the changing conditions around recent control systems and to meet the corporate philosophy of customer satisfaction, Yokogawa makes further efforts for enhancing the security of its products and services including handling of their vulnerabilities.

DEALING WITH THE VULNERABILITIES

Vulnerability

Vulnerability is defined in the Standards for Handling Software Vulnerability Information and Others (Directive #110, 2014) by the Ministry of Economy, Trade and Industry (METI) [2] as follows:

- A security flaw in a software product or other item that may be attacked by computer viruses or unauthorized access to cause damage to its function or performance

In the same directive, a software product is defined as:

- A software product or hardware, with software built in, product that has general versatility

Vulnerability and software defect are often confused with each other, and many causes of the vulnerabilities are, in fact, defects. However, vulnerabilities are different from the defects that cause system hang-up or other failures in usual operation by customers. Vulnerability is a potential risk under the usual operation environment of customers, which causes incidents such as system hang-up only after being attacked. From the viewpoint of preventing security incidents, vulnerability must be handled while it is in the state of potential risk.

Vulnerability Information Handling Framework in Japan

In 2004, METI released the Standards for Handling Software Vulnerability Information and Others (Directive #235, 2004); the original version of the directive #110 in 2014 referred to above. This directive triggered the establishment of Yokogawa's vulnerability handling framework shown in Figure 2. Vulnerability information is accepted by the Information-technology Promotion Agency (IPA) and the handling of vulnerability is coordinated by the Japan Computer Emergency Response Team Coordination Center (JPCERT/CC). This framework works in accordance with the Information Security Early Warning Partnership Guideline [3] and aims to suppress the damage caused by unauthorized computer access, computer viruses, and the like in Japan. In the 2014 version of this guideline, control systems are added to the supplementary explanation of software products, indicating explicitly that not only IT products but also control systems and the products constituting them are included in the scope of the vulnerability handling.

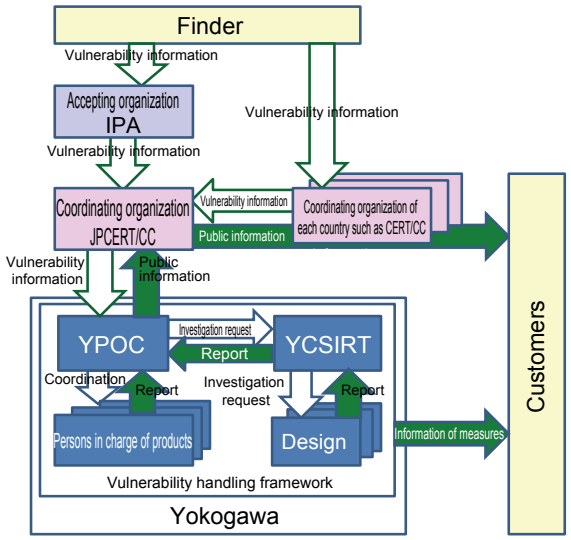

Figure 2 Yokogawa's vulnerability handling framework

Standards for dealing with vulnerability

Expectations regarding dealing with the vulnerability differ between markets and customers. Yokogawa considered dealing with vulnerability as a customer requirement and each business division or organization responsible for products handled their vulnerabilities. However, dealing with the vulnerability in the case of the CENTUM CS 3000 described above impacted on other products, and the necessity of standards and a framework for dealing with vulnerabilities as Yokogawa as a whole has been recognized. Currently, vulnerability handling standards are being drawn up under the initiative of Yokogawa Point of Contact (YPOC). These standards will be authorized as YPOC management documents and will be used as operating standards and procedures when handling vulnerability information. At present, preparation to publish those standards dealing with vulnerability as standards for the entire worldwide Yokogawa organization is under way in YPOC. The outline of the standards is described below.

1) Approach for reducing risks in customers' environments

To reduce risks in customers' environments, the standards instruct persons concerned to practice the following:

- Collect the latest vulnerability information.
- Prevent products from creation of and contamination by vulnerabilities
- Properly manage vulnerability and security information
- Promptly provide customers with vulnerability information, workarounds and measures when vulnerability is found

Yokogawa makes every effort to collect the latest vulnerability information, feed it back to the operations, and makes use of it for improving development processes, operation standards and operating procedures. Yokogawa offers customers not only secure products but also support regarding vulnerability through providing measures and workarounds for vulnerabilities based on the latest information. Yokogawa will also respond to changing conditions.

2) Tasks and responsible organization when vulnerability is found

Vulnerability dealing with the flow from acceptance of information to its publication is defined as shown in Figure 3, and tasks and the responsible organization in each phase are also clearly defined. Following this dealing flow, Yokogawa promptly offers accepted vulnerability information to customers, and helps customers to not increase vulnerability risks in their Yokogawa products.

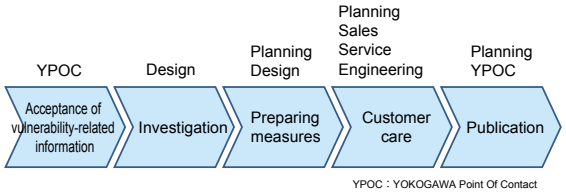

Figure 3 Handling flow of the vulnerability information,

3) Standards for action in the vulnerability reports

The standards clearly define the following items for dealing with vulnerabilities.

- Responsible organization for vulnerability handling
- Procedure for providing vulnerability information
- Time to provide vulnerability information
- Contents of vulnerability information to be provided
- Provision of workarounds or countermeasures

Yokogawa defines its fundamental policy for dealing with vulnerabilities and will work hard to gain customers' credibility in the field.

Yokogawa's Dealing with Vulnerability Framework

Yokogawa's dealing with vulnerability framework is shown in Figure 2, and its outline is explained below.

1) Collaboration with external organizations

Yokogawa established YPOC in 2005 as the contact point to JPCERT/CC in accordance with the Information Security Early Warning Partnership Guideline. YPOC has been collecting the latest vulnerability information and handling it. In addition, YPOC collaborates with external organizations including overseas CERT organizations.

2) Internal framework

Within Yokogawa, the Yokogawa Computer Security Incident Response Team (YCSIRT) has been organized under the initiative of YPOC as an internal communication framework for vulnerability information, while assigning persons in charge for each product group. The YCSIRT promotes the prompt informing of and smooth communication of vulnerability information within Yokogawa and conducts its impact study.

On the basis of the impact study, YPOC coordinates the whole action of dealing with vulnerability by supporting the organizations in charge of related products through creating response policies, preparing messages to customers, posting notifications to customers on the web, and others.

As described above, Yokogawa has established a

framework to deal with vulnerability, and behaves following the vulnerability handling standards when vulnerability is found in products delivered to customers. Yokogawa is making efforts to promptly provide correct information to customers so that the risks in customers' environments do not increase.

CONCLUSION

Security of control systems is an important requirement from customers and is expected to become more important in the future. Yokogawa will continue to enhance the security of control systems; however, maintaining the security level of customers' environments cannot be achieved by the internal efforts of Yokogawa alone. It is crucial that Yokogawa explains its efforts to customers for their understanding and that both parties work together for maintaining the security level.

Yokogawa supports customers' activities to maintain the security level of their production environments through its products and services. While continuing this support, Yokogawa must keep pace with changes in society and technology. For this purpose, Yokogawa will collaborate with external organizations and institutions for strengthening the security of its products and services.

REFERENCES

(1) Nobutaka Oguma, Stuxnet - the first malware targeting control systems -, JPCERT/CC, 2011 in Japanese, https://www.jpcert.or.jp/ics/2011/20110210-oguma.pdf
(2) Minister of Economy, Trade and Industry, Directive Number 110, Standards for Handling Software Vulnerability Information and Others, Ministry of Economy, Trade and Industry, 2014 in Japanese, http://www.meti.go.jp/policy/netsecurity/downloadfiles/140514kaiseikokuji.pdf
(3) Workshop for handling vulnerability information on information systems and others, Information Security Early Warning Partnership Guideline, 8th edition, Information-technology Promotion Agency, 2014 in Japanese, https://www.ipa.go.jp/files/000044732.pdf