Ensuring Information Security in the Sumitomo Chemical Group

Sumitomo Chemical Systems Service Co., Ltd.
IT Strategy Office
Kazuyo NAKAI
Takayuki KANEHIRA
Sumi SHIMIZU

Many companies have conducted various activities to ensure information security since utilization of information technology became one of the ways to support business. However, changes in the threats surrounding the current IT environment and changes in the environment such as IT technology and globalization also have an effect on revisions of international standards, and so security measures in companies need to be reexamined. This report includes a discussion of information security in the Sumitomo Chemical Group.

This paper is translated from R&D Report, "SUMITOMO KAGAKU", vol. 2014.

Introduction

Aiming for further growth as a global chemical company, we at the Sumitomo Chemical Group are rapidly establishing the foundation for IT that will support our global consolidated management. As part of this effort, we have created an environment in which the companies of the Group (including overseas affiliates) conduct business on the same network. Moreover, we have firmly established a basic information security policy and have promoted the implementation of information-security measures with respect to Sumitomo Chemical Co., Ltd., and all other member companies. However, threats from outside continue to increase each year, and they target our information system. It is therefore necessary to have measures to continuously maintain information security in order to ensure global consolidated management.

We at the Sumitomo Chemical Group place a high value on compliance management and CSR management. Accordingly, the maintenance of information security is one of our business challenges. Thus we have actively promoted group-wide information security management.

This paper will introduce the approach taken at the Sumitomo Chemical Group by explaining the method for maintenance of information security under the group management, the related issues and countermeasures, mainly from the perspective of management.

Changes in Threats

It is said that criminal activities in the IT environment—mainly on the Internet—have become extremely sophisticated. Numerous reported information-security-related incidents indicate that this is true. Reportedly, in such crimes the means and objectives are becoming more diverse. As the target range and types continue to expand, IT-related information-security risk becomes ever higher.

We will look back at the changes in threats in the IT environment and describe the company trend in response to such threats.[1)]

1. Changes in Cyber-attacks

(1) Changes in Threats Derived from the Establishment of the Internet

Broadband network operations became widespread in the year 2000, and subsequently the Internet became fully utilized by companies and private individuals. During the second half of 2000, Internet-based direct business transactions such as online shopping became popular in society.

As the IT environment advances, the threats to it change form.

Along with the expansion of Internet usage, the range of attacks using malware such as computer viruses and worms*[1] via the Internet has also expanded. It is well known that worms such as CodeRed*[2], Nimda*[3] and

SQLSlammer[*4] have brought tremendous damage to numerous companies. Although at first those attacks seemed more like crimes committed merely for personal pleasure with the purpose of being conspicuous, consequent with the popularization of commercial transactions on the Internet there has been an increase in the number of attacks intended to directly rob people of their money.

The Act on the Protection of Personal Information was enacted in 2005, thus making the management of personal information–which is useful for criminals in the virtual and real worlds–more difficult. Consequently, personal information became even more valuable in the black market, resulting in greater numbers of attacks aimed at exploitation.

As the attackers' objectives have shifted toward money, the means of attack have become more ingenious. In addition to the invasion method by which one takes advantage of technology and the vulnerability of the IT area, criminals have gone on rampages, attacking people by playing tricks on them and taking advantage of their vulnerability. One example is the "targeted attack mails." In this method a criminal impersonates one of a victim's acquaintances in a clever manner and sends an e-mail through which the victim is skillfully persuaded to activate a malware or a website.

(2) New IT Applications and Attacks Targeting Markets and Military Network Systems

Given the establishment of wireless LAN, smart devices and cloud services, recent years have seen significant advancement in online systematization, particularly in the civic and social realms. Moreover, general-purpose techniques are becoming more widely adopted in control systems, for which special infrastructures were traditionally utilized, thus causing important infrastructures such as manufacturing plants and power-generation facilities to be exposed to criminal threats, as with the general IT assets.

As the number of attractive targets increases, the means of attack also advance. Once attackers have created tools with which to identify vulnerabilities and the methods of attack, they will begin selling them in the black market, thus enabling anyone to effectively and successfully make attacks without the need for special technology or even a significant amount of time.

The previously known vulnerabilities easily allow invasions, and thus the frequency of "zero-day" attacks[*5] increases year by year. Regarding the targeted attack, which goes after one or more specific organizations, it has been reported that in some cases criminals attack with circumspection using several methods–such as e-mail attacks, infection with malware and exploitation of information–in order to invade deeper and remotely control computers in the organization, doing so through multiple stages until their purposes are accomplished. In March 2013 a large-scale targeted attack occurred in Korea. As a result of the attack, three banks and three broadcasting stations were forced to cease their financial transactions and broadcasting operations, respectively. Reportedly, several attacks had been made over the nine-month period before the incident, demonstrating the attacker's carefulness and persistence. It has also been reported that the number of attacks on control systems of important infrastructure continues to increase. This is a threat that shouldn't be ignored by manufacturers who operate plants. Furthermore, other cases of "hacktivism," by which hackers invade the websites of public and specific organizations in order to widely spread their principles and positions, have been reported, along with the cyber-terrorism aimed at countries. Thus the cyber-attack is used as a means of defense/offense over ideologies and political conflicts. The U.S. Department of Defense refers to cyberspace

[*1] Worm: Standalone malware that replicates itself and infects other computers.

[*2] CodeRed: One of the self-replicating computer worms that spread by taking advantage of the vulnerability of Microsoft products. CodeRed spread throughout the world in 2001, and due to its vigorous attacks the Internet became temporarily inaccessible at one point.

[*3] Nimda: A worm that infects other computers by taking advantage of the vulnerability of Microsoft products. This is an initial-type worm with multiple infection routes such as browsers, web servers and e-mails. It was spread in 2001, and the infection method–like that of CodeRed–targeted web servers.

[*4] SQLSlammer: One of the self-replicating computer worms that take advantage of the vulnerability of the Microsoft database engine. Immediately after its discovery in 2003, the worm explosively spread infections within only about ten minutes, causing worldwide network damage.

[*5] Zero-day attack: An attack that exploits a previously unknown vulnerability in a computer application, one that developers have not had time to address and patch. The attacker finds vulnerability in the software and begins to attack. It is called a "zero-day" attack because the programmer has no time to fix the flaw. Because an attack will be made when the software vendor or the victim company has no immediate countermeasure, there is a high risk that damage will occur.

as the “fifth battlefield” following the land, the seas, the sky and space. It has now grown to the point that each country has no choice but to undertake countermeasures.

2. Countermeasures Employed by Companies

Along with the changes in threats, the countermeasures undertaken by companies have shifted from topical measures focusing on technical aspects to a more systematic approach, through which priority is placed on raising employee awareness and achieving sustainable implementation.

Initially, with the popularization of the Internet, the mainstream was to introduce security products such as firewalls (which block invasion on the network from outside) and antivirus software. Subsequently, since the second half of 2000, due to progress in the establishment of security standards and regulations such as the ISMS Family of Standards and the Japanese SOX Act, as well as other reasons, more comprehensive management as an organization became necessary. Additionally, in response to more intensified threats to control systems as described previously, a unique management standard called CSMS has been defined as an international standard by taking into account the characteristics of control systems. The details of those standards will be discussed later in this paper.

The leakage of client information and attacks on control systems can also have serious consequences outside the company. There has been a case in which the effects of the attack on one weak overseas affiliate eventually spread to the entire group and various clients, causing enormous damage. Thus the purpose of the company’s information-security measures is not only to protect its own business but also to fulfill the need for social responsibility and make any threat to those measures one of the important management risks. For global companies that conduct group operations, it is urgently necessary to establish information-security measures across borders by bringing one’s entire business group into perspective.

Information Security Management

Companies have examined and implemented various types of information-security measures along with the changes in threats to information security and the establishment of laws and regulations. In order to establish and implement such measures properly, companies have relied on the ISMS Family of Standards, including ISO27000.

This paper will describe the concept of information security management defined in the ISMS Family of Standards as well as the typical information security management measures.

1. Definition of Information Security

“Security” means “protection” as a concept and a course of action.

A company must protect not only its “information” and “assets,” which are indispensable as the operational resources, but also the “company brand,” which has been created over many years, against various types of sophisticated threats as described elsewhere in this paper.

The reason for the above is that it’s now difficult to imagine any company conducting business without IT. Therefore, while business opportunities can be further expanded through the safe, proactive use of IT, it also contains a risk that once a company’s credibility has been lost in society due to the misuse or abuse of IT, it may become difficult to sustain operations. Furthermore, one can’t deny the risk of being framed as an offender by a malicious attacker.

It is therefore essential to determine who or which organization will establish and thoroughly implement a countermeasure suitable for each risk it faces. This sequence of activities is referred to as “information security management.”

“Information security” means that information is managed in such a way that it can be safely used even though it is under protection. The state in which security is ensured means the state in which the confidentiality, integrity and availability of information are appropriately maintained and managed.

Information security is more specifically defined in **Table 1**.

Table 1 3 elements of information security

3 elements of information security	Definition
Confidentiality	Only authorized people can appropriately use information asset.
Integrity	Information asset is not falsified by unauthorized persons.
Availability	Authorized individuals can use information asset when necessary.

The framework of information system management relies on the international information security standard "ISO/IEC27001:2013 Information Security Management System: Requirements." Furthermore, specific management measures for ensuring information security are divided into 14 categories in "Control Category Based on ISO/IEC 27002:2013," as shown in **Table 2**.

Table 2 Control category based on ISO/IEC 27002 : 2013 [2)]

Control category
Information security policies
Organization of information security
Human resource security
Asset management
Access control
Cryptography
Physical and environmental security
Operations security
Communications security
System acquisition, development and maintenance
Supplier relationships
Information security incident management
Information security aspects of business continuity management
Compliance

Actually, companies aren't required to implement all countermeasures equally at the same level in order to protect every single piece of information. Instead, it is important to undertake the optimal measures in consideration of cost-effectiveness, taking into account the value of information and the degree of impact if such a threat is made. In some cases business judgment may be required.

2. Typical Management Measures Described in ISO/IEC 27002:2013

The information-security measures can be categorized as shown in **Table 2**. Generally, however, they can be roughly divided into four categories as shown in **Table 3**: organized measures; human measures; physical measures; and technical measures.

Although numerous technical measures are shown in the table, they alone are not sufficient. Considering the changes in threat to information security, organized measures and human measures aimed at comprehensive management are becoming more important than technical measures.

Additionally, more specific explanations of management measures described in **Table 3** are as follows:

Organized Measures

It is necessary to determine rules regarding information security, obtain approval from the management, and disseminate such rules throughout the company and all parties involved. Moreover, it's essential that the management be responsible for information security and thereby promote it with a top-down approach, and that the person in charge of each department monitors and adjusts the implementation.

Human Measures

It is necessary to periodically provide employees with education intended to build their awareness of information security.

Physical Measures

In order to maintain security at an information-processing facility, it is necessary to create physical bound-

Table 3 Typical measures of ISO/IEC 27002 : 2013 [3)]

	Contents	Control
Organized Measures	5.1.1 Policies for information security	A set of policies for information security should be defined, approved by management, published and communicated to employees and relevant external parties.
	6.1.1 Information security roles and responsibilities	All information security responsibilities should be defined and allocated.
Human measures	7.2.2 Information security awareness, education and training	All employees of the organization and, where relevant, contractors should receive appropriate awareness education and training and regular updates in organizational policies and procedures, as relevant for their job function.
Physical measures	11.1.1 Physical security perimeter	Security perimeters should be defined and used to protect areas that contain either sensitive or critical information and information processing facilities.
Technical measures	12.2.1 Controls against malware	Detection, prevention and recovery controls to protect against malware should be implemented, combined with appropriate user awareness.

aries in information security zones, such as partitions and individual authentication doors.

Technical Measures

It is necessary to introduce antivirus software, allow users to become aware of its importance and of the updating of pattern files, and determine the procedures with which to respond to an abnormal situation.

3. Key Points of Revisions Made to ISO/IEC 27001:2013 and ISO/IEC 27002:2013

ISO/IEC 27001:2013 and ISO/IEC 27002:2013 were issued on October 1, 2013. Neither of them was intended to revise the basic approach shown in the existing standards, so the majority of their content is succeeded from the 2005 versions. However, along with the standardization of the standard structure of the other ISO management systems, those standards have been enhanced and clarified, being revised in order to accommodate changes in technology and the information environment.

The key points of such revisions are as follows:

ISO/IEC 27001:2013

- Application of standardization of the management system standards

Many companies adopt various management standards such as ISO 9001:2008 for product quality and ISO 14001:2004 for the information environment.

Therefore, in order to improve the integrity among management systems and thereby minimize the burden on each organization, the use of items such as “upper-rank structure,” “common text” and “common term definition” are imposed upon companies.

- Responding to the new business and system environments

It is no exaggeration to say that we now live in a risk-management society. Because it’s impossible to eliminate risk entirely, the question of how to control risks must be answered with respect to company activities.

Principally, the concept of risk is introduced to all management systems, which is based on the “ISO 31000:2009 Risk Management: Principles and Guidelines.”

It is also hoped that through the introduction of “information-security objectives,” which clearly indicates the organizational policy, each company will advocate and thoroughly accomplish those objectives by setting the goals to be used as milestones in such efforts, in order for the management and all other employees throughout the organization to contribute to company activities.

ISO/IEC 27002:2013

- Responding to changes in the information environment and information management/handling technology within the organization

Given the increased frequency of outsourcing, we are now in an environment in which one can’t say that employees alone constitute the circle of parties who often or regularly use the information owned by one’s organization. Therefore, management measures targeting outsourcees have been incorporated in the standards.

Additionally, various service applications including cloud services are described in the section on suppliers.

- The usability of those standards has been enhanced, aiming for a wider range of users.

Although guidelines are provided for information security management measures in those standards, technical details have been deleted. Such guidelines are more focused toward general interpretations of measures, so it is recommended that users refer to general interpretations of measures and other standards for technical details.

4. Shifting from PDCA to CAPD

The PDCA cycle (Plan → Do → Check → Act) has been established as a basis of management-system-related activities.

Recently, however, the use of the CAPD cycle is being actively advocated not only in the information security area but also in the areas of education, disaster prevention and marketing. This is based on the assumption that planning and implementing measures without thorough understanding of the current situation will not produce adequate effects.

First, in the CAPD cycle risks are visualized by accurately understanding the organization’s current situation. Based on that visualization, effective measures will be discussed. Needless to say, when the urgency is high, measures will be undertaken immediately. Lastly, measures suitable for each organization will be planned and implemented. In the area of information security, for example, the following activities will be undertaken for each phase:

- C: Visualization of risks through audit and self-inspection

- A: Examination of required measures based on the result of the risk analysis
- P: Planning of the introduction of measures suitable for risks
- D: Implementation of the measures

It is crucial, with respect to the PDCA or CAPD cycles, that one properly conduct the activities in each phase. As described above, international standards such as the ISMS Family of Standards and the concept of management will continue to evolve along with the changes in technologies and the information environment.

Control-System Security

It has been recognized that a control system has a unique, specialized structure and it is always "safe." However, as a result of the continuous shift toward networking and open/generalized systems, the myth of safety in control systems has collapsed, as seen in the case of the system damage experienced at an Iranian nuclear fuel facility due to Stuxnet.*6

It is necessary to tackle information-security measures for control systems based on the thorough understanding of such a trend.

1. Trend in Security Incidents

Subsequent to the Stuxnet incident, there has been no report regarding a serious cyber-attack on a control system. However, the threat has increased as seen in the case of the declared attack in Israel on the road-tunnel management system, which resulted in a roadblock that lasted more than eight hours.[4)] The U.S. Department of Homeland Security has also made known its concerns regarding more intensified, targeted cyber-attacks on important infrastructure providers.

2. Directivity of Control-System Security Measures

Regarding the directivity of control-system security measures, the CSMS (Cyber Security Management System) has been established.

The international standards of the CSMS are defined in the IEC62443 series. Although IEC62443-2-1 has its own control-system security requirements as shown in the **Tables 4** and **5**, it also has requirements in common with the ISMS Family of Standards (ISO/IEC27001 and others).

Table 4 Requirement analyses of IEC62443-2-1 and ISO/IEC27001[5)]

	IEC62443-2-1
Number of requirement	126
Unique requirement	26
Common requirement	100

Table 5 Unique requirement of IEC62443-2-1

	Number of requirement
Risk identification, classification and assessment	4
Security policy, organization, and awareness	3
Personnel security	2
Physical and environmental security	2
Access control	7
System development and maintenance	3
Information and document management	1
Incident planning and response	2
Review, improve and maintain the CSMS	2

3. Tackling Security Measures

As described in the previous section, it is easier to understand control-system security as follows: It has a two-story structure, and the distinctive factors unique to control systems (such factors being distinct from those of information-system security) are added as the CSMS on top of information-system security, which serves as the base. Because there are differences between an information system and a control system as shown in **Table 6**, previously there weren't many opportunities for the Information System Department and Engineering/Manufacturing Departments to collaborate. However, the myth that control systems are safe has been overturned in the wake of several incidents (e.g., the attack on the Iranian nuclear power plant), including the Korean case in which a nuclear power plant network system was cyber-attacked by North Korea, resulting in the complete isolation of the power plant from the network.4) Such threats are increasing,

*6 Stuxnet: One of the computer viruses targeting control systems. Discovered in the Middle East (mainly in Iran) in 2010, it affected an Iranian nuclear power plant.

and they can lead to serious incidents. It is important that all departments cooperate with each other without worrying about the areas of their previous responsibilities, so that the matter of control-system security can be urgently tackled.

Table 6 Difference between information system and a control system

	Information system	Control system
Priority	C: Confidentiality I: Integrity A: Availability	A: Availability I: Integrity C: Confidentiality
Renewal Term	3 – 5 years	10 – 20 years
Department	Information System Department	Engineering Works/Producing Department
Required Performance	Non-real-time Delay and a stop are permitted.	Real Time Delay and a stop are fatal.
Threats and Risks	Loss of data and business opportunities	Loss of human life, equipment, and products

Challenges in Information Security for Manufacturers Engaged in Global Operations

Given the existence of group companies, in which not only one's own company but also any member company is invaded by an attacker, there is a risk that the effect will spread throughout the group. The manufacturer whose main operation method is B to B (Business to Business) can't escape this threat either, as its control systems are also exposed to such threats.

The following section will explore the challenges facing global companies to maintain information security by controlling the entire group. We will also provide examples of our efforts to protect the information system at Sumitomo Chemical Group.

1. Global Control

(1) Framework for Control [6)]

The need to properly manage information-security risk requires that we not only introduce solution products but also establish a framework of management, as stipulated in the aforementioned standards. Moreover, we must implement measures continuously with the framework. In other words, it is necessary to follow the PDCA cycle by establishing rules, clarifying roles and responsibilities in the system as well as by ensuring and promoting the implementation of risk-management measures based on the aforementioned rules, roles and responsibilities.

However, the risks that companies face are also present in various areas other than information security. It is therefore necessary to allocate investments to each countermeasure against those risks, based on the business management policy. Furthermore, measures must be planned and promoted in accordance with a cross-sectional understanding of various risks, and the management must be able to understand and evaluate the status and results. In order to thoroughly improve such efforts and increase the awareness of information security throughout the organization, management must take the initiative.

(2) Framework at Sumitomo Chemical Group

Sumitomo Chemical Group has, in recent years, enhanced the promotion of the information security management activities commonly conducted within the Group under the leadership of the Information System Department at our headquarters. We are implementing the company-wide risk management through the establishment of Head Departments for each risk under the internal control committee comprised within the management. Thus information system security has been positioned as one of the major risks, and the measures are undertaken with the management's initiative.

First, in 2005 we established the information-system security policy at our headquarters. We then created the information system security management system, introduced/operated the information system, and determined and implemented the basic standards for the promotion of information-system security. Gradually we have ordered each group company to create and operate the similar rules and systems, and we are monitoring the progress of its establishment and operation from headquarters.

Furthermore, in response to increased risks as described at the beginning of this paper, we are striving to make the current rules of headquarters common throughout the Group in order to enhance the framework and ensure quick response to changes. By doing so, we will clearly present the requirements to each company in the Group, thereby enabling the yardstick evaluation of progress in all the companies of the Group. By maintaining and managing those rules at the Information System Department in our headquarters, we will enable the Group to respond to changes in external threats.

Additionally, we are planning to determine a common self-inspection scheme as a monitoring/evaluation activity, which will be voluntarily implemented on a yearly basis by each company in the Group. The objectives are that not only the Information System Department of our headquarters will present rules and inspect compliance status of the Group companies but also that each company in the Group will independently follow the CAPD cycle of self-inspection, understand issues, devise an improvement plan and implement that plan.

(3) Efforts in Controlling Overseas Group Companies

Companies that conduct global operations often find it difficult to supervise their overseas business bases from remote headquarters. As mentioned previously, there have been instances in which such weaknesses have been exploited. For that reason the proper management of overseas bases is an important issue for the information security of such a business group.

We at Sumitomo Chemical Group have established regional headquarters in the major overseas business regions and positioned IT-dedicated staff. Thus we control the IT management of our group companies and provide guidance for the promotion of information security within the region. However, in some regions it is difficult to obtain IT staff who would promote information security of each company in the Group. In other cases high mobility in employment can be a problem: The IT staff person who was finally obtained after a struggle may quit once his/her skill has reached the required level. So, in many cases information security activities can only progress slowly merely with efforts undertaken by the Sumitomo Chemical headquarters and the regional headquarters. Additionally, there is a concern that even if information security is outsourced to an external IT vendor and a security-solution product has been introduced, if the vendor isn't adequately controlled, the product may not be used appropriately. Furthermore, if each company in the Group individually procure resources or obtain solutions, the duplication of running cost may occur when the solution is put into the perspective of the entire Group.

Accordingly, we at Sumitomo Chemical Group are about to launch the common IT services for each region. It is aimed to enable each company in the Group, which is struggling to manage IT on its own, to be able to maintain a consistent level of information security with the optimum cost by providing the basic IT infrastructure, including IT management service.

In regions such as Southeast Asia, which consist of many different countries and languages, we attempt to introduce a system in which the following roles are allocated to the most suitable parties: control of the entire IT services; IT management/service-desk work of each

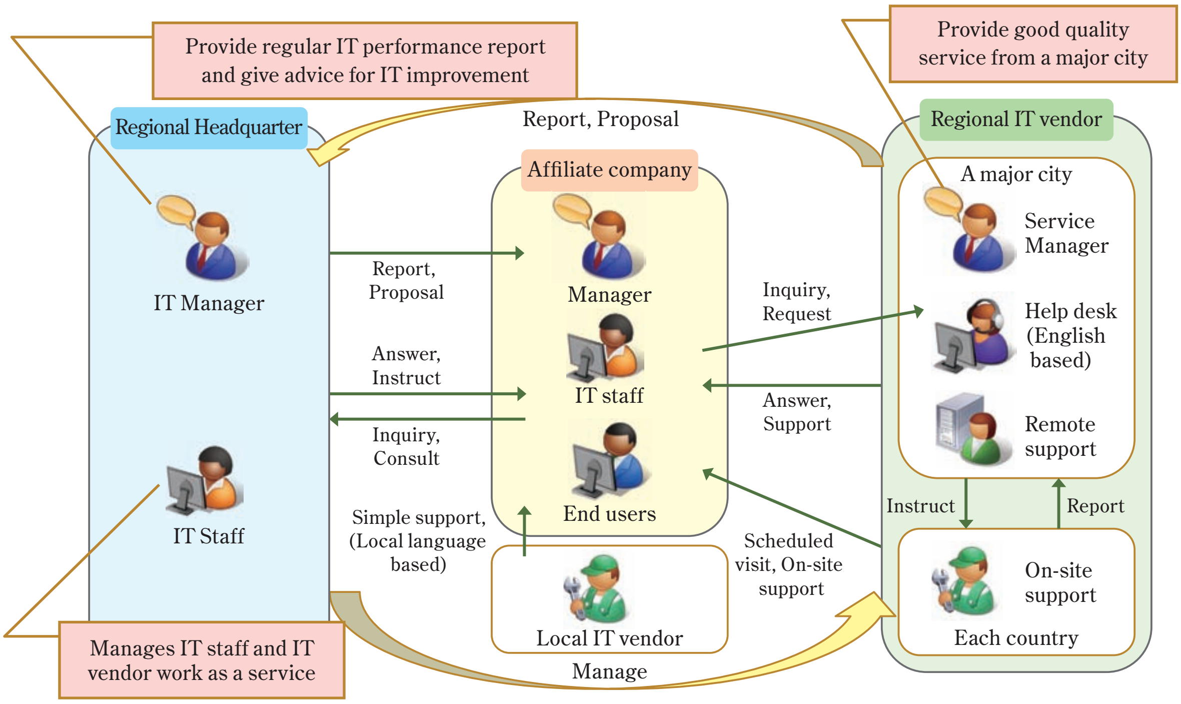

Fig. 1 Operational image of the Regional IT Service

company in the Group that utilizes the IT services; and actual IT management work at the local sites. The regional headquarters will be responsible for the control of the IT services in their entirety, and a leading local vendor who can cover the entire region will take care of management/service-desk work. Regarding the local work, the idea is that for ones that require advanced skills, the leading vendor will give directives to the local site of each country, and for ones that are relatively easy, the local vendors used by each company in the Group will be used as before (**Fig. 1**). Through this method, we will be able to handle multiple languages and achieve fast on-site work, while at the same time maintaining the quality of responses to user needs and IT management. Furthermore, by making the most of local vendors, running cost can be minimized.

Although part of such common IT services is already in operation, we must fully expand these activities to each region. Upon expansion of the IT service, it is our challenge for the future to precisely comply with laws and regulations of various countries of the world.

2. To Create Management/Service Culture of the Entire Group

Although the framework of IT management and the common IT services have been firmly established, introducing a new service or undertaking countermeasures against new problems discovered during the monitoring activity can be a burden on each company in the Group. Needless to say, each company in the Group wants to minimize information security cost. Particularly, the requirement of cost reduction is severe due to the difficulty facing the petrochemical industry in recent years. It can be assumed that even though the top-down approach is promoted in the company-wide risk management organization, if risks are not accurately understood, appropriate investment decision can't be made because the cost and security derived from this cost must be balanced.

In order to avoid such a situation, education and enlightenment programs must be provided on a regular basis to Group companies' higher-ranking employees, who make investment decisions, so that they will accurately understand threats and the importance of information security.

Moreover, before employees will be promoted to higher ranking positions that are closer to the management, we will provide them opportunities to thoroughly understand precautions to be undertaken for basic use of the information system, as well as responsibilities suitable for their positions, on a regular basis and every time their positions are changed. It can be assumed that doing so will enable us to manage information security more smoothly as an organization, and thereby minimizing the cost of information-security measures.

In the meantime, in order to have each company in the Group to accept and implement information-security measures, we will continue to strive not only to explain the necessity of information security to them, but also consistently provide more attractive services and put effort on cost reduction. As the only information system company in the Group, our challenge is to explain information-security measures to each company in the Group in details and develop acceptable scenarios.

Conclusion

This paper has explained the trends and threats in the IT environment along with the typical methods by which companies seek to manage information-security risks. Moreover, we have introduced challenges facing global companies, using cases from the Sumitomo Chemical Group as examples.

IT has evolved significantly. Thus it has enhanced the convenience of our daily social life and continued to transform our work environment. In the economic environment, in which the competition has intensified due to globalization, companies should not hesitate to make the most of their IT in order to expedite the business process and increase their corporate value.

The proper understanding of one's attackers and threats, along with the appropriate management of information security, is now mandatory for any company that seeks to continue and thrive. Accordingly, in order to continue provide products and technologies that contribute to solving problems facing international society in various areas such as resources, energy, food and the environment, we at Sumitomo Chemical Systems Services will establish information security management within the Sumitomo Chemical Group.

References

1) "10 Major Security Threats 2013 ~ They Are About To Get You and You Just Don't Know Yet ~", Information-technology Promotion Agency, Japan (ISEC/IPA) (2013).

2) "ISO/IEC 27002:2013 Information technology – Security techniques - Code of practice for information security controls" (2013), piii.
3) "ISO/IEC 27002:2013 Information technology – Security techniques - Code of practice for information security controls" (2013), p2.
4) Toshio Miyaji, "Status and Prospects on ICS Security Looking back over this one year", JPCERT/CC (2014), p.11, http://www.jpcert.or.jp/ics/2014/20140205ICSC JPCERTCC_Miyachi.pdf (Retrieved 2014/3/24).
5) Seigyo shisutemu ni okeru sekyuritei manejimento shisutem no kouchiku ni mukete – IEC62443-2-1 no Katsuyou no apurochi ["Building security management systems with control systems - Approaches to application of IEC62443-2-1"], Information-technology Promotion Agency (2013), p. 16. http://www.ipa.go.jp/files/000014265.pdf (Retrieved 2014/3/24).
6) Jouhou sekyuritei gabanansu dounyuu gaidansu ["Guide for introducing information security governance"], Japanese Ministry of Economy, Trade and Industry (2009) http://www.meti.go.jp/policy/netsecurity/downloadfiles/securty_gov_guidelines.pdf (Retrieved 2014/3/24).

PROFILE

Kazuyo NAKAI

Sumitomo Chemical Systems Service Co., Ltd.
IT Strategy Office

Sumi SHIMIZU

Sumitomo Chemical Systems Service Co., Ltd.
IT Strategy Office
Senior Manager

Takayuki KANEHIRA

Sumitomo Chemical Systems Service Co., Ltd.
IT Strategy Office