Business Management and Cybersecurity

Digital Resiliency for Executives

Shinichi Yokohama
(shinichi.yokohama.pa@hco.ntt.co.jp)
Head,
Cyber Security Integration
NTT Corporation

Table of Contents

Introduction

The day the world cried

On Friday, May 12, 2017, ransomware dubbed "WannaCry" infected computers in Europe and then spread worldwide. The term "ransomware" implies a demand for ransom payments. This type of malware (software such as viruses used with ill intent) encrypts data within personal computers or servers, locking it until ransom is paid, at which time the encryption is reversed and the data freed. The encrypted data becomes the "hostage" and the money is the "ransom," explaining the nomenclature of this type of malware.

Ransomware had been an issue for some years, but the sheer scale of WannaCry, which infected some 200,000 computers in 150 nations worldwide by May 16, 2017, prompted mass media and others to spotlight this emerging crime. Around noon local UK time on May 12th, the computer system serving Britain's National Health Service (NHS) became infected, causing over 20 hospitals to cancel surgery and exams, and interrupting ambulance service. A ripple effect promptly followed across Europe, with reports of similar damage emerging next from the US, and then from Asia.

Due to the time difference, most of Japan's companies had already wrapped up their workweek on Friday by the time the cyberattack hit. Moreover, the Information-technology Promotion Agency (IPA) overseen by Japan's Ministry of Economy, Trade, and Industry (METI) successfully dispatched a weekend alert forewarning companies about their computers, e-mail, and information systems, minimizing damage from the infection on Monday morning. Nevertheless, automobile manufacturers' factory computers became infected, delaying outbound shipments, while electrical appliance manufacturers suffered breakdowns in systems governing e-mail and incoming orders, as the locations in the Western hemisphere were the infection sources. Many Asian nations were greatly victimized, with the largest number of infected devices reportedly occurring in China, the US, Russia, and India, in decreasing order.

The government and a hacker group facilitated WannaCry

The WannaCry attack was distinctive in its scale, geographic reach, and origin. It utilized EternalBlue as an exploit, which is basically an attack tool literally exploiting a vulnerability in certain software or data for unauthorized access and

often malicious intent. EternalBlue was developed by the National Security Agency (NSA) in the US and propagated through a vulnerability in the Microsoft Windows operating system. The hacker group "Shadow Brokers" stole EternalBlue from the NSA and made it available on the Internet, leading an unidentified party to reprocess it into the ransomware WannaCry which ultimately generated the criminal attack.

A variety of circumstantial factors thus intertwined, leading to the WannaCry attack. This is what happened:

- A vulnerability in the Windows OS was the originating factor.
- The NSA capitalized on this vulnerability, creating the attack software.
- A hacker group stole the attack software, posting it on the Internet as EternalBlue.
- An unidentified person or group weaponize EternalBlue, resulting in WannaCry.
- It remains unknown whether WannaCry's creator, or another individual, perpetrated the ultimate crime.

Each of these factors introduces further questions. First, why was there a gaping vulnerability in Windows OS, a commercial product? Did Microsoft commence sale of a defective product? Assuming, for the sake of argument, that the vulnerability was discovered after product launch, did the company not fully correct it?

Furthermore, why did the NSA capitalize on the vulnerability, turning it into an exploit? Why did the hacker group which stole it then post the find on the Internet? If the purpose was to censure the NSA, why did the group not find a more appropriate method than posting the exploit on the Internet? Finally, questions surface surrounding the creation and subsequent usage of WannaCry: who made the ransomware, and who launched it?

Experts debated these issues, one by one, yielding a hypothesis as to what had occurred. (On December 19, 2017, the US government announced that North Korea was implicated in the WannaCry attack.) However, the purpose of this book is not to elucidate the consensus of these experts. It is rather to emphasize that cybersecurity is not merely a technological problem involving networks and software, but also a social one encompassing economic and political factors, among others.

Business Executives may leave the technical details to others

WannaCry was one incident among many; reports of cyberattacks abound, both

in Japan and elsewhere. Such events are becoming more frequent and familiar, and their damage is driving home the point among Japanese business executives that cybersecurity is an issue they must face. However, the WannaCry example illuminates the complex entanglements in this challenge. Some may be difficult for a single company to address on its own. Cybersecurity thus represents an intimidating challenge for senior management.

The technical side alone covers a broad spectrum. Many factors are involved: telecommunication equipment including networks serving the Internet and in-house LAN, routers and like devices, servers and computers, and devices such as smartphones, as well as software, from basic operating systems (OS) such as Windows OS to a wide range of applications. And to that, one must add factory line management and store point-of-sale (POS) systems. Cybersecurity is distinctively cross-disciplinary in the field of computer science. Experts conversant in all areas are few and far between, making it difficult to reach a well-balanced, cross-disciplinary perspective even among a team of in-house engineers.

Looking beyond the technical side complicates the issue even further. Coping with realities like the international political situation and solutions to crimes initiated overseas is more than a single company can handle on its own. Moreover, maintaining and safeguarding cybersecurity is a broad topic, considering all that it encompasses: client and employee privacy protection, internal controls extending to subsidiaries and group companies, contracts with business partners, public relations, and working from home.

It seems practically impossible for busy executives to grasp the complex web of factors involved in cybersecurity. Though some may find it ludicrous, I suggest that senior management need not understand the totality of cybersecurity in order to deal with it.

Briefing business executives on the essence of cybersecurity

Even so, there is no denying that those standing on the sidelines may invite serious consequences. In May 2017, the CEO of US credit reporting company Equifax was driven to resign over an identity theft incident impacting 140 million customers. To ensure that their business does not suffer a similar fate, upper management should avoid getting bogged down with details, and instead focus on grasping the essence of cybersecurity, while leaving the particulars to trusted employees.

Publications on cybersecurity abound, but most probe the technical side or, if

not that, then the argument for national security, with few identifiable as a management book. This publication, on the other hand, addresses complex cybersecurity issues from a upper management standpoint. For that reason, its purpose is to brief executives on the essence of cybersecurity.

Managing executives and board members who have an awareness of the cybersecurity problem, but find it complex and intimidating, may find this book useful. I suggest that they absorb the key message introducing in each chapter, and then read the chapters which they find intriguing.

Resilience may be defined as tenacity, but it also connotes the ability to endure transformation of shape or substance from an external source and accomplish restoration of stability. The subtitle of this book—Digital Resilience—suggests that the time has come when companies in today's digitized economic society must embrace a risk management practice unlike anything they have yet experienced.

Overview

The book is comprised of six chapters, as follows:

Chapter 1, "Business Management and Cybersecurity," presents examples demonstrating the inseparability of these dual activities in the current age of digitized business.

Cybersecurity falls under the umbrella of corporate risk management, in which the standard approach is to prioritize initiatives according to risk appetite. Digitization of value-added assets is evolving and permeating every corner of business operations, rendering cybersecurity strategy inseparable from management strategy and impacting corporate competitiveness.

Chapter 2, "Revisiting Cybersecurity as a Management Issue," examines the three reasons cybersecurity is a management issue:

1. There is a tendency to fixate solely on the threat of data breaches in Japan, but from a management standpoint, the endangerment of business continuity is the real worry.
2. The trust of stakeholders, such as clients, business partners, shareholders, and authorities, is what lies in the balance.
3. Cybersecurity is the foundation for activating digital innovation, the key to corporate growth.

Chapter 3, "Imperative Actions for Business Executives," enumerates the three steps management should take:

1. Managers should prioritize target areas requiring protection and

implement layered defense.

2. As perfect protection is impossible, managers must build organizational capability for quick detection, response, and recovery on the premise of a security breach.
3. (1) and (2) above should be reviewed periodically in meetings among business executives as well as in corporate board meetings.

Chapter 4, "Collaboration with Other Companies," discusses ways firms can work together to overcome the universal corporate challenge of cybersecurity human resource insufficiency, such as information sharing and human resource development. Such intra-industry collaboration is a practical first step, as issues, information, and human resource needs are similar. Chapter 4 includes examples of information sharing and capacity building, both in Japan and abroad.

Chapter 5, "Global Management," points to the necessity for all companies, not just multinationals, to recognize their need to incorporate a global perspective on cybersecurity. In-house global security governance is an imperative for companies expanding overseas, as are protection of supply chain cybersecurity and international cooperation on policy harmonization.

Chapter 6, "Collaboration with Government," demonstrates that instead of passively awaiting policy, firms should proactively petition and pressure the government for measures answering industry needs. This is already happening in the domain of human resource development, and this chapter proposes that further expansion into the information sharing domain is a must. Cybersecurity is a public goods service, but companies must take a proactive stance in its creation, implementation, and maintenance.

This book sets out to present executives with the essence of cybersecurity from a business management perspective, and in the process, hopefully to contribute to cybersecurity initiatives undertaken by all industries.

Chapter 1: Business Management and Cybersecurity

The progressive digitization of valued-added corporate assets such as intellectual property and brands also elevate digitization of corporate risk. Maintaining cybersecurity means management of digitized corporate risk, and is inseparable from management strategy. The success or failure of cybersecurity management will differentiate business competitiveness within the digital economy.

1. Assessing economic damage

Cybersecurity incidents and related breaches are reported almost daily in Japan and abroad, but how much financial damage do they wreak? There are no formal assessments from governments or other official organizations, but think tanks and such groups have published survey results. The Center for Strategy and International Studies (CSIS), an American think tank, calculated total global damage from cybercrime as somewhere between $375 and $575 billion (Net Losses: Estimating the Global Cost of Cybercrime). The figure roughly equates to 0.5-0.8% of the world's gross domestic product (GDP) of $70 trillion. As CSIS's report appeared in 2014, one assumes a higher percentage today, as the global economy has shifted increasingly toward an online basis, with a corresponding uptick in cybercrime. CSIS issued its latest report, Economic Impact of Cybercrime – No Slowing Down, on February 21, 2018), revising its estimate of worldwide economic damage upward to between $445 and $600 billion.

The CSIS report shows the estimated cost breakdown by nation (Figure 1-1).

Comparing figures against GDP, Japan comes out lowest among G20 nations, with only 0.02%. The survey analysts concluded that Japan's low ranking was probably due to underreporting by Japanese corporations. This would explain why Japan seemed to suffer less economic damage from cybercrime. Japan's GDP is about 500 trillion yen, 0.02% of which is about 100 billion yen. If Japan suffered as much as other nations on average, the figure would be about 0.5-0.8% of 500 trillion yen, or roughly 2.5-4 trillion yen.

The report's preliminary calculations of economic damage reflect only on the corporate sector. The assessed damage extends beyond financial loss to include other areas impacting business activities, such as theft of intellectual property and business information, lost business opportunities, brand and other recovery costs, third party injury, and ICT infrastructure recovery costs. In other words, the social

costs from damage to consumers through online scams and social chaos are not included in the CSIS report. One can estimate that cybercrime has cost Japan's businesses some 100 billion yen, or perhaps upwards of a trillion yen. Whatever the figure, it will certainly continue to climb.

Figure 1-1:
Cyber crime damage per country

Country (shaded are G20)	% of GDP
Germany	1.60
Netherlands	1.50
Norway	0.64
USA	0.64
China	0.63
EU	0.41
Singapore	0.41
Brazil	0.32
India	0.21
Ireland	0.20
Zambia	0.19
Malaysia	0.18
Canada	0.17
Saudi Arabia	0.17
Mexico	0.17
UK	0.16
Colombia	0.14
South Africa	0.14
Vietnam	0.13
UAE	0.11
France	0.11
Russia	0.10
New Zealand	0.09
Australia	0.08
Nigeria	0.08
Turkey	0.07
Italy	0.04
Japan	0.02
Kenya	0.01

2. What is cybersecurity?

Having established that cybersecurity ties into vast economic damage, it is time to reexamine the precise meaning of the word itself. The term is often used to connote "measures guaranteeing safe and secure usage of the Internet," but is there an actual definition? Let us separate the term into its dual components of "cyber" and "security," and examine each in turn.

Let us begin with "security," the more familiar of the two words. Security

management is often described as “defining the conditions necessary to maintain a specific system, and the sequence of activities maintaining that condition.” Any factor with the potential to cause deviation from “the conditions to maintain a specified system” is deemed a “threat.” As threats are innumerable, standard procedure is to conduct risk assessment of likelihood and scope, list countermeasures by priority, and execute a series of initiatives accordingly.

If you identify corporations and business entities and their business partners or clients as the specified system targeted for security management, your definition becomes “corporate security management.” The conditions to be maintained would be those ensuring normal continuation of business activities, with anything threatening or causing deviation from those activities viewed as a business risk. As there are diverse risk factors, some are reduced and avoided, and some accepted, while executing a series of prioritized initiatives designed to sustain business activities. As you will have noted, this is, in short, risk-based management.

You can thus see that cybersecurity is simply part of overall corporate security management. All businesses take security-related measures. They take steps, for example, to ensure that intruders do not enter the premises without permission. Similarly, most consider protective measures against the eventuality of a natural disaster such as an earthquake or flood. Businesses must take cybersecurity measures just as they address other security management issues.

Now let us return to the second word: “cyber.” It is said to derive from the term “cybernetics,” reportedly first used by American mathematician Norbert Wiener in a 1948 book title to describe the mechanism of control and communication in living creatures and machines. Cybernetics” is reportedly derived from the Greek “kybernetes,” which suggests “skill” or “taking the helm.”

Using the mechanism of control and communication among living creatures and machines as the starting point, the word “cyber” (originally describing the commingling of life-forms and information systems in a networking condition) now commonly serves as a prefix indicating an Internet or computer network, since those systems have continued their explosive spread. “Cybersecurity,” “cyberspace,” and “cybercrimes” exemplify this usage.

Though “cyber” suggests “Internet,” its original meaning of commingling of life-forms and information systems in a networking condition is truly profound. Information systems have penetrated every corner of modern businesses; individuals use them and these information systems manipulate and control other information systems, increasingly underpinning business operations. Networks

commingling individuals and information systems are progressively being established between business partners and customers. You might say that the prefix "cyber" could apply to the entire economic society.

3. What does "prioritized cyber assets" imply?

Precisely what, then, does "cyber" mean vis-à-vis business management? I believe that one major reason cybersecurity measures are viewed as problematic is the perceived vagueness of the term "cyber." Surely few businesses clearly grasp the meaning, extent, or status implied by the abovementioned "complex commingling of people and machines in a networking condition and system." Consequently, we lack a clear definition of exactly what cybersecurity should protect. The renowned Chinese general Sun Tzu's advice that "if you know yourself and know your enemy, you need not fear 100 battles" is relevant, as businesses do not yet fully know themselves.

At present, "complex commingling of people and machines in a networking condition and system" is ubiquitous in businesses. Companies themselves have become "cyber." Therefore, prioritized cyber assets must be addressed, and businesses must identify the core function of operations which would yield great damage if terminated or compromised. For a manufacturer, for instance, it would probably be plant operations/line management, whereas for an online shopping site, it might be receipt of product orders.

Cybersecurity measures are reportedly challenging due to the invisibility of attacks making them hard to detect and the increasing sophistication of attackers' skills. Cyberattacks are indeed unseen by the human eye, unlike intruders who physically trespass. We cannot watch confidential information in our networks being stolen, altered, or encrypted.

Nevertheless, though invisible to humans, those acts are detectable by machines, and can be made visible to the human eye. Many commercial security products now inform the company when they detect irregular communication with entities outside the organization.

Furthermore, though it is impossible to protect against all attacks employing sophisticated new technology, not all attacks are necessarily leading-edge in nature. The Data Breach Investigations Report 2016 published by Verizon, a major American telecommunications firm, found that 10 well-known vulnerabilities accounted for 85% of successful cyberattacks in 2015. The WannaCry attack introduced in the "Introduction" of this book similarly targeted a vulnerability in

Microsoft OS; in March 2017, the OS was updated to resolve the vulnerability, and most companies incorporated the correction.

Reasons like invisibility and swiftly advancing technology are unacceptable root causes for sidestepping cybersecurity measures. Companies should face the fact that they must define their own in-house "prioritized cyber assets" before they will be able to "see" cyberattacks and defend their systems against them.

4. Scope of assets to protect

Exactly how should businesses define the scope of their objectives for cybersecurity protection?

Let us examine traditional corporate information systems. These of course include email, schedulers, and electronic payment, but also embrace payrolls, financial accounting, and other systems. Electronic mail systems routinely connect to the Internet, and the in-house LAN used by many companies adds to the sphere of systems needing protection.

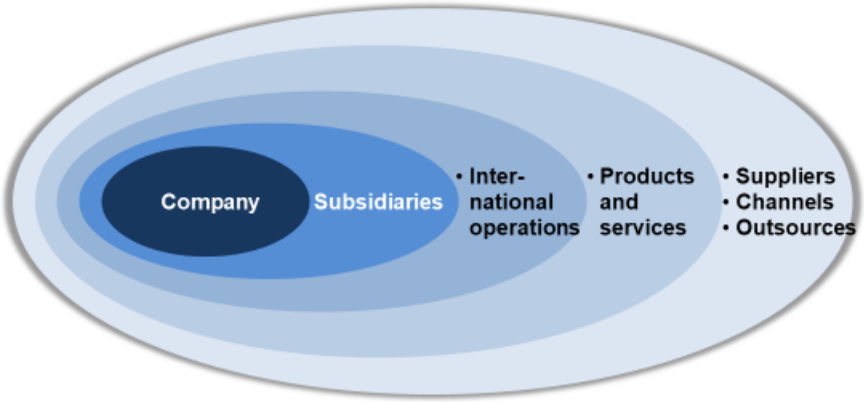
Businesses should be cognizant of the importance of protecting not only the information systems supporting these corporate functions, but also those sustaining site operations. Myriad system types support the core of each business. Manufacturers dealing with assembly and treatment have systems monitoring factory production line operations, those handling materials and processes have plant operation control systems, retailers and restaurants have point-of-sale (POS) systems, and those in the service industry have systems governing customer contacts and call centers. From a management perspective, protecting these is even more important than protecting systems governing corporate functions.

Special Focus: The fallacy in declaring, "We're not hooked up to the Internet, so we're fine."

Occasionally, executives assure me that cybersecurity is not an issue for them as their factory or plant systems do not access the Internet. This argument does not hold up. "Normally" not accessing the Internet and "never" accessing the Internet are two separate matters. Even those who do not routinely access the Internet may well do so, at some point, unintentionally or indirectly. Equipment and systems at plants and other worksites not overtly connected to the Internet are often accessed remotely via an external source to detect failures or conduct maintenance work. Moreover, even though the equipment is not normally connected to the Internet, equipment manufacturer engineers

visiting plants to perform scheduled maintenance work or testing of plant machinery often use Wi-Fi routers for Internet access to perform diagnostics. Even if they do not connect to the Internet on-site, the computers they use may be connected to the Internet sometime, somewhere, and possibly introduce viruses through malware.
Viruses are not limited to computers; they may also be introduced through indirect Internet access via USB memory. The Internet has permeated life to the extent that even if not used routinely, it may be accessed indirectly and transiently, so it behooves us to be practical and assume that we are in fact connected to the Internet. (Figure 1-2)

Figure 1-2:
Scope of assets to protect

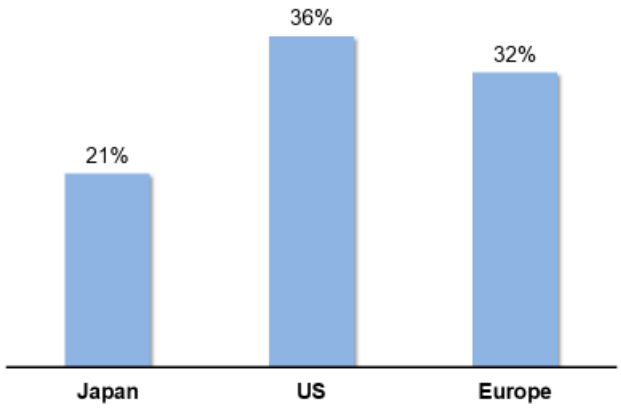


The mantle of protection should embrace subsidiaries and group companies as well as one's own. Most Japanese firms have subsidiaries which are grouped according to function, and are group-managed, with major corporations having almost 1,000 first- and second-tier subsidiaries. Many of these group companies may not have sufficient management resources to safeguard their cybersecurity. If entities are only as strong as their weakest link, then companies must cast a protective net over their entire corporate group.

This applies equally to local overseas subsidiaries and group companies. Many Japanese companies reportedly leave administration, particularly that of

information system operations, to on-site managers of overseas bases and subsidiaries. Most companies probably have no clear idea of how cybersecurity is actually handled at those overseas sites. According to a fall 2015 IPA survey of Japanese and Western companies, 21% of Japanese respondents reported that they exercised sufficient control over cybersecurity at their overseas bases, a figure which paled in comparison with the 36% reported by American, and 32% by European, firms. (Figure 1-3)

Figure 1-3:
Companies regulating cybersecurity of international operations



Source: Research on CISO and CSIRT 2016 (IPA; May 2016)

The ability of firms to protect the products they market is of utmost importance. Businesses should enhance the safety of these products to ensure that business partners and customers on the receiving end will not be vulnerable to cyberattacks.

As an example, a single vehicle produced by an automobile manufacturer reportedly embeds 10 million lines of software code. A single passenger aircraft reportedly carries 6 to 7 million lines of code. The computerization and digitization of products has now spread to home appliances, medical equipment, and other commodities.

Numbers do not tell the whole story, but domestic shipping of such items includes some 7 million computers, 10 million smartphones, 5 million cars, 3.5 million cameras, and 30 million major household appliances. “Internet of Things” (IoT) expresses the concept of all things being linked through networking, and IHS

Global Inc. estimates that 17.3 billion things are globally linked through networking as of 2016, a 13% increase over the previous year's figure of 15.4 billion. Some 30 billion things are projected to be networked by 2020. Today, as we advance further into the IoT age, it is inevitable for companies to shoulder the responsibility of enhancing the cybersecurity of their marketed products.

If products are the objective for protection, then inevitably, the supply chain must be protected as well. These days, one often hears the term "supply chain risk" when cybersecurity is discussed. It references cybersecurity from the viewpoint of component and material suppliers as well as subcontractors.

In the manufacturing industry, for instance, guaranteeing component security is an additional issue for companies working to enhance product cybersecurity. Partial outsourcing is quite common even in areas outside the manufacturing industry. If the subcontractor is remiss in safeguarding cybersecurity, the company may unwittingly be at risk for a cyberattack. For example, as many companies utilizing a membership system for customers likely outsource customer service calls and queries, that subcontractor's system for protecting privileged customer information should receive careful scrutiny. Finally, many companies outsource development and operation of information systems, and must carefully examine those systems to confirm that the security level is sufficient.

As we have seen, companies should protect every aspect of their business activities. Moreover, protection should extend beyond the company itself to embrace related exterior entities such as suppliers, subcontractors, and clients.

5. The importance of an integral perspective

How can you determine your company's "prioritized cyber assets" once those "objectives for protection" have been clarified?

A segmented and comprehensive approach comes to mind. Specifically, this would entail exposing hypothetical threats to corporate information systems, factory line and plant operation control systems, subsidiaries, overseas bases, suppliers, subcontractors, and clients, respectively, performing a quantitative threat assessment of probable frequency of occurrence and related damages, and including a risk-based management approach to solutions.

However, such a segmented approach is inadvisable. This is because the objectives for protection involve a mutual dependency. For instance, the security of a corporate information system necessitates reliance on the security level of the subcontractor building and running the system, as well as on the terms of the

outsourcing agreement. Meanwhile, the security level of overseas factories and plants is interrelated with that of domestic factories and plants. Moreover, in the end, some security measures may cover all objectives for protection. Basic security training for employees is one measure that should be implemented for most objectives to be protected.

Therefore, companies should not assign segmented security measures for each objective for protection; rather, security should be seen through a wide-angle lens and integrated after comprehensive risk assessment, with measures listed by priority. This is the process that generates "prioritized cyber assets." The key concept is not to segment, but rather to integrate the whole through a macro perspective, determining relative priority, and considering appropriate measures.

Specific examples of prioritized cyber assets are found in the second section of Chapter 3 (Key point #1: list objectives for protection by priority and formulate a layered defense accordingly), but such an integral perspective is not unique to cybersecurity. All business executives have experienced this in considering corporate-wide strategy, in which strategies for each business unit or area such as finance and marketing are ultimately integrated into the formation of a single corporate strategy. Truly outstanding corporate-wide strategy is not an aggregation of individual area or functional strategies, but rather one considering reciprocal causal relationship and synergy. Similarly, truly outstanding cybersecurity does not produce a mishmash of isolated strategies for each objective for protection, but rather considers business issues in prioritized order from the perspective of the entire company and yields an integrated set of security initiatives.

At present, then, as business activities continue leveraging digital technology, entire companies are increasingly becoming a commingled networking of life-forms and information devices and those systems. In other words, the corporate entity itself becomes "cyber." If you accept that premise, then cybersecurity has an inseparable duality with overall corporate strategy.

6. Incident Case #1: Bennesse

In cybersecurity, any event generating actual harm is referred to as "an incident." These could be external cyberattacks or internal incidents—inadvertent mistakes or intentional and internal acts. Many incidents, in fact, are composites. The broad-based term "incident" is thus used. Damage associated with "incidents" similarly ranges broadly from minimally-anticipated harm to maximum damage.

Now let us turn our attention to specific examples of how incidents arise, how

they impact business, and which countermeasures are most suitable. These examples will facilitate detailed consideration of how cybersecurity relates to corporate management.

Our first example highlights Benesse Corporation, a major provider of educational services in Japan. The event, which heavily impacted corporate performance, was not a typical cybersecurity invasion initiated from an external network, but remains one of the few examples in which the specific origin was clarified through criminal and civil litigation. Benesse issued a public statement (Investigative Committee Report on Data Breach Incident) which serves as a basis for this discussion.

Incident overview

Following a June 2014 customer inquiry suggesting that client data might have been leaked, Benesse established a crisis management center in its headquarters and lodged a criminal complaint with the Metropolitan Police Department, leading to an arrest on July 17. The offender was contracted by an outsourced company known as Synform, which had been contracted to develop Benesse's information system. (Synform was disbanded in March 2015, and subsequently Benesse Infoshell, a joint venture between Benesse and security-related LAC Co., Inc., was established, to continue its work on the information system).

While working in the Synform office, the offender accessed the Benesse database and stole client data by copying it into his smartphone. He sold the information to a mailing list broker; from there, it was repeatedly passed around. When one of the Benesse customers received direct mail based on the stolen data, that individual contacted Benesse. The Benesse incident was caused by a contract employee of a subcontractor, making it an outsourcing management issue as well.

A high-level system security was in place.

The database from which the offender stole client information had undergone repeated security measures and had a considerably high level of security. Specifically:

- Whenever the server housing the database was accessed, it triggered an automatic record on its access log and communication log. Moreover, the security system issued an alert when data exceeding a certain quantity was transmitted.
- A certain level of authorization was required to access the server storing

the database from a client computer, with permission granted only to client employees needing such access to fulfill their responsibilities.

- Controls were added to restrict exporting of data from client computers, and files could not be copied to USB memory or smartphones from client computers.

Loopholes

There were layers of security safeguarding the data, but an insider familiar with the system would be aware of loopholes.

- As the data was stolen before the security system was launched, the measures were not yet set to issue an alert when the offender's computer accessed the database. In fact, the alert was not triggered even though the offender downloaded a vast amount of data onto a client computer.
- Authority granted to the engineers accessing the database was not periodically reviewed. The offender retained authorization to access the database even after involvement in the system development was completed.
- Security had been beefed up to limit exporting of files from client computers via USB memory and most smartphones, but the offender knew that this upgrade did not include certain types of new smartphones, information he exploited to copy the data.

Litigation and impact on corporate performance

The criminal was apprehended, prosecuted, and sentenced by the second hearing. One cannot assert a definitive causal link, but shortly after the incident, Benesse's client number and profit plummeted, and its stock value dropped, representing a profound corporate impact. Civil proceedings against the company and its corporate management continue even today.

- The offender was arrested and prosecuted on suspicion of violating the Unfair Competition Prevention Law (obtaining/disclosing trade secrets). Following the first hearing at the Tokyo District Court, the offender was sentenced to three years and six months of hard labor and a fine of three million yen. Following the second hearing at the Tokyo High Court, Benesse was also found culpable, and the offender's sentence was reduced to two years and six months of hard labor along with the fine of three million yen.
- Benesse's client number dropped by 30% following the incident, from 3.65 million in April 2014 to 2.71 million in April 2015, and 2.43 million in April

2016. Net profit also dropped. In its fiscal year ending March 2014, the company reported 19.9 billion yen in net profit; one year later, it reported a loss of 10.7 billion yen (including an extraordinary loss of 26 billion yen). And in the fiscal year ending March 2016, Benesse had a net loss of 8.2 billion yen. The company's stock also dropped from 3,945 yen at the end of March 2014 to 3,780 yen in March 2015, and 3,240 yen in March 2016, signifying a "before/after" drop of about 20%. The damage represents about a 72 billion yen drop in corporate value.

- Corporate management dealt with civil proceedings which occurred separately from the criminal procedures against the offender. One such civil action was a shareholder lawsuit asking for 26 billion yen in damages from six corporate board members (at that time). In a separate class action lawsuit, the defense team recruited plaintiffs on the Internet, with some 12,000 accusers ultimately petitioning for 700 million yen in damages. These two civil lawsuits are still pending.

7. Incident #2: JTB

Incident overview

In June 2016, JTB, Japan's largest travel agency, announced a possible leak of client data from 6.79 million individuals, including the numbers of 4,300 valid passports. An employee opened email (containing an attachment) disguised as being from an airline company. As a result, JTB's in-house computers and servers were infected by malware, and the company feared that the offender might be able to order client data to be sent to him remotely. As the email was addressed to JTB specifically, it appeared to be a targeted attack by the criminal.

The clue was targeted email with an attachment containing malware.

On March 15, 2016, JTB subsidiary i.JTB received email disguised as correspondence from an airline company. An employee opened the attached file, causing two servers and six computers to become infected, launching a suspicious external transmission.

- The email bore the title "Notice of attached airline ticket receipt." The email itself read: "Thank you for your business. Kindly find your e-ticket attached," and contained the referenced attachment.
- An employee opened the attachment, but as the individual listed on the ticket was not registered as a JTB customer, the employee attempted to

return the email, noting that it was “inapplicable.” However, the email was undeliverable.

- Subsequent investigation pointed to a crime originating overseas, but the content was in fluent Japanese, and the expressions used generated no suspicion whatsoever.

Slow response, delayed escalation

- On March 19, i.JTB received a report of suspicious transmission from the company entrusted with security surveillance, but due to a delay in blocking further communication with the suspicious IP address associated with the suspicious email, a large-scale leak of customer data was feared. Even after the potential leak was confirmed, a significant amount of time passed as the incident was escalated from the group company and system subsidiary to headquarters’ system division, and then on to headquarters’ executive management, with 3 months ultimately elapsing following initial incident detection before an external announcement was made.
- On March 19, the subsidiary handling security detected a suspicious transmission and forwarded a report. The following day, JTB added the IP address of the intercepted email to its blacklist. Until March 25, all suspicious IP addresses were sequentially blacklisted the day after they were detected. This day-by-day measure allowed communication to continue, resulting in large scale damage.
- On April 1, JTB discovered traces showing access to the unencrypted in-house customer database, as well as to creation and deletion of the file extracting customer data. The in-house database had been accessed on March 21, just after initial detection.
- Subsequently, JTB destroyed the malware, reconstructed the created and deleted file, and began investigating the unauthorized access. On May 13, the company discovered that the file had contained client data. An incident response center was established, and the corporate president was informed.
- The company decided to make a public announcement only after client names were identified and began reconstructing the file. When they finished on June 10, it became evident that data pertaining to 7.93 million individuals may have been leaked. On June 14, the company went public with its announcement (subsequently correcting their assessment to 6.79 million individuals).

Damage extended to companies subcontracting to JTB

It became clear that client data from companies asking JTB to handle their clients' travel arrangements—NTT Docomo, KDDI (au), Yahoo, and DeNA— may have been included in the data breach. The incident embodied what we call a supply chain risk.

- On June 14, when JTB made its public disclosure, NTT Docomo announced that 330,000 individuals who had booked domestic lodging and tours, as well as overseas tours online through its "dTravel" service, were included in JTB's 7.93 million individuals.
- DeNA Travel (6,562 individuals), au Travel (4,462 individuals), and Yahoo Travel (unspecified number of individuals) also made announcements.

8. Incident #3: Target Brands, Inc. (US)

Incident overview

Target is an American hypermarket (GMS) with some 2,000 stores in the US and Canada. In 2013, just prior to the Christmas shopping season, credit and debit card data from some 40 million individuals was stolen through their POS system, greatly harming Target's Christmas sales. A subsequent investigation found that an early alert from Target's security company was ignored, and that other procedures were bungled, leading to the CEO's resignation in May 2014. It was later learned that the attacker entered through the building's air conditioning system and used the in-house network to gain access to the POS system. The technique was sophisticated.

Security measures were in place.

As Target handles many customer credit and debit cards, it held PCIDSS (Payment Card Industry Data Security Standard) certification. It also implemented a remote security monitoring service offered by a security firm.

The attacker gained entry through an unexpected source.

The attacker first invaded the air conditioning system company outsourced to manage ventilation for Target's chain of stores, and stole information. He used that information to enter Target's air conditioning system, and from there, hacked into the POS system via the in-house network. The malware was a new variety which eluded the POS terminal's virus-detection software. The security company issued a warning as soon as it detected a suspicious external transmission via the POS

system, but Target's security personnel ignored the warning, resulting in a large-scale data breach.

Impact on corporate performance and management response

Information concerning some 40 million credit cards was stolen, resulting in poor Christmas sales and a drop in the company's stock value. Corporate performance slowly improved in the new year, but trust in corporate management was compromised, resulting in the CEO's resignation in May 2014 prior to the general stockholders' meeting.

- Sales during the three-month period from October to December 2013 (which included the Christmas shopping season) were $21.5 billion, holding at 4% less than the same period during the previous year. Profit was about $500 million, an enormous 46% drop.
- The stock price, which had been $66 prior to the incident, dropped to $55 in February. Total stock loss was about $6 billion.
- The Canadian market into which Target had entered was in a slump, adding a contributing factor which led to the CEO's resignation in May.

9. Incident #4: Presbyterian Hospital (US)

Incident overview

Presbyterian Hospital (formally known as Hollywood Presbyterian Medical Center), located in California, is a facility with over 400 beds and 500 doctors. On February 5, 2016, the hospital's computer system was infected with malware which prevented access. The malware was actually ransomware. The hospital paid $17,000 in ransom and the computer system was restored on February 15, but during the 10-day interim, hospital functions were greatly impaired.

The attack origin was a file attached to a randomly-distributed email.

The hospital was infected with the ransomware known as "Locky," formatted as a Microsoft Word (MS Word) document disguised as a bogus invoice. This randomly-distributed mail with the "Locky" attachment was presumably received and opened by a hospital employee, thus launching the infection. No details have been disclosed by the hospital about how the malware infected the hospital's system or about the trigger itself.

Hospital functions were greatly impacted.

During the 10-day period when the hospital network was frozen, hospital functions were greatly impaired. Patient data could not be referenced, test results recorded as electronic data could not be shared, and all administrative business had to be recorded on paper. Some patients were transferred to other hospitals. Fortunately, no patient's life was endangered.

- In-hospital networks failed, staff could not read old mail, some patient data was inaccessible, and external communication needed to rely on faxes and phones.
- Medical records were continued on paper, and CT scans, paperwork, and pharmacy business all proceeded offline. Some patients were transferred to other hospitals.
- In the radiation cancer department, patient records could not be accessed, and X-ray, CT scan, and other test results could not be shared.

Ransom payment for restoration may encourage similar future crimes.

According to the hospital's public statement, there was a demand for $17,000 in ransom. The hospital considered the gravity of the situation and acquiesced. The hospital system was restored and no further unusual events occurred. On the other hand, many other examples of "Locky" ransomware were detected on the Internet, with the hospital incident identified as having encouraged similar crimes.

- Some sources reported that ransom was 9,000 bitcoins ($3.4 million with the value of 1 bitcoin at the time), but a memo disclosed by the hospital on February 17 showed the ransom to be 40 bitcoins ($17,000), which the hospital paid to resolve the situation quickly and restore stability.
- The hospital's electronic medical records system was restored on February 15, and all hospital departments could resume usage. All systems were inspected to ensure malware destruction, and normal operations resumed thereafter.
- The criminal remains unidentified. American security company Palo Alto Networks detected 500,000 copycat incidents shortly after the hospital attack. Symantec, another American security company, similarly reported having removed five million "Locky" threats by February 17.

10. What these examples imply

These four incidents suggest three viewpoints for discussion: "prioritized

objectives for protection," "protection," and "response."

First, looking at these examples from the viewpoint of "prioritized objectives for protection" shows us that **a company's business may be profoundly impacted if it does not protect its priceless crown jewels**. Conversely, it is important to clarify the company's highest priorities for protection, and to emphasize deployment of funds and human resources to safeguard them.

In the Benesse incident, I believe that the company's business model shows that the "prioritized objective for protection" was Benesse's client data. Though various safeguards were constructed, the company failed to protect its customers' data, lost trust, customers and profit, and forfeited corporate value. Target presumably also had customer credit card data as its "prioritized objective for protection." The theft of that data led to loss of customer trust.

In the Presbyterian Hospital incident, the question subsequently arose as to whether there had been backup of important data. The hospital did not clarify the matter, but it would be important to implement a contingency plan with backup of critical patient treatment and recovery information impacting life or death, even if there was not backup of all in-house data.

Next, reviewing the incidents from a protection viewpoint, we can see that **it is actually irrelevant whether or not the system is connected to the Internet**. Although an attack e-mail via an Internet link initiated the JTB and Presbyterian Hospital incidents, in the Benesse case, a contracted employee of a subcontractor hired to perform system development was the offender, and in the Target incident, invasion occurred by accessing the air conditioning system and the POS system to gain entry to the in-house network.

The JTB incident can be interpreted as showing the changing landscape—namely, that **the Japanese language is no longer a protective barrier against cyberattacks in Japan. Attacks easily transcend national borders and languages**. Previously, Japan escaped major cybersecurity damage, as the language presumably blocked crimes from overseas. However, one could also say that offenders' Japanese language capability has improved, and that greater precision in machine translation has resulted in the dissolution of such barriers.

Moreover, the Presbyterian Hospital event was a random incident, with bogus mail sent to random targets, while the attack against JTB was what is called a targeted incident. The Target chain store incursion featured multiple steps, with the offender first stealing information about Target's air conditioning system from a ventilation contractor, then using that to gain access to Target's air conditioning

system, and from there, to invade the POS system. Quite a bit of reconnaissance was required to survey Target's systems and network configuration.

Clearly, targeted attacks reflect skillful use of exceedingly intricate methods. The JTB incident seemed to involve a comparatively simple approach, but had the targeted mail failed, the attacker might have tried once again with a more sophisticated plan.

In any event, targeted attacks do not simply involve targeting a victim. Rather, they reflect "persistent and repeated efforts which are not abandoned until the attacker succeeds," as an engineer friend of mine explained. He added that "**it is impossible to safeguard 100% against cyberattacks**"

The final point concerning protection, is that **humans are the greatest and weakest security vulnerabilities**. The Benesse incident (an insider job) and the JTB and Presbyterian Hospital events (external invasions) all exploited humans on the inside. Knowing that people are the greatest and weakest security holes, the respective attackers carefully surveyed wording and timing which would likely provide an opening, and persistently and repeatedly lay their traps.

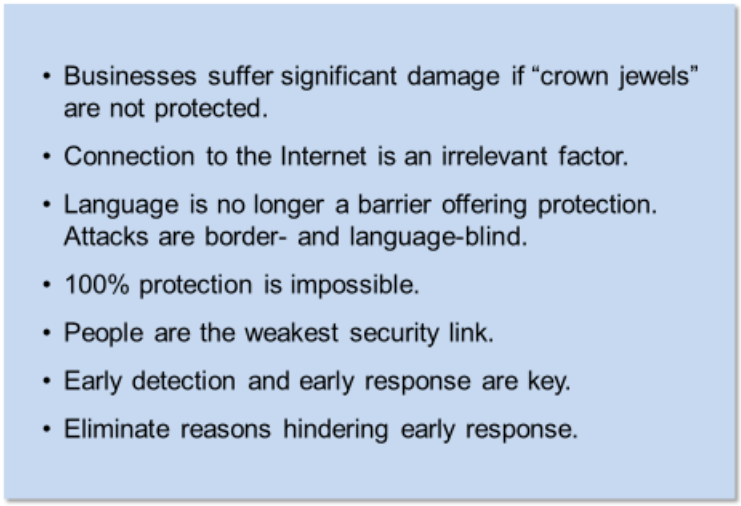
Response, our final viewpoint, demonstrates that **early detection and early response are both key**. In the JTB and Target incidents in particular, relatively early detection was followed by slow response, forfeiting the opportunity to minimize damage.

In the JTB incident, a March 19, 2016 report from the security firm was received, with the suspicious address being blacklisted and thus blocked on the following day, March 20, but there was no decision to block all external communications. That lack of judgment invited the creation and leak of a large-scale file of client information on March 21.

The security company provided a similar warning of a suspicious transmission in late November in the Target incident, and a stronger warning in December. Nevertheless, these alerts were ignored by Target's security arm.

Why was the company unable to achieve an early response? The corporate public statements offer no clue, but one can surmise that **some unknown factor (aside from technical difficulties) gave the company pause**. That unknown factor may itself have possessed a deeper root cause. Chapter 3 ("Imperative Actions for Business Executives") discusses the importance of early detection, early response, and the approaches surrounding each. (Figure 1-4)

Figure 1-4:
Implications drawn from actual incidents



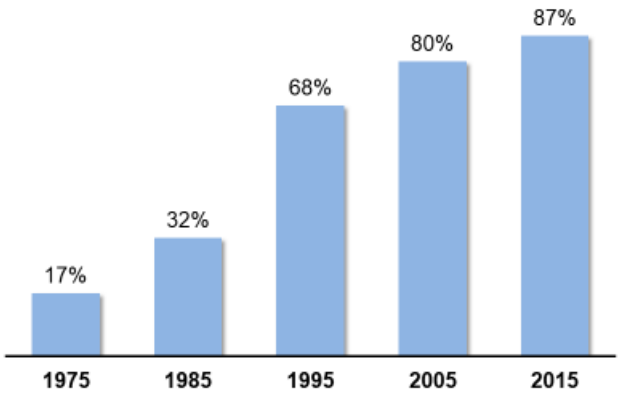
11. Digital resilience

The implications from four examples depicted in Figure 1.4 show that qualitatively new responses to risks are required of companies going forward. In conclusion, let us consider the circumstances from the viewpoint of shifting value-added corporate assets.

Companies operate through business activities which produce profit. This profit equates to corporate value. From the 19th century through the late 20th century, corporate value was generated by tangible fixed assets such as land, resources, manufacturing plants, shops, and the like. However, from the 1990s onward, as the century waned, assets generating corporate value shifted greatly from tangible to intangible sources.

Specifically, importance was placed on intellectual property such as patents and trade secrets, as well as brand equity, partnerships, and skills (human resources) as sources of corporate value. Results of an Intangible Asset Market Value Study conducted by Ocean Tomo, an American firm consulting on intellectual property assets, demonstrated that 87% of market value generated by S&P 500 companies now originates from intangible assets such as intellectual property. (Figure 1-5)

Figure1-5:
Value of intangible assets within S&P 500 companies' market value



Source: Ocean Tomo: 2015 Annual Study of Intangible Asset Market Value

Now, almost 20 years into the 21st century, we are witnessing the ongoing genesis of digitization, an intangible asset generating value. Intellectual property itself is digitized, and can be processed, shared, or used freely through digital technology. The percentage of digital communication between participants is similarly growing rapidly in business partnerships. Companies are ensuring enjoyable user experience and boosting brand value by switching to online channels for customer interaction.

This digitization of value-added assets provides the freedom to create more added value for the customer ultimately generating enormous wealth. The future will doubtless bring new value-added creations which we cannot imagine at present. And, no doubt, the structure of our social economy will shift greatly. This is certainly the era of digital transformation.

On the other hand, the digitization of value-added assets simultaneously introduces the digitization of corporate risk. Risks requiring cybersecurity management are increasingly a part of digitized corporate risks. The four incidents—Benesse, JTB, Target, and Presbyterian Hospital—surely offer true accounts of digitized corporate risk. They also show that success level in managing digitized corporate risk hugely impacts the ultimate success of business management.

The free creation of added value allows for generation of enormous wealth, but digitization of assets invites a fundamental vulnerability for companies which requires strengthened and evolving response. As corporate risk is digitized, risk management must also become digitized for companies to be resilient. We are now in an era in which successful corporate resilience will impact business competitiveness.

The next chapter, “Why Cybersecurity Is a Business Management Issue,” examines the dual issues of vulnerability inherent in digitization and flexibility.

Chapter 2: Why Cybersecurity is a Business Management Issue

In Japan, the focus is overwhelmingly on data breaches, but those are not the only management risks. Let us redefine why cybersecurity is a management issue. Namely: (1) Business continuity may very well be threatened; (2) Cybersecurity protects stakeholder trust while (3) Underpinning digital innovation spurs corporate growth.

1. The implications of digitization in autonomous driving

Autonomous driving, the most rapidly-evolving area of digital innovation, is a concrete example of the latter's impact on society.

I had the opportunity to listen in on a round-table discussion on autonomous driving at a cybersecurity symposium. The five participants included a senior engineer for a major automotive OEM, a security representative in the new business area of autonomous driving services, a mid-level executive in a national government agency, a renowned cybersecurity lawyer, and a university professor specializing in personal information protection. All were eminent individuals.

The discussion was wide-ranging and replete with opinions. Issues were debated on a macro level: when, and at what level, self-driving cars would materialize, what infrastructure that would require, and the ideal balance between international competition and cooperation in development of cartography, reportedly the key to autonomous driving. The discussion further included technical issues such as whether communication latency between transit-related devices and systems could be reduced to milliseconds and how best to create safety benchmark criteria, plus legal challenges such as ownership of driving-related information, issues surrounding new legal systems, and how collecting legal precedents can aid creation of those legal systems.

I was most intrigued by how concepts of safety would change with digitization-based autonomous driving. For example, devices and components have failure rates which are engineering metrics used by development and manufacturing to realize safety initiatives. However, most cyberattacks are malicious and expected to evolve over time. Someone indicated that dynamic measures encompassing technical advancement should replace static failure rates.

Moreover, as cars are used for about 10 years in the marketplace, we need a plan for incorporating updates once vehicles leave the factory.

We must also decide who will guarantee safety. Currently, the mainstream opinion is that OEMs should take that role, but once companies offer autonomous driving as a mobility service, how will they and OEMs fairly share responsibility for safety? The expectation is that service companies, not OEMs, should guarantee customer safety.

Participants also suggested that individual drivers need safety education, most likely a standardized level required of all drivers, before being allowed to utilize driverless cars.

Under our current social structure, responsibility for safety is shared by many: the manufacturing industry, including OEMs and component manufacturers, transport service providers such as taxi companies, and individual drivers, plus systems sustaining safety, such as recalls, passenger transport agreements, and driver license requirements. Driver and pedestrian education are also included. The round-table discussion clarified that these boundaries for responsibility, as well as our social systems, will need reconsideration when autonomous driving materializes.

The five round-table participants continued their exchange and ultimately agreed on the following: Recurring problems shared by the software and Internet security field for over a decade have been met with specific resolutions spontaneously advanced in the marketplace. Setting aside debating the ideal approach for software issues, it might be useful to learn from those experiences and implementations as society grapples with autonomous driving.

2. What transpired in the software field

The software field's specific experiences and initiatives arose because many security problems were detected after software products were shipped; society accepted software companies' ad-hoc approach to updates.

In discussing the WannaCry case in the "Introduction," we questioned why Microsoft marketed Windows OS if the product was imperfect due to vulnerabilities. The answer is that Microsoft strove to remove all vulnerabilities prior to shipping, but new vulnerabilities unavoidably emerged. The product was technically imperfect, but software's inherent idiosyncrasies make it impossible to release a perfect bug-free product; supplemental corrections are thus a premise to product release, and user acceptance of that fact is a market principle.

Home computer virus detection and protective software ("antivirus software") follows the same market principle. Such software, though purchased and installed, is useless against new viruses which can slip through. Therefore, definition files which detect the newest viruses are periodically released at no additional cost. This business model has become the marketplace norm.

"Time to market" is a term describing lead time until a product is released, and one which is highly regarded in the software field. This is because a product released quickly and well-received by users may achieve de facto market domination.

The situation is particularly applicable to software, as so-called "switching costs" can be expensive for the user. Once a user adopts certain software, he or she will avoid switching to a different product as it may cause loss of accumulated data assets, require adjusting to new functions and formats, and/or be incompatible with other software already running on the computer. For these reasons, it is easy to retain customers by easing them over to a newer version of familiar software.

Software companies often have their developers quickly release new versions (such as "beta versions") and incorporate user feedback, enabling speedier product evolution, rather than seeking pre-release perfection in an original product. This evolution-oriented product development accelerates market release while answering market needs.

Thus, the software field has adopted this development/marketing mechanism of letting products meet standard tests and survive user trials while permeating the marketplace. This "lead with speed" dynamism presumably aids marketing of vulnerable products, but it also meets user needs and is a marketplace reality.

3. Risk digitization

In the final section of the last chapter, we identified a trend since the late 20th century—namely, that business-generated value is increasingly from intangible assets, and that progressive asset digitization brings increasing digitization of accompanying risks.

What does risk digitization mean? It is an exceedingly important topic deserving of consideration from broad-ranging viewpoints. Here are three preliminary thoughts to the challenges presented by risk digitization. The first is the need for dynamic and ongoing measures. Digital technology advances daily, as do cyberattack methods. There is no avoiding discovery of new vulnerabilities in products and devices which previously seemed completely safe. We therefore cannot

view risk as something solvable with fixed, static measures; we must maintain dynamic measures while constantly reevaluating and revising. This also suggests necessary awareness of a time horizon. Since dynamic measures are required, it is inevitably essential they be applied throughout the product and device life cycle.

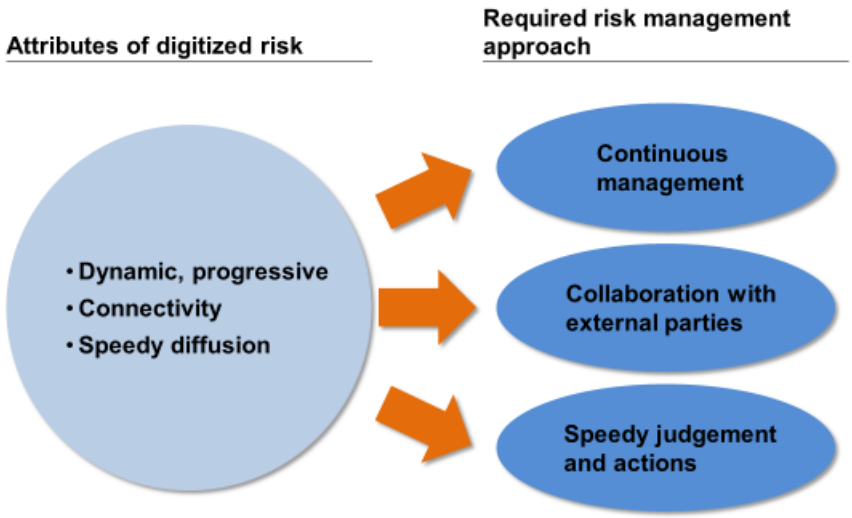
The second approach necessitates external cooperation. Digitized products and devices are often linked to one another. This connectivity is an outstanding benefit brought on by digitization. It requires reciprocity with surrounding linked products and devices as part of risk response. This extends beyond products to companies, which, if digitized, can collaborate through connectivity in business and risk responsiveness, signifying that no company stands alone, but must work together with clients and business partners.

The third approach underscores the necessity for rapid response. When a defect is identified in digitized machines and equipment, problems can snowball in the blink of an eye. Thus, rapid response should immediately follow risk detection.

Let us take the example of autonomous driving, discussed at the outset of this chapter. Prioritizing technical advances means shifting reliance on static metrics (such as safety index failure rates) to dynamic risk response. It also demands a continuous response approach, agreeing up front that continuous software updates will be required for ten years following product launch. It also compels service providers and users to join manufacturers in understanding, accepting, and sharing responsibility for risk, requiring cooperation and collaboration among companies. In the WannaCry ransomware discussed in the “Introduction,” the cyberattack which began in Europe spread like wildfire to the rest of the world. The example clearly demonstrated that without rapid assessment and response, large-scale infection and damage may well occur.

In sum, these three preliminary thoughts describe what is required for countering the substantial characteristics of digitized risk: continuous response measures due to risk being a dynamic entity, external collaboration/cooperation due to connectivity, and rapid assessment and response due to speedy diffusion. (Figure 2-1)

Figure 2-1:
Digitization of risk



Autonomous driving symbolizes the penetration of digitization into everyday life. As this penetration proceeds, so, surely, will the digitization of risk. The ubiquitous security gadgets known as "network cameras" in urbanized areas have built-in computers. They capture live images which may be viewed and stored remotely. However, if such cameras are accessed and remotely controlled by cyber perpetrators, the recorded images will be in the hands of the criminals.

The word "bot" describes a digital device that can be controlled remotely ("bot," from "robot"). When a digitized device is controlled as a bot, it can be used to launch cyberattacks on other devices. Installation of security cameras can unwittingly result in cyberattacks on the camera owner, as images captured by the cameras are secretly leaked. Worse yet, the victim may be accused of being the assailant.

Digitized devices have already become stepladders to the launch of large-scale cyberattacks. In October 2016, major Internet service providers such as Twitter, a social networking service (SNS), and the online music distributor Spotify, were temporarily inaccessible. The cause was a major cyberattack on Dyn, an American IT infrastructure firm providing services to those companies. The cyberattack used IoT malware to infect and robotize hundreds of thousands of digitized devices worldwide.

The Presbyterian Hospital incident introduced in Chapter 1 is an example of

cyberattacks in the medical field, in which medical equipment and information systems are hacked. One case was reported in 2011 at Black Hat, a major security event held each summer in Las Vegas to introduce the latest hacking technology. In the 2011 case, vulnerability in wireless functions enabled hacking of a diabetic patient's insulin pump to gain remote control over insulin dosing (source: IPA, Security Report on Medical Equipment, April 2014, p. 6). Similar reports indicate that embedded medical equipment with wireless communication capability presents a security vulnerability.

4. Corporate implications

Digitization continues to permeate society. As a result, new types of risks will spread. How should businesses respond to these changes?

Legal restrictions may be considered to counter the reality of digitized products with imperfect security. Even stopping short of legal controls, many fields will doubtless enter discussion on security protection of products and services and new rules for assessment. As a result, manufacturers, service providers, and users will ultimately agree on a tradeoff between economics/convenience and safety, reflected by gradual development of social systems.

As systems evolve, I believe the dynamism of consumer preference for convenience (in consumption and purchase) despite safety concerns surrounding product launches is inevitable. As we saw with the software example, perfect product security is impossible, and market needs will continue to emphasize convenience. While corporate entities help develop a legal system and social rules, they will at the same time need to find ways to accommodate digitized risks into their business operations in the market dynamism and business environment.

Businesses will have dual roles; they will be users and providers of digitized products and services. They must therefore implement risk management for the digitized products and services they both use and provide.

The corporate entity itself is becoming digitized, as is society. This change is bringing new risks. How should these new risks be confronted, and will management advance in the digitized age? This topic is surely just now beginning to be addressed by most companies. There is no uniform solution; each company must be allowed its own opinions, evaluation standards, and approaches to digitized risk management in accordance with its individual business strategies and objectives.

Business is all about risk management. Assuming that risk digitization requires changes to the current ideal of management, I believe we can say that cybersecurity

is digitized risk management. For convenience, we will continue to use the phrase "cybersecurity," while recalling that we really mean "corporate digital risk management."

What imperatives must business executives consider in managing digitized risk or in establishing cybersecurity? These are, in other words, the issues which must be recognized as cybersecurity management challenges. For instance, information leaks are undoubtedly an important cybersecurity issue. An external leak of protected information is certainly an alarming issue, and if customer information is involved, those customers may actually suffer great damage and anxiety. And finally, since mass media and society issue blame whenever there is a data breach, cybersecurity is now seen as a management issue. However, the import and scope of stolen content determine impact on management, so equating "data breach" with "management issue" is an oversimplification.

I myself believe that there are three reasons why cybersecurity should be seen as a management challenge: (1) it threatens business continuity; (2) it supports stakeholder trust; (3) it creates the foundation for corporate growth. I will interweave examples of these into the following section.

5. Reason 1: Business continuity

Endangered business continuity, not data breach, levies the greatest impact on business when cybersecurity incidents occur.

In Chapter 1, we saw that Presbyterian Hospital was unable to access its in-house systems, greatly compromising hospital function after a ransomware attack. Activity was not completely shut down, but patient records could not be viewed, staff had to rely on paper and pencil, and some patients had to be transferred to other facilities. You could say that hospital business continuity nearly reached crisis pitch.

Attacks threatening business continuity are largely based on ransomware and its ilk, and are increasing. Some 2,000-plus computers from the San Francisco municipal transportation bureau were infected in November 2016, causing subway ticket machines to freeze. Meanwhile, the Turracher Hotel in the Austrian Alps experienced a ransomware attack in January 2017 which paralyzed both the reservation and electronic keying systems. In another January 2017 incident in Washington, DC, just prior to President Trump's inauguration, police security cameras were infected by ransomware and were unable to record images. In June 2017, Maersk, a major Danish container shipping company, experienced a

ransomware attack which temporarily halted systems forcing the harbor terminal department to halt operations temporarily. The company announced damages totaling somewhere between $200 to $300 million. In each of these cases, the criminals threatened continuity of business to heighten the likelihood of ransom payment.

Many cyberattacks are not launched for ransom money, but as direct threats to business continuity. In the third section of this chapter, as we saw, online services such as those provided by Twitter (US), Spotify (Sweden), Netflix (US), and the Wall Street Journal (US) were stymied for six hours in October 2016. This occurred because Dyn, the American company offering IT infrastructure to these online services, suffered a massive cyberattack. Dyn's infrastructure system was impeded by Distributed Denial of Service (DDoS) attacks, in which multiple transmissions of large amounts of data are sent to servers and networks.

Special Focus: What are DDoS attacks?

Let us define a Denial of Service (DoS) attack. Most ICT services are offered through servers. If the processing power of those servers is overpowered by a huge volume of requests, the server cannot cope and the system shuts down. For example, if a website developed by you, the reader, is overwhelmed with simultaneous requests, it becomes difficult to browse. If this occurs intentionally, it is known as a DoS attack.

However, if all the requests originate from a single device, outgoing volume is limited, and the source is easy to detect. This gave rise to DDoS attacks, in which outgoing volume is decentralized and dispersed on the Internet. An attacker sends malware to all sorts of devices linked to the Internet, each of which becomes infected. The various devices are controlled remotely and send massive volumes of data to the targeted server. This system allows transmission of massive volumes of data, complicating source detection. As these numerous decentralized devices are manipulated robotically, they are known as "botnets." "Bot" is borrowed from "robot," and signifies "networked robots."

Recent DDoS attacks have been vast in scale, facilitated by development of malware which can generate over 100,000 robotized transmission devices. As we advance into the IoT era, many kinds of digitized devices are used to access the Internet, further increasing security issues. For example, attackers can remotely turn devices like the digital cameras and routers found in many homes into robotized transmission devices.

Another recent trend is the emergence of "ransomware attacks." Users receive a message ("Your device is about to experience a DDoS attack. To avoid this, pay the ransom.") forcing them to pay money. In some cases, the DDoS attack is launched before the threat is sent, with the offender showing off his ability to stop the target's services. Vicious attacks now aim at companies for which online service means survival, such as online security brokerage firms. The cost of launching DDoS attacks has dropped, explaining why such threats demanding ransom are on the rise. Some black-market websites provide DDoS attacks for just several dozen dollars.

There are currently few reports of threats to corporate systems supporting continuity of backbone business, such as those managing operations for assembly factories and plants, POS systems for stores, and order processing systems for call centers. However, such threats may well rise in the future. In December 2015, a major power outage caused by a cyberattack damaged tens of thousands of homes in western Ukraine. A power grid's transformer substation and a customer support center suffered damage almost simultaneously, in what became identified as a well-planned attack. This is considered the first example of a power company losing business continuity due to a cyberattack causing a widespread power outage.

The potential for a cyberattack to threaten business continuity is increasing, making it the prime reason why cybersecurity is a management issue. On the other hand, most companies seemingly feel they will not likely experience an extreme cyberattack. However, this is a misguided view. Most ransomware, like the malware threatening business continuity in the WannaCry example, is not targeted at a specific victim; it is random. In other words, it is an indiscriminate attack. Moreover, companies with no security measures are highly likely to be infected. The ransom level ($300-$600 in the WannaCry incident) does not suggest major firms. We should be aware that the potential for a cyberattack threatening business continuity is rising for all firms, even those which are small and medium-sized.

Even if the attacker's target is not business continuity, executives should keep this topic in mind as they plan response measures. There is a tendency to overlook this point, but it is important all the same. In today's world, all businesses, not only those supporting social infrastructure, should plan for business continuity, as we can see by revisiting the JTB example introduced in Chapter 1.

The JTB incident occurred on March 19, 2016; JTB was informed by a security company, and blocked communication with the suspicious IP address on March 20, but did not cut off all external communication. This led to a suspected data breach

involving personal information from some 6.79 million individuals on or after March 21. Why, one wonders, did JTB not block all external communication on March 20. Delayed decision-making led to a magnification of damage, as it did in the June 2015 Japan Pension Service case.

As neither JTB nor the Japan Pension Service publicized their reasons for not blocking external communication immediately, the following conjectures are strictly my own. First, blocking external communication would likely have greatly inconvenienced other business operations, probably leading them to conclude that measures of that magnitude were unnecessary. They might not have considered the impact on business continuity which failing to block external communication might have had. It is unclear who decided what, and when, but the decision could have been made by someone handling information systems and networking operations, or by someone at middle management level who should have sought guidance from top management.

These are strictly my conjectures and may differ from reality, but we can extract two lessons from the JTB and Japan Pension Service examples. First, though the attackers did not directly threaten business continuity, the company should have considered it once the offense was detected, and should have debated halting business operations, at least temporarily, as measures and restoration were discussed. Second, the company must train and prepare its members for quick decision-making when the situation calls for a temporary shutdown of business operations.

Once an in-house system is infected, management must discuss continuation vs. temporary vs. partial shutdown of business. Decisions should be at the executive level, which is why cybersecurity is a business management issue. Following management consensus, the company should prepare for a potential security incident. Even if countermeasures are limited to technical areas such as IT and network modifications, management must evaluate the effect both damages and protective measures might have on business, and then determine the scope of countermeasures. Any missteps here could result in unexpected harm to the business side. The company should decide who will assume responsibility for judging what, thereby avoiding delayed response during emergencies when confusion reigns. Who should make the judgment to take action? Should it be he IT department and the security team, the supervisor in the potentially impacted business area, or the top brass since the entire company could be impacted? Such debate should occur ahead of any incident.

6. Reason 2: Protecting trust

In the third section of Chapter 1, we discussed the need to prioritize cyber assets for protection, suggesting that one reason protecting cybersecurity is challenging is the difficulty in defining the exact targets for protection. Another worry which executives shared with me is their uncertainty about the proper scope of cybersecurity protection.

Attackers improve their game, not at a monthly or even daily pace, but minute-by-minute. Furthermore, though attackers only need to succeed once, companies must protect against all attacks. Cyberattacks give the attacker the upper hand. Once a company has been targeted, it is almost impossible to enact 100% protection. The key is not only safeguarding, but also ensuring early detection and early response. This is easy to understand on the surface, but exactly how far must a company take safeguarding measures, not to mention early detection and early response. Companies crave an absolute rule or benchmark, yet there is no definitive answer.

When attacks yielding real damage occur, companies are likely to explain current cybersecurity efforts to stakeholders, claiming extreme attacker sophistication to explain the damage, and adding that this particular incident was unavoidable. There may likely be dismay at the company's paltry efforts, with stakeholders claiming no surprise that this level of damage was incurred. If the company had only taken proper measures, things would have been different. The reality is, there is a world of difference in what we think is enough, and what is enough, when it comes to cybersecurity.

One Chief Information Officer (CIO) offered this allegory. There is a huge difference between a thief waltzing into an unlocked home and stealing a pile of money stacked on the table, and managing to steal money from a locked safe inside a locked home. The CIO added that there is no absolute measure for adequate cybersecurity, no way to know what level of measures justify declaration that an incident "couldn't be helped."

Clearly, we do not undertake precautions simply to declare that the attack "was inevitable." The reality is that post-attack reactions from stakeholders such as clients, business partners, shareholders, and authorities will reflect their evaluation of the degree of countermeasures taken rather than the actual damage. Indeed, stakeholder trust lies in the balance.

A company's business activities are premised on the belief that all the information they handle is true and correct. Clients, business partners, financial

institutions, and the capital market all trust that corporate information and the devices and services handling it are authentic, and see trust as a prerequisite for corporate business operations. Digitized risk and risk management are not only corporate matters, but increasingly matters involving clients and business partners. Therefore, inadequate initiatives will impact your reputation as a reliable business partner. You will also lose the confidence not only of business partners, but of a wide array of stakeholders.

Asking how far precautions should extend can be replaced by the question of how far they should extend to protect stakeholder confidence. A more specific answer is discussed in Chapter 3, but a company should essentially invest resources to protect its prioritized targets in preferred order, from a company-wide stance, as suits its distinctive corporate characteristics. This should subsequently and periodically receive executive review. This entire process requires executive judgment and defines the second reason why cybersecurity is a management issue.

7. Reason 3: Underpinning digital innovation to spur corporate growth

Digital innovation is accelerating at a frantic pace. We encounter terms such as AI, big data, FinTech, and biometrics on a daily basis, while digital technology advancements facilitate the appearance of new markets on a global scale.

According to Disruptive Technologies, a 2013 survey report by McKinsey & Company (US), digital innovation may produce new economic value totaling $14 to $33 trillion by 2025. There is no doubt that a company's ability to sustain growth will depend on its ability to incorporate and activate this explosive digital innovation. Success in digitization promises great new strides, while failure dooms one to lag in global economic growth.

Companies activating digital innovation in their business will find it imperative to be digitally secure—to initiate measures ensuring cybersecurity. Being digitally secure implies enacting security covering daily work and the digital technology in marketed products, plus managing these in line with corporate objectives.

For banks, as an example, ensuring reliable security for Internet banking should be part of ensuring quality customer services. When retailers initiate online supermarket business, they should ensure safe and reliable online payment. In the future, heightening security for a company's own products will transcend the cars and medical devices referenced earlier to include networked cameras, home appliances and other daily gadgets, traffic signals, and factory and plant operational equipment…in other words, all kinds of products.

I suspect that any day now, product and service ads will mention strong protection against cyberattacks. Cars, for example, will not only tout their mileage and cost-efficiency, but also their cybersecurity as part of overall safety. Financial services will hasten to promote the security level of their bank accounts, money transfers, and payment services. Moreover, home appliance manufacturers will publicize the safety and reliability of their products against "cyber-takeovers."

I do not believe this is a mere daydream. As mentioned in the fourth section of Chapter 1, expanding safeguarded targets implies corporate supply chain protection with enhanced cybersecurity measures for component suppliers and subsidiaries. In 2016, the UK government announced that it would cease outsourcing to companies not certified in accordance with its Cyber Essentials guidelines. This demand for proper corporate cybersecurity measures prerequisite to becoming a governmental supplier is gradually expanding among global governments and is expected to follow suit between companies themselves.

Firms leveraging digital technology in new markets or fields often collaborate instead of trying to manage alone. Cybersecurity would help realize selection for such a partnership. Internationally, due diligence in M&A necessarily includes surveying the partner's cybersecurity measures.

The skill manifested in a company's cybersecurity measures also reflects on corporate value. When Yahoo (US) was bought by the American telecommunications firm Verizon, a data breach involving the personal information of over a billion individuals precipitated a discount of about $350 million off the acquisition price. In response to this trend, the American Bar Association published its Guide to Cybersecurity Due Diligence in M&A Transactions in September 2017.

As the digitization of the economic system continues, proper cybersecurity measures will help ensure that companies are popular candidates, while those failing to become digitally secure will remain unchosen wallflowers when peers seek business partners. In other words, we have entered the era in which cybersecurity is increasingly viewed as the fountain of corporate competitiveness.

Business continuity and trust were discussed in the fifth and sixth sections of this chapter as two objectives avoiding downside risk; the 3rd point, the fountain of competitiveness underpinning corporate growth, relates to gaining upside risk. The new trend is to gain upside risk as well as to safeguard, which is critical.

The lingering assumption is that cybersecurity is a key management issue for entities supporting social infrastructure, such as power, telecommunications, finance, water, gas, petroleum, railways, airlines, land transport, medical care, and

the like. For other entities, such as small- and medium-sized enterprises (SMEs), cybersecurity may be recognized as a management issue, but rank low on the prioritized list of problems needing attention. However, the ability to exploit unprecedented growth opportunities brought by digital innovation is a key business issue for companies of all sizes and types. These SMEs must notably confront cybersecurity when creating foundations for pursuing corporate growth.

In its Cybersecurity Strategy published in September 2015, Japan's Cabinet acknowledged cybersecurity as the foundation for corporate growth sustainability. The publication declared that cyberspace, home to innumerable computers, sensors, and actuators networked by IT, underpins the world's free societies and democracies, adding that this cyberspace—or digital space—produces new business models and technological innovation which represent the frontier of economic growth. The objective of cyberspace, it concluded, is to protect free expression and innovation, while contributing to the enhanced vitality of our economic system.

The entire world joins Japan in viewing cybersecurity as the foundation for economic development. The UK government, for example, declares in the executive summary of its National Cyber Security Strategy 2016-2021 that, "The future of the UK's security and prosperity rests on digital foundations. The challenge of our generation is to build a flourishing digital society that is both resilient to cyber threats and equipped with the knowledge and capabilities required to maximize opportunities and manage risks."

The US President established the Commission on Enhancing National Cybersecurity to report on ways to strengthen cybersecurity over the next decade and beyond. Its subsequent Report on Securing and Growing the Digital Economy in December 2016 began with the declaration that, "Recognizing the extraordinary benefit interconnected technologies bring to our digital economy…"

8. Industry should be proactive

We have examined the three reasons why cybersecurity is a business issue. This chapter concludes with the points companies should proactively pursue with initiatives.

Business executives often confide their wish for the government to take proper cybersecurity measures. The main reason is that both attack and safeguarding technologies are advancing rapidly, and attackers are sometimes presumed to represent overseas governments or government-sponsored groups. As criminal acts transcend borders, governmental cooperation is indispensable in managing the

problem.

I completely agree with the opinion that proper governmental measures are necessary. However, this does not eschew passive reliance on the government or assume that the industry will respond when there is demand from the government. There are two reasons for this.

The first is that whoever the attacker, the victims are companies, and it is companies who take responsible measures. Cyberattacks are launched by many offenders, from pranksters to international criminal economic entities to government-supported groups. However, whoever the criminal may be, if a company is attacked, it is the company which suffers the damage. As we saw early in Chapter 1, damage totaling between $375 billion and $575 billion is incurred globally, and about 100 billion yen to several trillion yen (deduced) in Japan, all by companies.

It is the companies themselves who must take measures to minimize damage. Let us create a fanciful example. A cyberattack is launched on the operations control system at a company's plant, and the plant can no longer carry on. The situation is reported to the police and a cybercrime task force runs to the rescue. What can they do? The first assessment is to stop or curtail operations, which occurs. The network needs to be intercepted to prevent the virus from spreading to other in-house systems. Finally, to cap damage, the system is examined to determine whether a similar virus has also been triggered in the system. These steps must be taken by the owner of the plant and in-house system: the operating entity, which is none other than the company itself.

The law also stipulates the company's own initiative. Article 7 of Japan's 2014 Basic Act on Cybersecurity states that the business entity should ensure cybersecurity voluntarily and proactively, indicating cybersecurity must begin with independent initiatives by the company itself. Please do not misunderstand; this is not to say that governments should not engage internationally or that new technology is unnecessary. The point is that governmental cooperation and initiatives cannot protect each individual company, so companies must pursue their own initiatives proactively.

The second point—that one cannot simply rely on the government—means that government outreach cannot keep pace with threat expansion. The drawback to government action is the time it takes. For example, in response to international cybercrime, if one government negotiates with another, the back-and-forth will take quite some time. Alternatively, if government funding is allocated for security R&D, months will elapse between the funding request and its consideration and final

approval by the Diet. Diet deliberations are also required to enact a ban controlling cyberattacks or revise a law, and lead time is needed for ministerial ordinance revision and preparation of guidelines needing consensus. The reality is that governmental countermeasures remain a step behind.

Despite the slow pace, cooperation and negotiations with foreign governments are of course extremely important, and technological development and requisite statutory revisions must occur. Governmental initiatives are necessary. However, it is also a fact that, while cyberattack methods evolve daily, governments are poor at delivering quick response. Companies should avow to protect themselves even as they encourage governmental action.

The industry community sometimes declares that it wishes the government would enact guidelines, but even when the government complies, it would be dangerous for companies to see the guidelines as a cure-all prescription. "Prescription" implies that if you comply, all will be fine, and that the same guidelines apply to all companies.

As you surely know, both assumptions err. There are no blanket guidelines in the field which can protect all companies from the myriad cyberattack techniques being devised. Even if there were, the moment they were shared, attackers would launch a counteroffensive. Cybersecurity is a component of risk management, and as individual companies should assess and execute their own business strategies and project operations, guidelines cannot universally apply to all companies. What the government can offer is the minimal level of recommended measures, or reference material helping companies debate and execute their respective initiatives.

The Ministry of Economy, Trade, and Industry (METI), collaborated with the Information-technology Promotion Agency (IPA) to issue Cybersecurity Management Guidelines in December 2015, which were revised in November 2017. These are simply guidelines for business managers —references as they draft their own individual corporate initiatives. However, they may provide a helpful yardstick in answering how far initiatives should reach, so those who have not yet read the Guidelines may wish to do so.

Let us close this chapter by emphasizing the necessity for each individual company to establish its own measures proactively. Chapter 3, "Imperative Actions for Business Executives," explains the steps executives should take while delegating tasks to trusted employees.

Chapter 3: Imperative Actions for Business Executives

There are three imperative actions which business executives should take: (1) Prioritize objectives for protection, and create layered defense accordingly; (2) Ensure early detection, response, and recovery, as 100% safeguarding is impossible; (3) Review all preparations periodically at board and executive management meetings.

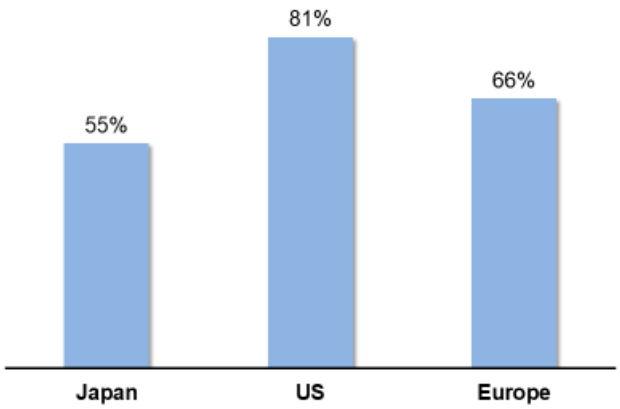
1. Corporate Japan lags behind the West

How do cybersecurity measures taken by Japanese corporations stand up against those taken by their Western counterparts? The IPA conducted a survey spanning November and December of 2016, examining some 500 corporations with 300+ employees in Japan, the US, and three European nations (the UK, Germany, and France). The results appeared in the IPA's subsequent report: 2017 Fact-Finding Survey on Corporate CISO and CSIRT.

The initial point of comparison was risk assessment, the starting point for cybersecurity. Companies were asked to respond to the statement, "We analyze and evaluate risks concerning information security." Some 81% of American, 66% of European, and 55% of Japanese, companies agreed with the statement. Nearly half of all Japanese companies surveyed do not include information security in their corporate risk assessment (Figure 3-1)

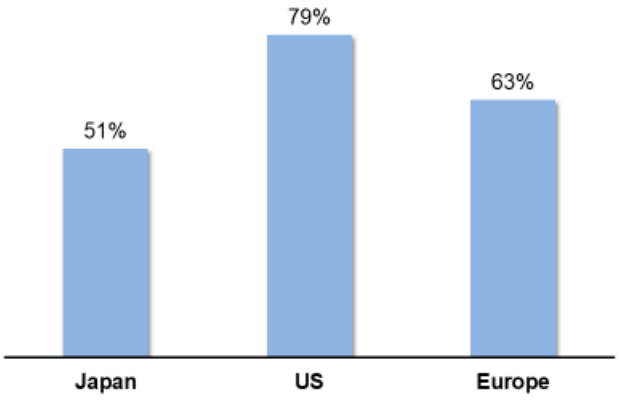
Surveyed companies were further asked whether they create cost estimates for damage from a potential cyberattack such as malware infection. Some 79% of American, 63% of European, and 51% of Japanese, companies indicated that they do specify such estimates (Figure 3-2). Half of Japanese companies fail to conduct risk assessment or estimate fiscal damage; moreover, some 27% do not evaluate the return from their security investment, compared to 3% of American, and 6% of European, companies (Figure 3-3).

Figure 3-1:
Companies that include information security in risk assessment



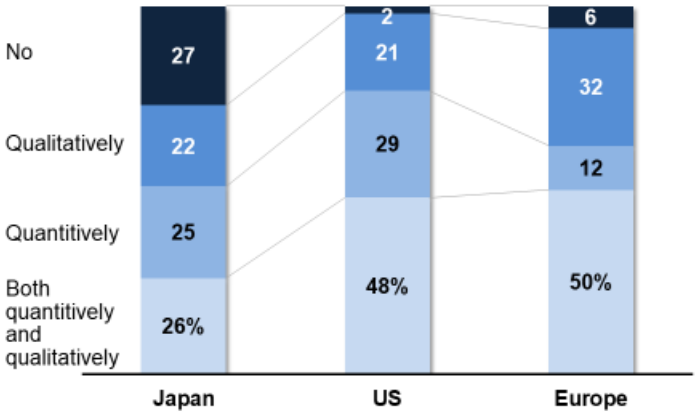
Source: Research on CISO and CSIRT 2017 (IPA; April 2017)

Figure 3-2:
Companies that estimate damage cost of hypothetical cyber attacks



Source: Research on CISO and CSIRT 2017 (IPA; April 2017)

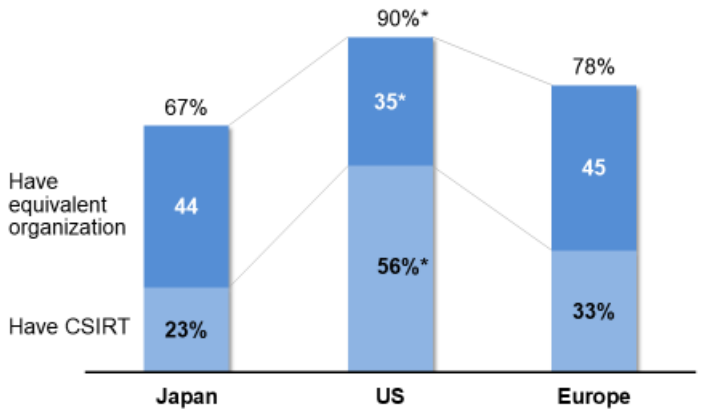
Figure 3-3:
Companies that assess cost benefit of security investments



Source: Research on CISO and CSIRT 2017 (IPA; April 2017)

The companies were next asked if they have appointed a Computer Security Incident Response Team (CSIRT) to handle a prospective incident. Some 56% of American, 33% of European, and 23% of Japanese, companies answer in the affirmative. Meanwhile, some firms indicated that, although they have not established a CSIRT per se, they have a similar entity. In total, some 90% of American, 78% of European, and 67% of Japanese, companies have established some type of cyber incident response entity (Figure 3-4).

Figure 3-4:
Companies that possess CSIRT or equivalent



** Sum does not match due to rounding of figures
Source: Research on CISO and CSIRT 2017 (IPA; April 2017)

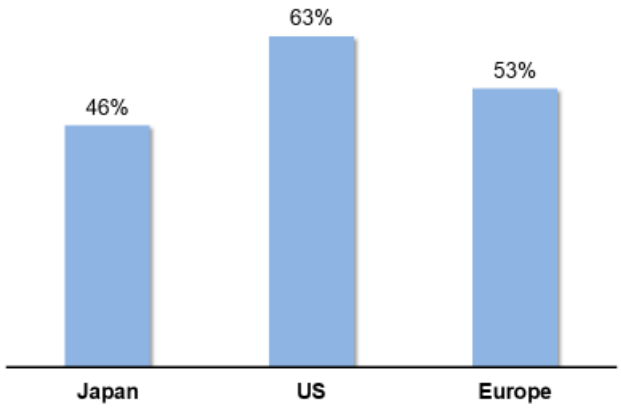
Special Focus: CSIRTS are proliferating

CSIRTs are organizational units established to handle potential information security incidents. “Handling” includes the chain of events from receiving the initial report of an incursion to conducting requisite surveys, and proactively minimizing the impact by involving related departments in emergency situations. The composition of CSIRTs varies. Some are comprised strictly of full-time team members, others are solely staffed by members concurrently holding other full-time jobs in the company, and the remainder reflect a mixture of the above two patterns. In times other than incident outbreaks (emergencies), full-time CSIRT team members work on other activities such as responding to in-house security-related inquiries, conducting education and training of employees, formulating new security rules, and supporting the CISO (Chief Information Security Officer).

The Nippon CSIRT Association (NCA) was formed in 2007 to support and advise companies interested in establishing a CSIRT and promote collaboration between CSIRTs themselves. Some 70 firms were listed as NCA members in 2014, increasing to 106 in 2015, 194 in 2016, and 272 as of January 2018, reflecting an explosive increase of CSIRTs in Japan from 2014. However, as some 2,000 firms belong to the first section of the Tokyo Stock Exchange, there is plenty of room for further expansion.

In the IPA survey, companies were also asked whether they have formalized guidelines for public disclosure of security incidents, as a part of preparing incident response. Some 63% of American, 53% of European, and only 46% of Japanese companies, responded that they have formalized such guidelines (Figure 3-5).

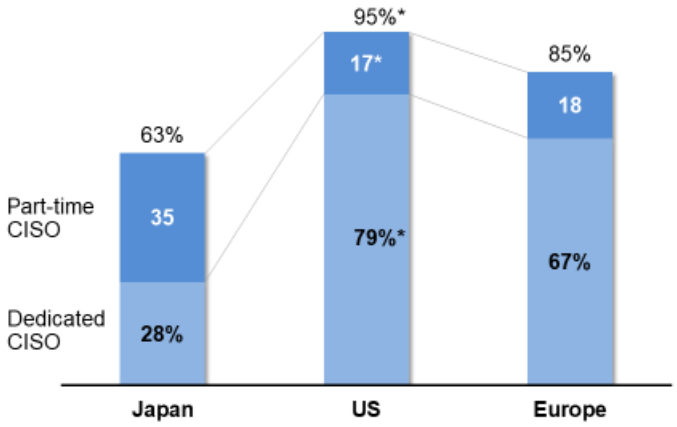
Figure 3-5:
Companies specifying disclosure criteria for cyber incidents



Source: Research on CISO and CSIRT 2017 (IPA; April 2017)

Differences were also noted in executive-level security structures. Companies were surveyed concerning the appointment of a CISO or similar individual. Some 79% of American, 67% of European, and 28% of Japanese, firms responded that they have appointed such an individual. In most Japanese companies appointing such an individual, the CISO concurrently serves in IT or risk management. In fact, when asked if the company has a CISO concurrently serving in another capacity, 17% of American, 18% of European, and 35% of Japanese, companies responded in the affirmative, reflecting a Japanese corporate tendency to create such a dual position at a rate roughly twice that of their Western counterparts. However, when comparing the total percent of firms appointing CISOs (either full-time or concurrently-serving), some 95% of American, 85% of European, and only 63% of Japanese, companies have appointed such individuals (Figure 3-6).

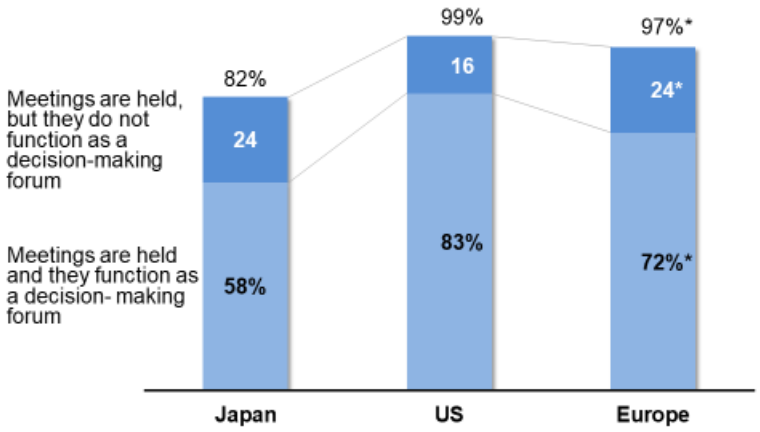
Figure 3-6:
Companies retaining a CISO



** Sum does not match due to rounding of figures
Source: Research on CISO and CSIRT 2017 (IPA; April 2017)

Companies were next queried about executive-level meetings to deliberate information security risks, responses and investment planning. The firms were asked whether they had created a specific opportunity, such as a regular meeting, where decision-making pertaining to information security occurred. Some 83% of American, 82% of European, and 58% of Japanese, companies responded that they indeed have (Figure 3-7).

Figure 3-7:
Companies with executive-level information security meetings



** Sum does not match due to rounding of figures
Source: Research on CISO and CSIRT 2017 (IPA; April 2017)

Based on the above responses, Japanese companies clearly lag behind their American and European peers from the three standpoints of risk assessment, incident readiness, and executive-level security structure. Just because few companies take security measures does not necessarily mean those measures lag behind, but there is a high probability that the level of maturity is currently lower among Japanese firms.

However, it is important to note that, as Japanese and Western companies operate in differing business environments, not all Western approaches may be effective for Japanese firms. For instance, many Western firms appoint full-time CISOs, whereas in Japanese firms, such individuals tend to serve concurrently in other capacities.

Western firms already have trained and experienced senior employees who can take over the reins of the company's information security. Also, we cannot overlook the fact that external labor markets for senior executive positions exist for Western companies, and that those firms have plenty of experience in external hiring of executives. As many Japanese firms have few trained senior cybersecurity human resources, as the external labor market is immature, and as there are few executives available for external hire, it is doubtful that the random appointment of a CISO would result in more effective business operations. Firms need to take approaches in line with their own personnel system and organizational structure.

In the next three sections, we will examine the imperative actions required of business executives, based on the status quo of Japanese companies.

2. Imperative action #1: Prioritize objectives to be protected, and implement layered defense measures

The keywords for this first imperative action are "prioritization" and layered defense." To repeat what has been said many times already, one cannot safeguard 100% against cybersecurity. With that accepted as a major premise, cybersecurity measures must be implemented, and is essential that consideration be given to prioritization of objectives needing protection and implementation of layered defense measures.

"Prioritization" means clarifying relative importance, as well as identifying which objectives must take a lower spot on the list. If no prioritization is provided by management, what would take place in security operations? For instance, let us assume that a company decides it will "absolutely not tolerate a data breach." Operational site employees may do their best to comply; however, if human

resources, materials, and money are not forthcoming, or an unrealistic security rule hindering daily business operations is enforced, the policy cannot be fulfilled. As a result, employees will lose respect for the rule and the company may ironically invite a data breach.

Another example milder than the above extreme of "absolutely not tolerating" a data breach might involve a policy to "do our best" to protect the company's safeguards. However, such a lackadaisical policy would require that all areas are fairly equally prioritized for protection, causing a situation in which vocal departments or individuals dominate. This approach will increase the chances for an attacker's success as he aims at wreaking major damage on a company or accessing valuable information assets. Any corporate policy which does not prioritize targets for protection is playing into the hands of attackers.

Achieving perfect protection is impossible, and the attempt produces a negative impact. I strongly urge management to employ straight-forward determination in their fundamental way of thinking. Executives exhibiting clear determination approach questions by asking, "What are the corporate crown jewels we seek to protect?" The answer to that, along with subsequent multilevel initiatives, enables creation of realistic and highly effective strategy.

It is vital to answer the question of prioritized targets for protection from a business standpoint. Yet, I do not feel it is wise to assume an information or asset management viewpoint in which management declares it will prioritize targets for protection among its data, IT devices, and tangible as well as intangible assets at plants and elsewhere. Most companies have "shadow IT," meaning data, IT devices, and other system assets unknown to the information division. An asset-based approach would initially require management to inventory their assets. Taking inventory is a good thing, but this inventory would show that important corporate activities involve a complex commingling of individuals and machines in a networked manner, and that advancing risk management incorporating suppliers and subcontractors is needed. Such an "inventory approach" would likely not be effective when considering expense and time involved.

Managers should adopt a business perspective considering factors such as corporate traits, identification and protection of elements providing a competitive edge, and future market trends, and including a realization of their own corporate risks. Managers need to begin by weighing risk scenarios, such as the competitive disadvantage of developing a new technology only to have it stolen, the danger level if main plant production were halted and product delivery delayed, or sales loss

level if an e-commerce site were disabled. Once that is done, they can recommend elements such as information assets, intellectual property assets, or plant operation management systems to be prioritized for protection.

It may seem difficult to prioritize targets for protection from a company-wide perspective, but when executives engage in a round-table discussion, priorities soon become clear. For example, one chemical products manufacturer acknowledged its lack of in-house cybersecurity professionals and debated priorities. It decided that protecting the plant control system was its greatest priority, while protecting the security of the corporate information system was determined to be of lower relative importance. Management accordingly decided that the system infrastructure supporting the corporate information system should be externalized to a public cloud source, with reliance on security offered by a cloud vendor.

In another example, when I asked the Asia regional security officer of a foreign financial institution what his firm was prioritizing for protection, his reply was immediate: "our money transfer system, payment system, and client information." His response may seem self-evident, but it is nevertheless crucial for management to list its priorities by relative importance and then translate those into corporate policy.

Next, let me explain the layered defense assigned to the prioritized targets for protection. "Layered defense" may not be a term with which everyone is familiar. Its meaning is extremely simple, signifying the multiple barriers functioning during the attack process, from the moment of its launch until the completion. Let us consider the simple example of safeguarding against a thief breaking into your home:

- Surveillance camera installation (general access prevention)
- Double-locking doors with chains (entrance protection)
- Unauthorized entry alarm (retreat effect)
- Safe for valuables (removal prevention)
- Valuables dispersal (isolation affect)

As the thief must penetrate all the barriers to succeed, it is likely that at least one safeguard will protect the valuables. Moreover, as thieves often scout out their target prior to an actual burglary, they are likely to be discouraged by safeguards clearly requiring effort and risk to overcome. It is possible to create a balanced policy combining layered defense and prioritized objectives for protection, implementing significant barriers for the most valuable objectives and lesser barriers for low-priority areas.

There is one further effect delivered by a layered defense. Since it requires the

attacker to penetrate one barrier after another before stealing the desired information and destroying software, the attack will take time. That enables detection and response, which will minimize damage. The next section shows that quick detection, response, and recovery is an effective approach in stalling the attack process.

The following steps exemplify barriers (countermeasures) for layered defense against malware attached to mail.

(1) Create e-mail settings for automatic incoming mail inspection, diverting mail from suspicious addresses.
(2) Check for clues such as filename extension (.doc, .xls, etc.) and attachment type, diverting suspicious mail and alerting the intended recipient.
(3) Ensure that security is alerted if any suspicious mail is opened to prevent others from opening that mail.
(4) Separate in-house networks to prevent widespread infection.
(5) Ensure that infected terminals will not transmit externally through detection and automatic interception.

These barriers, erected in order of priority, will help protect information handled by mail recipients.

As attack techniques are constantly enhanced, it is essential for layered defense barriers to be reevaluated as well. The WannaCry incident introduced in the Introduction was characterized by a worm targeting a specific vulnerability and directing infected computers to spread the infection automatically to nearby devices without the required step of opening any attachment. This implies that even if the company had erected an additional barrier against opened attachments, there would have been little to gain. Attackers are thus devising attacks to elude one safeguard after another; companies must similarly alter, which is to say update, their layered defense.

3. Imperative action #2: Readying for quick detection, rapid response, and recovery

The second imperative action is ensuring readiness to implement quick detection, response, and recovery. Accepting the premise that 100% safeguarding is impossible suggests minimizing, not preventing, damage. Attackers always gain internal access, so the job at hand is quick detection of the invasion followed by thorough and quick response to minimize damage.

"Malware" also goes by the term "computer virus." In order to avoid contracting the flu, we protect ourselves from the infectious virus by washing our hands, gargling, wearing a mask, and getting sufficient sleep. Nevertheless, the measures do not work 100% of the time. Cybersecurity is much the same; quick detection and quick "medication" are needed in the rare case that infection strikes.

The Japan Pension Service incident surrounding leaked pension information involved targeted mail sent on four occasions between May 8th and May 20th in 2015. Actually, the first round of suspicious mail sent by infected computers to targeted recipients on May 8th was detected. However, the supervisor did not share that information with others in the system, leading to subsequent episodes, with the final occurrence on May 20th resulting in a data breach involving some 1.25 million subscribers.

This was a case of quick detection but no successful response or recovery. Written reports by both the Japan Pension Service and an independent investigation committee established by the Ministry of Health, Labour, and Welfare concluded that neither response nor recovery were satisfactorily accomplished because: there was no CSIRT to execute response, countermeasures were not specified, and the fact that, despite a CISO with a delineated role, there was no substantial system in place for the CISO to distribute emergency directives. This indicates that the major failure of Japan Pension Service countermeasures was an organizational issue. Technical preparations are important, but organizational response capability is even more critical.

Moreover, regular in-house system data backup also aids rapid recovery. This is especially true of the recently popular ransomware; data backup facilitates effectively streamlined recovery.

We often hear that repetition of the PDCA cycle is generally effective in elevating organizational response capability when problems arise. Repeating the Plan/Do/Check/Action cycle helps companies learn from both successes and failures, enhancing corporate experiential wisdom. Nevertheless, this deeply familiar cyclical PDCA management tool is not easily adapted to cybersecurity. Cybersecurity has a different aim—responding to a threat—which does not correspond to the active "Do" in PDCA.

In order to elevate organizational capability in cybersecurity, PDCA should be replaced by the more appropriate cycle of: Strategy □ Implementation □ Training □ Evaluation. As noted in the previous section, "strategy" refers to prioritizing objectives to be protected in accordance with overall business strategy and forming a

corresponding layered defense. “Implementation” refers to the installation and management of security devices and mechanisms in accordance with the layered defense plan, and the readiness of the internal system, organization, and rules to ensure quick detection, response, and recovery.

As the next two steps of training and evaluation are extremely important, I would like to address them in some detail. Training examines whether the implemented system or mechanisms are functioning according to strategy. There are several types of training which I would like to introduce, as each has its own specific content designed for differing targets and purposes. The most common type is basic training of employees. Most companies incorporate security training into their novice orientation, but in some firms, security departments and CSIRTs visit each department and subsidiary offering focused training. Most sessions have employees respond to pseudo attacks and threats for firsthand experience. Pseudo fake mail is sent to participants to teach how to recognize it as suspicious. Employees also practice reporting an emergency upon receiving targeted mail or opening an attachment, allowing them to confirm to whom they should report, and with what details.

Another form of training involves CSIRTs or security divisions conducting major, company-wide sessions. Some are conducted in a simulative role play among employees without using IT systems, while others incorporate pseudo attacks on IT systems. The purpose of large-scale practice is clarifying mobilization and cooperation routines in the event of an incident. Simulations start with a pseudo attack. A report is communicated from the operational site to CSIRT and the security division. From there, general affairs, public relations, legal, personnel, and sales departments become entangled and active in the incident response.

Finally, evaluation is the process focusing on post-training assessment and consideration of improvements. Meanwhile, security level evaluation following a surprise pseudo attack is also very effective. “Penetration test” is the term referring to such evaluation. The tester is the pseudo attacker, who levies an attack on an employee and the corporate system. This enables any system or response weaknesses to become visible from a safeguarding/defense viewpoint.

There are two types of penetration tests: internal and outsourced. It may sound ridiculous to outsource a pseudo attack to reveal security weaknesses, but security companies include penetration tests billed as “gap analysis,” or “risk analysis advisories” in their service menus. The overwhelming benefit of outsourcing is to see the company from a potential attacker’s point of view. A secondary benefit is to learn

how one's company stands up against the industry. As security companies test multiple firms, they are often positioned to make intra-industry comparisons. As discussed in section 6 of Chapter 2, "Protection of trust," although no definitive answer exists for managers wondering how extensive protection should be, comparative information is valuable input for those making cybersecurity decisions.

It seems that very few Japanese companies have the human resources and teams to perform in-house penetration tests. Meanwhile, such in-house tests increasingly occur in Western firms, with teams safeguarding security being dubbed "blue teams," and those launching penetration tests known as "red teams." Upper management usually permits the latter to conduct attacks if they cause no real damage to the company. The penetration tests are conducted without warning, heightening their worth. Though not indicative of the norm, one security officer for a foreign financial institution declared that his firm had 150 red team members worldwide conducting 2,300 global penetration tests annually.

4. Imperative action #3: Periodic reviews at board and executive management meetings

The third imperative action is for the status of cybersecurity initiatives to be included on the agenda for periodic review at board and executive management meetings. Prioritized objectives and layered defense, and early detection, rapid response, and recovery should not be left to the operational site or related managers, but rather should be recognized jointly by executive management in toto. The third imperative action could be described as a policy ensuring that the first two actions deliver reliable results.

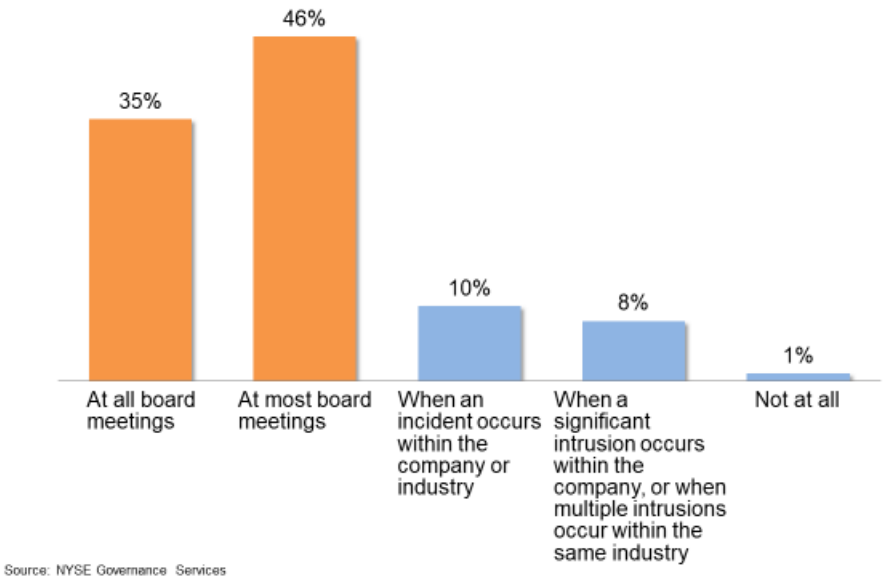
It is important for management to pursue cybersecurity measures and decision-making company-wide, but the content of those measures is even more important. If specific initiatives and discussion topics are not clearly stated prior to board and executive management meetings, they will gradually disappear from the agenda. For that reason, I would like to discuss how American companies, which lead in this area, debate these initiatives at their board meetings.

As you read, please remember that management and execution are clearly separated in American firms. Boards are generally comprised of external board members who are expected to oversee execution by executive officers on behalf of shareholders. On the contrary, board members and executive management members often overlap greatly in Japanese firms, with the roles played by board and executive management meetings varying from one company to another. For

simplicity's sake, this chapter refers to board meetings and executive management meetings collectively. The intended meaning is: what needs to be discussed and determined vis-à-vis cybersecurity from a management point of view, in order to supervise business operations.

In May 2015, NYSE Governance Services, a subsidiary of the New York Stock Exchange (NYSE), published results of a survey it had conducted of over 200 board members serving American companies. Some 35% of surveyed board members said they discussed cybersecurity at all board meetings, while 46% said they discussed it at most board meetings. In other words, over 80% of those surveyed said they discussed cybersecurity at practically all board meetings in which they participated (Figure 3-8).

Figure 3-8:
Frequency of cybersecurity discussion at corporate board meetings



Source: NYSE Governance Services

Precisely what, then, do they discuss at these board meetings? *Cybersecurity Oversight*, a publication issued by the non-profit National Association of Corporate Directors (NACD), offers some insight. The organization publishes a series of handbooks addressing points for board members to keep in mind in various areas as they go about their professional duties. Cybersecurity Oversight is the handbook covering board meeting discussions on cybersecurity. The five basic principles presented in the handbook are, essentially, as follows:

Principle #1: Board members should understand cybersecurity as a company-wide risk management issue.

Specifically, cybersecurity should not be undertaken from an IT viewpoint, but rather from strategic, cross-departmental, and economic viewpoints, and should continually be viewed not from the perspective of the company alone, but from that of the entire ecosystem impacting the company.

The handbook addressed the frequency of cybersecurity debate, recommending discussion by the full board at least once every half-term, with executives providing an overview. Furthermore, it recommended establishment of a cybersecurity committee, suggesting that it meets at least once per quarter.

Moreover, cybersecurity should not only appear on board meeting agendas on its own strength, but should also factor into discussion of such issues as launching new business and entering new markets, new product R&D, M&A, adoption of new technology, and investment in large-scale facilities.

Principle #2: The Board of Directors should understand the legal implications of cyber-risks in terms of the overall corporate situation.

The Board of Directors should understand the legal risks borne by the corporation, by individual board members, and by the directors as a group. As a protective measure against litigation, the handbook recommends that minutes taken of cybersecurity discussions at board meetings should be preserved, and that such discussions should be disclosed to shareholders as necessary, with important information communicated not as general remarks, but rather as individual incidents or lawsuits.

The handbook offered concrete examples of recommended information to be shared, such as frequency and seriousness of past incidents, likelihood of a future incident, estimated costs and damage associated with incidents, appropriateness of safeguards, and risk level of attacks.

Principle #3: The Board of Directors should have access to security experts, and periodically devote appropriate time segments to discussion of cyber risk management.

The handbook emphasizes the importance of listening to the opinions of experts. Board members themselves have no professional knowledge of cybersecurity, and no need to study the subject thoroughly. Instead, the handbook recommends inviting knowledgeable third parties such as security company professionals, members of the

security industry, or regulatory officials, to brief the Board.

On the other hand, if the Board does not possess updated information on its security status, it will not be poised to prioritize objectives for protection from a management standpoint, or approve decisions related to cybersecurity. Therefore, the handbook recommends asking questions such as those below to the executive officers:

- How well do the executive officers feel they understand the company's current cybersecurity status?
- What are the executive officers' insights into company directionality (priorities for protection, etc.) and operational site management (budget and protection system, subcontractors, etc.)?
- How sufficient are existing countermeasures in the event of an incident?

Principle #4: The Board of Directors must set an expectation for management to create a framework for company-wide cybersecurity management based on appropriate human and budgetary resources.

The handbook recommends that the Board of Directors set an expectation for management to protect company-wide resources sufficient to maintain cybersecurity. Specifically, management should organize a cross-departmental "cyber risk management team" incorporating members from business divisions, the legal and internal audit divisions, financial affairs, human resources, IT, etc. The team should formulate a cybersecurity implementation plan incorporating all divisions and gain consent to budget resources not only for the IT and risk management divisions, but for all divisions.

Principle #5: The Board of Directors should discuss concrete policies for cybersecurity risks, including which should be avoided, allowed, mitigated, and insured against.

As risk is a factor to be managed, the Board should not simply endorse cybersecurity risk avoidance, but should assess which risks are to be reduced, transferred, or accepted. Toward that end, the company's cyber risk tolerance should be translated into a company-wide business strategy supported by sufficient resource allocation.

Specifically, the handbook recommends clarifying the corporate crown jewels and priorities for protection. Once that is done, the Board should strike a balance between a basic policy for investing in risk mitigation, and a higher-level policy,

based on the priorities to be protected. Debate should include the possibility of transferring risk through options such as insurance.

Special Focus: Acceptance of remaining risk

A key point in Principle #5 is discussion of risk acceptance. The tendency in Japan is toward risk avoidance, so even when individuals discuss risk management, what they really mean is sidestepping risk. Policies reducing and avoiding risk should be balanced with an understanding of residual risk, which companies can attempt to minimize further, but ultimately must plan for in terms of estimated costs in the event of an attack. In other words, it is important for management to accept a certain level of residual risk. Management should not close their eyes to the reality that 100% protection is impossible, imposing limitless goals and responsibilities on operational sites. Management's acceptance of residual risk, after risk reduction, risk avoidance, and risk transferal measures, enables operational sites to fulfill their defined and limited responsibilities.

These are the five basic principles which (predominantly external) directors keep in mind as they participate on boards of American companies. Not all are applicable to Japanese companies, but all provide great reference for those participating in board and executive management meetings of Japanese companies which have generally not discussed cybersecurity issues to date.

We can expect to see a push for strengthened corporate governance in Japanese companies. This will increasingly include calls for management to explain cybersecurity to help fulfill the board's oversight as well as duty to shareholders. This implies the need for periodic review of corporate cybersecurity measures at board and executive management meetings.

5. The role of the CISO (Chief Information Security Officer)

We dedicated three paragraphs to discussing imperative actions for executives, but we also increasingly hear reference to CISOs, those ultimately responsible for corporate cybersecurity. In the first section, we indicated that Japanese companies lag behind their Western counterparts, with 63% of the former appointing a CISO (either full-time or concurrently-serving). Japanese companies tend to rely on a CISO's entire staff rather than on the CISO individually. What is expected of the role, whether held by an individual or a team, bearing responsibility for cybersecurity?

During interactions with Western CISOs, I noticed that their backgrounds tend to fall into either of two possible categories. One is that of a computer science specialist, an expert in IT and network technology. The other is that of individuals emerging from legal or risk management backgrounds. The majority seem to belong to the former category.

The position of CISO began to proliferate from the late 1990s. At that time, most experienced CISOs reflected a computer science background. Some served as CISOs in several companies, gaining experience in various industries. CISOs with fewer years of experience tend to join the ranks from the latter category: legal or management backgrounds. Indeed, when one of my non-technical friends was asked to serve as CISO for a certain company, he was thoroughly flabbergasted.

I find that the background and responsibilities of the typical CISO have evolved over the years, and that this position is by no means well established even in Western companies. In the late 1990s, the responsibility of the Chief Information Security Officer was as the title suggested: protection of internal information. The post required technical IT and network knowledge, and the capability to lead a cyber defense team.

The CISO's role has expanded; the chief is now expected to be a leader and coordinator in overall corporate management. Technical issues are now delegated to the CISO's team, while the CISO handles risk assessment for the company, requiring communication skills to negotiate and coordinate with other corporate officers.

The change in CISO qualifications and role seems to follow a change in corporate handling of cybersecurity. In the past, there was no reference to "cybersecurity." Instead, companies stressed "protection of corporate information" and "preventing external leaks." As discussed in Chapter 2 (Why Cybersecurity Is a Business Management Issue), however, as the business environment has rapidly "gone cyber," cybersecurity has moved into areas such as business continuity, protection of trust, and growth infrastructure.

Japanese companies rely more on the entire CISO team than on the CISO's individual attributes. The team's value is not limited to the CISO's qualifications, but also extends to a more flexible and broader area. What role, then, does the CISO's team play? It is not limited to data breach prevention, but also supports assessment of influence attacks might have on business continuity, creation of durable stakeholder trust, and protection of digital security vis-a-vis growth infrastructure, among other issues. However, exactly how should this role be

fulfilled?

I believe CSIRT creation is one of the most critical activities. As we discussed in the first Special Focus article of this chapter, the CSIRT is the in-house incident response team. If its members serve concurrently in other roles, they can function in task-force style in the event of an incident. However, I recommend a "pure" CSIRT of dedicated members who not only respond to incidents, but also handle in-house inquiries about the company's security, review corporate security policy, and organize in-house security education and training for employees. This will enhance the overall level of corporate security. What the company does on a day-to-day basis is key.

I believe that response to internal inquiries about corporate security is the most important activity among those mentioned above. This extends beyond inquiries from the IT division. The CSIRT should be the company's all-purpose security advisor. Digitization is progressing in almost every area comprising any business. The hiring process is going online in many companies, and many firms are using social media for marketing. The CSIRT can advise on security issues as each department takes advantage of digital technology. This CSIRT function is of great importance to every division of the company, and essential for corporate growth.

The importance of this advisory role extends beyond enabling each department to maintain corporate security. Responding to inquiries company-wide offers the CSIRT the important opportunity for real-time assessment of concerns and issues at various operational sites. Allowing team members such exposure facilitates more practical and fruitful education and training sessions.

Understanding operational site issues is also indispensable in creating and reviewing security-related rules. Most such rules typically hinder employees' everyday work. Restricting system usability with layered red tape requirements reduces work productivity. As too many rules can be annoying, employees may ignore or simply pretend to follow them at operational sites. At the same time, the CSIRT may approach its job somberly, only to end up with "security for security's sake," as operational site employees distance themselves from the imposed rules.

Sidestepping "security for security's sake" involves more than just responding to in-house inquiries by explaining the rules or insisting on adherence to them. Rather, it requires communication of their underlying intent and philosophy, and of how rules also benefit employees at the operational sites, suggesting an invitation to "share rules." If the CISO team can maintain the emphasis on "sharing rules," employee inquiries will increase, and the distance between the CISO members and

operational site employees will shrink. If the team questions whether existing rules reflect the reality of ongoing business, that is a signal that the team is maturing. If the rules do not reflect actual day-to-day business, they should be reviewed.

New problems arising at an operational site must be solved together. Rules should be created based on real concerns, reviewed when necessary, and utilized in employee education and training. Through the chain of events beginning with an employee inquiry, the security process can become a part of the corporate culture and merge with daily business activities. That is the key function of the CISO team.

What about contact between the CISO team and executives? Executives have overall responsibility for determining prioritized objectives, creating an organization and mechanisms capable of quick detection and response, and conducting periodic reviews for board and executive management meetings. How can the CISO team support these management activities?

In clear discussion of the three imperative actions for executives in the second through fourth sections of this chapter, we mentioned that issues must be put on the agenda for discussion at board and executive management meetings. Yet in order to advance frank discussion with everyone's participation, management must have some knowledge about cybersecurity. It is the important responsibility of the CISO team to ensure that management has this shared foundation of knowledge.

One way to create this shared foundation is to arrange a periodic cybersecurity discussion session for executives. One trick is to avoid board or executive management meetings for this session, instead choosing an informal setting in which discussion, not reports or deliberations, can be the focus. One company began such sessions originally focusing on IT, eventually dedicating two sessions a year to cybersecurity. Those discussions focus on current security issues, which might include how to handle recent increases in ransomware threats, or responses to increasing geopolitical tensions in East Asia. Such discussions held at appropriate intervals foster shared basic knowledge and awareness of issues within management ranks.

The second point is to create a common language among management. As we discussed in the Introduction, cybersecurity is difficult to understand, borrowing heavily from English ("malware," "incident," "CSIRT," etc.). Even among experts, terms like "operation systems" and "security personnel" can mean different things in different settings, keeping individuals on differing wavelengths. It makes joining such meetings challenging for executives with minimal knowledge of, and experience in, cybersecurity.

The National Institute of Standards and Technology (NIST, a US Department of Commerce agency) created the Cybersecurity Framework to serve as a shared language for managers. The Framework lists five core activities for corporations: identify, protect, detect, respond, and recover (Figure 3.8). These five steps are further broken down into 22 categories, which are further subdivided into 98 subcategories. (Note: NIST is currently revising its Framework, with the latest draft introducing 23 categories and 108 subcategories.) These categories offer detailed descriptions, but for executives, the major five categories of identify, protect, detect, respond, and recover sufficiently provide a common language. The Framework is an American publication, but METI includes it in its management cybersecurity guidelines (2nd edition, November 2017); it is being gradually adopted as a substantial global standard. Adopting this Framework for a common language is worth serious consideration.

Special Focus: NIST Framework

The Cybersecurity Framework was based on an Executive Order by President Obama, formulated through input from industry, standards organizations, and academic organizations, and published in February 2014 by the National Institute of Standards and Technology (NIST) under the Department of Commerce. The English version of the Framework can be accessed here: https://www.nist.gov/cyberframework.

The Framework was originally created for critical infrastructure protection, but was determined to be useful in other areas as well, and has begun to serve a central role in governmental cybersecurity policy.

The five steps (officially referred to as "functions") of identify, protect, detect, respond, and recover, with the further stipulation of 22 categories and 98 subcategories, describe exactly which initiatives are required. Companies need not adhere to the entire content, drafted as guidelines or standards; rather, the publication serves as a framework, allowing each organization to assess its own goals independently, evaluate its status quo, and take actions accordingly. The publication offers companies in discrete industries such as finance, telecommunications, IT, and petroleum practical examples of how to apply the content. NIST is enthusiastically helping the Framework to "go global," and is dispatching staff members to Europe, China, Japan and other countries to sponsor orientations. NIST staff have already conducted several orientations

and workshops in Japan since 2014.
The second edition is currently being planned (NIST refers to it as Version 1.1) and is targeted for publication in the first half of 2018.

Thirdly, role playing is an effective tool for use in cybersecurity training. I experienced one role-playing training event with the following scenario: A pseudo client declared that our pseudo company had served as a stepping stone for a cyberattack on the client's system. Apparently, a disgruntled employee had devised a cyberattack before resigning, and now we, the pseudo management, were instructed to generate a response and measures.

Participants were assigned to play the roles of executives including the CEO, CIO, and CISO, and those in charge of sales, personnel, legal and PR functions, among others. Solutions were to be discussed at an "executive management meeting." The training event only lasted for 30 minutes, but allowed participants to get a real feel for the process, including searching company-wide for the cause of the attack, determining factors in drafting a response, and choosing the role each corporate division should play. Many companies surely have annual retreats or training opportunities. Such gatherings offer precious opportunities to assemble all executives for discussion of a shared topic, and it might be useful to dedicate 30 minutes to a role-playing event shared by all executives. Surely the return and newfound knowledge would exceed the 30-minute investment of time.

Chapter 4: Collaboration with Other Companies

Companies can mitigate their workforce and resource deficiencies through mutual collaboration in information sharing and workforce development. As intra-industry firms have similar concerns, and greatly shared needs in terms of workforce and information, collaborating within an industry represents a practical first step. Sector-based Information Sharing and Analysis Centers (ISACs) have arisen within industries, and I recommend participation in, or formation of, one of these organizations.

1. The importance of information sharing

In the preceding chapters, I have reiterated that the offender maintains the advantage in cybersecurity attacks. All he must do is strike repeatedly, varying his method and tools until one offensive succeeds. The defense team, on the other hand, must succeed every time against every type of attack, or else suffer damage. I continue emphasizing why, structurally, the attacker has the upper hand. I have yet one more reason for this—the fact that attackers share information.

If they could capitalize on government back-up and a wealth of financial and human resources, they could unearth hidden vulnerabilities and devise unknown new attack tools. However, not all offenders have overwhelming R&D resources at their beck and call. Nevertheless, their ability to test all means of attack rests on their access to information about corporate software vulnerabilities and attack tools and methods.

Attackers benefit from an Internet-based black market that facilitates the exchange and sale of information. Also known as the “dark Web,” this black market usually lurks in a hidden domain which cannot be accessed through normal Web browsers. Once one enters the dark Web, however, all manner of attack tools await purchase. Information on newly-discovered software vulnerabilities, and attack tools for exploiting them, spread like wildfire on the black market. Usage of anonymous virtual currencies such as Bitcoin has simplified cash transfer, and the trend is accelerating.

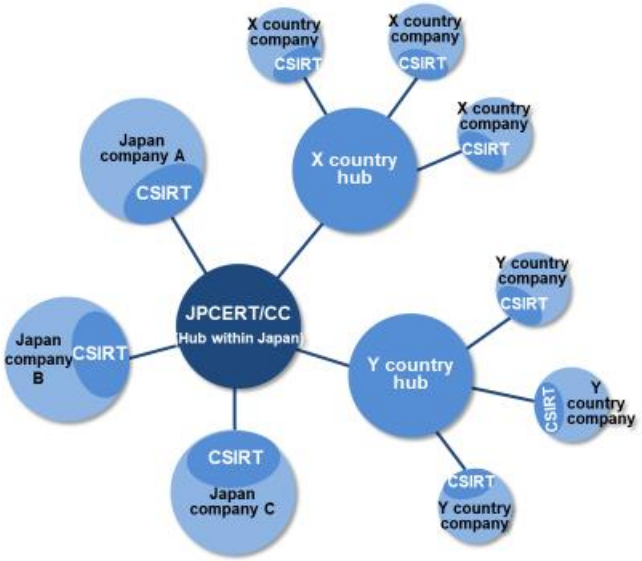
In the Introduction, I introduced the hacker group Shadow Brokers, which established a website in June 2017, about a month after the WannaCry incident, announcing online sale of attack tools for Windows 10 and smartphones, plus other items. Reports also surfaced that another black-market site had attack tool kits on

sale targeting Android OS ($50), Windows OS ($500), and iOS ($1,000).

Attackers have thus transcended a mere give-and-take of information to create a new mechanism for market-based attack information and tool transactions. You can now see why corporate defense requires a mechanism for sharing cutting-edge information as well. This serves not only for self-protection, but also to maintain awareness of launched attacks and to ensure launch of speedy response and recovery.

No sooner did society learn of cybersecurity and the need for shared information than grassroots and volunteer organizations sprang up to bolster cyberattack defense. Each company usually appoints a CSIRT as its contact point for sharing information with external sources, with the Japan Computer Emergency Response Team Coordination Center (JPCERT/CC) coordinating CSIRTs nationwide as an information hub. This system facilitates volunteer-based circulation of information, much like similar organizations found in most countries. JPCERT/CC also represents Japan as it liaises with corresponding overseas groups (Figure 4-1). The JPCERT/CC website provides the latest information on vulnerabilities, and issues alerts, all accessible to anyone at no charge.

Figure 4-1:
Information-sharing structure (conceptual)



JPCERT/CC announces specific new software vulnerabilities and increasing occurrence of a specific type of attack. It is extremely important for companies to

remain aware of the latest information, provided by JPCERT/CC, and to adopt the latter's recommended countermeasures. In the WannaCry incident in which attackers capitalized on a vulnerability in Windows OS, the world first learned of Microsoft's corrective program ("patch") in March 2017. Unsurprisingly, companies which suffered damage were those that failed to utilize the patch. Responding to the JPCERT/CC alert was the minimal step companies should have taken to ensure they did not invite similar damage.

On the other hand, the JPCERT/CC alerts remain insufficient to offset more complex attacks or attacks targeting specific industries or companies. For example, new types of illegal remittance malware are targeting the Internet banking industry, while novel forms of malware exploiting vulnerabilities in the unique systems controlling chemical plants are targeting the chemical industry. Intra-industry collaboration must occur to share information quickly and in sufficient depth. Information Sharing and Analysis Centers (ISACs) are organizations promoting such intra-industry cooperation.

2. ISAC initiatives in the US

The United States, well advanced in the cybersecurity field, naturally has its own versions of JPCERT/CC: US-CERT and ICS-CERT. However, JPCERT is an NPO boosted by governmental financial support, whereas US-CERT (the United States Computer Emergency Readiness Team) and ICS-CERT (the Industrial Control Systems Cyber Emergency Response Team) are government entities. In fact, these two organizations fall under the umbrella of the Department of Homeland Security (DHS), which oversees cybersecurity along with defense against threats such as natural disaster and terrorism. US-CERT and ICS-CERT function as security information-sharing hubs for computers and control systems, respectively. They also share information through the DHS portal site dubbed HSIN (Homeland Security Information Network).

US-CERT and ICS-CERT are by no means the only information-sharing systems in the US. In 1998, President Clinton signed Presidential Directive PDD-63 amidst growing awareness of the importance of supporting the critical infrastructure and incorporating sectors such as power, finance, and telecommunications sustaining the social base. This directive strongly encouraged the establishment of ISACs to support each segment within the critical infrastructure. And as we mentioned previously, these ISACs facilitate intra-industry sharing of information, its analysis, and ensuing results by member

companies.

There are no standards or government-sponsored certification processes governing creation of ISACs. Consequently, it is difficult to pinpoint how many ISACs exist in the US. What we do know, however, is that a National Council of ISACs (NCI) exists and functions as a liaison among the ISACs serving each industry. The NCI website lists 20 affiliated ISACs.

As the origin and history of each ISAC varies, as do corporate membership size and needs, ISAC activity is not uniform. One of the most active ISACs, the Financial Services Information Sharing and Analysis Center (FS-ISAC) serving the financial industry, maintains a busy schedule of information sharing and other activities supported by a full-time staff. FS-ISAC outsources the development of automated information-sharing software which it provides to member companies. It also offers this software to other ISACs. The organization proactively collaborates with overseas entities, including dedicated staff liaising with Japan's financial ISAC. Its annual general meeting is held in Florida and includes participants from Japanese financial institutions.

The Communications ISAC (National Coordinating Center for Communications) serving the telecommunications industry emerged before the Internet, back when the telephone was our prime communication tool. It was established jointly with the government to safeguard communication, which contributes to national defense by protecting against natural disasters and overseas attacks. It works in tandem with the government to maintain stable operations and services in the communications industry, gaining its ISAC label following President Clinton's 1998 PDD-63 signing. It works closely with DHS. Every Monday morning at 9am, for instance, it meets in a DHS agency building in a Washington, DC suburb, asking government agencies and major telecommunications carriers for updates on new threats to the telecommunications infrastructure.

What I am trying to emphasize here is that ISAC activity is not spearheaded by the government, but rather by industry. Although the Communications ISAC meets Mondays at 9am in a joint public-private sector meeting chaired by the DHS, the government participants depart after the meeting, allowing industry representatives to switch gears and engage frankly with member companies. I asked the DHS representative about this dynamic public-private cooperation. Ultimately, indicated the official, it is the private sector protecting and managing the telecommunications infrastructure. "The government has no choice but to trust the

word of the industry" was the exceedingly direct and honest response.

When I sat in on an NCI meeting, I had the similar sense that ISAC activity is spearheaded by industry. An FS-ISAC representative chaired the meeting, which featured a software demo for automated information sharing, impressions from the retail industry ISAC which had tested the software, and issues facing cooperation between regional (county/state) governments and ISAC. It was impressive to see how actively ISAC members participated, commenting on every topic raised at the meeting. The DHS representative functioned more as an observer, leaving actual debate to corporate participants.

The NCI meeting also included an explanation of Cyber Storm, a nationwide, government-led cybersecurity exercise. The DHS representative summarized the plans, and requested participation from all ISACs, spurring an industry member to ask, "Was there a post-mortem on the last Cyber Storm? What was learned from it? One hesitates to participate this time without hearing what was gained from the last exercise." That comment clearly demonstrated the industry's ownership over ISAC and its activities.

Both public and private sectors feel that industry should spearhead cybersecurity protection, as it is the primary owner, operator, and service provider of critical infrastructure. This shared belief comes through loud and clear in the tenor of discussion. Let me emphasize that in the US, cybersecurity activity begins with corporate self-help.

I would also like to mention another recent ISAC-related development: the Information and Analysis Sharing Organization (ISAO). ISACs work independently in their respective industries, as we have seen, but in early 2010, people began seeking options for companies unable to participate in ISAC. There was a firmly-rooted belief that ISAC favored larger companies, with small-to-medium-sized corporate members left behind from the get-go.

Awareness grew that ISAC was not serving the entire industry, and that society's overall cybersecurity would remain unprotected if the cybersecurity of ISAC's core of smaller firms was not ensured. As a result, President Obama signed Executive Order 13691 in March 2015 (Promoting Private Sector Cybersecurity Information Sharing), advocating for establishment of ISAOs. The premise behind ISAOs was provision of an "umbrella" for smaller firms unable to participate in ISACs, NPOs, and independent local community groups: a format for establishing independent groups in which cybersecurity information could be shared and analyzed. The rationale was enhanced cybersecurity for industry members and

others not covered by ISACs, and a new ecosystem producing a nationwide mesh of information sharing (be it through ISAOs or ISACs), upgrading US cybersecurity as a medium-term goal.

There are currently varied opinions on ISAOs in the US. “How do they differ from ISACs?” “ISAC members are intra-industrial, so collaboration comes easily, but ISAOs are a mish-mash of participants finding collaborative dynamism difficult.” There are already innumerable self-styled ISAOs, but time will tell whether they continue to spread in number. Meanwhile, the creation of an information-sharing ecosystem blanketing the US (for those not served by ISACs) offers not only a well-organized system, but also an example of how myriad techniques can effectively and practically disseminate, a point which Japan should well note.

3. ISACs and related organizations in Japan

ISACs serving individual industries (and like groups) sprang up in Japan around 2014, as word spread from the US. Some called themselves ISACs, while others serving essentially the same information-sharing mission did not. It is important and significant to note that ISAC-type activity is spreading in Japan. I was aware of the existence of five ISACs in Japan as of December 2017.

Finance ISAC

The Finance ISAC traces its roots back to 2012, when seven banks created its predecessor, the Cyber Intelligence Sharing SIG for Banks (CISS), as a private organization. About that time, illegal remittances began via Internet banking. The Finance ISAC was established in August 2014 as rival firms saw intra-industry cooperation as vital in dealing with tricky issues unrelated to IT such as customer relations and legal issues, and as they felt corporate status suited their ongoing group activities. The ISAC was launched with about 20 companies, ballooning to 320 by August 2017.

Activities are largely sustained by nine working groups, separated according to: (1) joint intelligence and (2) resource co-ownership. The former involves information sharing among members on incidents and vulnerabilities via “Signal,” an information-sharing portal established by JPCERT/CC. For example, if one member discovers a vulnerability, another might share his/her company’s approach and ask how others handled the same vulnerability, offering an active platform for information sharing and inquiries.

Meanwhile, preparation of handbooks and training exercises exemplify resource

co-ownership activities. Handbooks include collections of DDoS countermeasures and targeted mail countermeasures, while other publications feature good practice guides concerning illegal remittances. Joint training exercises have been organized annually since 2015, with some 200 firms participating in 2017.

Participants are in their late 30s to early 40s and represent various financial institutions, with most individuals bearing substantial business leadership responsibility in their respective institutions. The organization sponsors an annual day-long meeting, and conducts biannual two-day workshops in regional cities, ensuring opportunities to enjoy fellowship and exchange knowledge. Board Chairman Michihiro Taniai's motto is for members to feel "attached" to the Finance ISAC. The organization was established based on mutual trust and respect, building an environment for fostering collaborative activities.

The Finance ISAC proactively interacts with ISACs from other industries. Electric Power ISAC and Auto ISAC are invited as guests at Finance ISAC events. Meanwhile, Finance ISAC participated in the January 2017 ICT-ISAC training exercise, and the two groups regularly share information on illegal remittance issues. The Finance ISAC has a sister group relationship with FS-ISAC in the US, with a dedicated individual directing information from the US ISAC to its Japanese counterpart in a reflection of the close ties between the two.

ICT-ISAC

ICT-ISAC grew out of Japan's first ISAC, the Telecom-ISAC established in July 2002, and was incorporated in March 2016. Its members include the founding firms from the telecommunications industry, as well as broadcasting and security companies, and firms in system integration (SI), which is incorporated into the ICT field, encompassing a total of 34 companies as of October 2017.

Activities are conducted by individual working groups (WG). The ICT-ISAC was formalized to facilitate overall information sharing in the ICT industry, in addition to the pooling of specialty information in each member field. WGs reflect this, as they separately pursue ISAC-wide and specialty activities. ISAC-wide activities include anti-cyberattack training exercises, workforce development, and Wi-Fi literacy improvement, for example. The latter encourages public awareness of safe Wi-Fi use benefiting both users and providers in response to the recent upswing in public Wi-Fi. These activities are organized more for consumer benefit (targeting a safe ICT environment) rather than protection of participating firms. This sponsorship of activities benefiting the end-user is a distinct characteristic of ICT-

ISAC.

One of the specialized working groups within the telecommunications industry field organizes DoS attack response activities. As DoS attacks may occur at any time, the activity promotes information sharing within the four phases of prediction, detection, coordinated response, and review. Information sharing is an umbrella term, with its content and approaches differing from one phase to another. The prediction phase extends from two weeks to a few days prior to an attack, and includes information sharing concerning prediction or advanced notice of an attack and may ease the response phase for each company. The detection and coordinated response phases require speedy shared information in near-real time. Extra detection input allows all corporate employees to share information and enables the work group members to facilitate a countermeasure. The review phase requires a bit more time to share information on the attacker, attack technique, and any ensuing damage.

ICT-ISAC proactively coordinates and cooperates with other ISACs at home and abroad. For instance, the ICT-ISAC extended an invitation for the Finance ISAC to join in its February 2017 cyberattack training exercise. In November 2016, the group organized a trilateral discussion in Tokyo, inviting Communication ISAC and IT-ISAC from the US, along with Germany's eco (Association of the German Internet Industry). In 2017, Japan's ICT-ISAC became a partner of the US-based National Council of ISACs (NCI). The organization was notably praised overseas for its involvement in the Cyber Clean Center (CCC), launched in 2006 before ICT-ISAC evolved from Telecom-ISAC, and continuing through 2011. Supported by the Japanese government, Telecom-ISAC and JPCERT/CC informed victims that their computers were infected by malware and provided them with the tools to eliminate the infection. Some 76 ISPs and 7 security vendors participated, successfully decreasing the percentage of infected broadband users from 2.0 – 2.5% in 2005 to 0.6% in 2010.

Japan Foreign Trade Council (JFTC)-ISAC

The Japan Foreign Trade Council's (JFTC) information systems committee established the JFTC-ISAC in April 2016 amid increasing awareness that diverse and sophisticated attack techniques plagued trading firms, which had limited routes of information available to them. As of December 2017, 23 of the JFTC's 42 members had joined the new ISAC.

JFTC-ISAC sponsors an information exchange gathering for executives, as well

as a liaison session for staff, each meeting every other month. The executives' meeting features guest experts from JPCERT/CC and other organizations, who update members on recent trends and enhance their cybersecurity knowledge. Staff meetings involve workshops and group discussions where participants can share experiences and elevate their skill levels. The group interacts with other ISACs; in the autumn of 2016, for example, JFT-ISAC invited a lecturer from Finance ISAC to enlighten them on that group's training exercises.

These meetings are supplemented by day-to-day information-sharing activities using various platforms to share details on myriad types of threats. From its inception in April 2016 through August 2017, the group shared information on over 2,000 incidents of malware-infected attachments, vulnerabilities, and the like. The group follows the commonly-used Traffic Light Protocol (TLP) to ensure that sensitive information is shared within given limitations by the recipient, and shares information on threats and countermeasures to the best of its ability.

There are two major advantages to joining the JFTC- ISAC. The first is shared human and financial resources, as the group jointly supports extensive and sophisticated procurement, analysis, and provision of countermeasures relating to cybersecurity information. The second benefit is efficient capacity building. The ISAC office leverages its staff liaison meetings above all to help companies further develop their workforce, including fostering personnel networks. By-product benefits include knowledge about shared cybersecurity initiatives, helping companies understand how their own initiatives measure up against industry standards.

J-Auto-ISAC

Automobiles' electronic systems (for operation controls) and information systems (for entertainment) together comprise the in-vehicle network. These differ from normal information systems as they not only utilize distinctive technology, but also vary in detail from one auto manufacturer to another. Cyberattacks could both endanger driving safety and generate a data breach of passenger and other information. The Japan Automobile Manufacturers Association formed J-Auto-ISAC in January 2017 as a preventive measure against such an eventuality. The membership comprises Japanese OEMs.

The purpose of J-Auto-ISAC is to safeguard the security of onboard systems, but not to protect auto manufacturers' corporate information systems, plant control systems, or other related areas. J-Auto-ISAC's main activities are broadly divided into information sharing and investigative studies. The former focuses on

prevention and/or quick detection, supported through shared details on vulnerabilities in onboard software and IC parts, attack-related information, and technical countermeasures. Investigative studies focus on new hacking techniques introduced at domestic and global conferences, as well as examples of attack techniques from fields related to the auto industry.

Information sharing occurs in encrypted e-mails sent between the members and the J-Auto-ISAC secretariat. Specifically, the secretariat removes the sender's name from incoming information before sharing the mail with all members. Like the JFTC-ISAC, the Auto-ISAC follows the Traffic Light Protocol (TLP). It is important to note that the J-Auto-ISAC does not interfere with existing recall procedures; individual companies are responsible for reporting directly to the appropriate regulatory agency overseeing recalls when they occur.

J-Auto-ISAC has also been participating in the IPA-sponsored Initiative for Cyber Security Information Sharing Partnership of Japan (J-CSIP) as an auto industry SIG since October 2015, primarily to share information on targeted attacks.

JE-ISAC

The Japan Electricity Information Sharing and Analysis Center (JE-ISAC) was established in March 2017 in response to industry recognition that increasingly sophisticated cyberattacks impeded individual power providers from creating cybersecurity initiatives and conducting training exercises on their own. The new ISAC was established to share threat information, information analysis results, and information on appropriate and speedy cyberattack responses. As of March 2017, JE-ISAC included 26 power companies, with the Organization for Cross-regional Coordination of Transmission Operators, JAPAN (OCCTO) participating as a "special member."

JE-ISAC was created to provide and highlight pertinent information for members in a speedy and timely manner. This includes material available to the public as well as insights gained from the IPA-run J-CSIP, the NISC-run C4TAP, and other sources. To improve the information sharing infrastructure, the group also works to clarify the sphere and definition of shared information.

JE-ISAC also supports five working groups (WG): issue studies, best practice sharing, security education, security products, and security trends. The WGs additionally function to enhance mutual trust through face-to-face encounters among members. For example, in July 2017, the security trend WG sponsored an

event for some 30 participants from member companies and the ISAC secretariat to debate cybersecurity trends from the first quarter of fiscal 2017. The debate supported frank discussion on future threats and related countermeasures.

JE-ISAC outreach to international ISACs in the power industry and proactive engagement with trusted partners led to a friendship agreement with the European Energy Information & Sharing Analysis Center (EE-ISAC), signed in May 2017.

The above paragraphs have summarized the formation of ISACs in the five industries of finance, ICT, trading, automobiles, and electrical power. Similar organizations (which do not use the ISAC appellation) exist in industries for information sharing on cybersecurity. For example, the Japan Chemical Industry Association (JCIA) and the Japan Petrochemical Industry Association (JPCA) jointly sponsor regular information sharing opportunities for interested companies. These trends suggest that the number of ISACs, or ISAC-like activities, will continue to spread.

I would like to conclude this discussion of Japan's industry-based information-sharing initiatives by mentioning a committee transcending industry boundaries: the Cyber Risk Information Center (CRIC)'s Cross-Sectoral Committee for Cybersecurity Human Resources Development. This committee was established in June 2015 through the cooperation of some 30 companies in key areas of infrastructure including finance, credit, railway, aviation, electricity, gas, oil, chemicals, ICT, and medical care. Its focus was collaboration on capacity building as described in section 6 (http://cyber-risk.or.jp/cric-csf/membership.html), but the committee also conducts monthly activities to promote information sharing.

The monthly meeting fosters information exchange on corporate cybersecurity systems, employee training, and innovative ways to brief senior management on security-related issues. It also sponsors occasional study groups, inviting guests from a variety of ISACs to discuss cybersecurity topics. This Cross-Sectoral Committee differs from typical ISACs. Rather than focusing on speedy information exchange on vulnerabilities and cyberattacks as ISACs typically do, it includes members from the operational site in the discussions, thus fostering inter-industry comradery.

The Cross-Sectoral Committee aims to acclimate participating companies to information sharing and its format, and to increase their awareness of ISAC activities in other industries. The hope is that committee participants will create and help spread ISAC-like activities in their respective industries. This bottom-up

activity is also expected to promote information sharing across the entire industry, thereby strengthening cybersecurity for all.

4. Identifying what to share

As we have noted, information sharing has begun among companies within individual industries in Japan. I recommend that companies in industries with initiatives in place become participants; if initiatives are not in place, I suggest companies reach out to similar firms to begin the process. However, information sharing should not be the goal, but rather the means for achieving a goal. The phrase "information sharing" is simple enough, but if companies do not specify what information is to be shared, and how and why they choose to share information, they will likely remain at cross purposes.

For information sharing to succeed, it is vital for companies to identify two points concerning proactive use of that information: (1) what information is needed from other firms and (2) what is expected from information sharing with other firms. This specifically illustrates our discussion of the three imperative actions for business executives discussed in Chapter 3. I would like to reemphasize that before companies can establish means for information sharing, they must first engage in their own individual cybersecurity initiatives, and proactively put their own information to use.

Now let us examine exactly what information sharing entails. In the second section which discussed ISAC initiatives in the US, I introduced the ISAO. The ISAO Standards Organization (ISAO-SO) promotes ISAO activities. In September 2016, the organization published guidelines (ISAO 300-1: Introduction to Information Sharing) to help groups establish and operate information sharing entities. The IPA subsequently translated and posted these guidelines in Japanese: (https://www.ipa.go.jp/security/publications/isao/index.html). They cover the various purposes for acquiring information, classified into three areas: (1) for situational awareness, including a grasp of new threats; (2) for decision-making on action-taking; and (3) for execution of such actions.

To facilitate situational awareness, companies may seek information on current threats, further highlighted by information on vulnerabilities and threat actors. To facilitate decision-making for in-house action, firms may seek information on coping measures for security threats and incidents, and on practical steps for managing security systems. Finally, to facilitate actions, firms may seek information on tactics, techniques, and procedures, or "TTP," as it is commonly known.

Special Focus: Types of shared information

The ISAO-SO Guidelines define and categorize the shared information as follows:

- Indicators: Indicators include information enabling early detection, or that relate to the source of the attack or hijacking, the IP address which should be treated as suspicious, phishing mail content, malware hash value, etc.
- Vulnerability: Vulnerabilities found in specific software and information concerning the level of threats they represent.
- Courses of action: Recommended countermeasures for threats and incidents. Blocking specific IP addresses, limiting application usage, and other specific actions.
- Incidents: Wide-ranging information on incidents. Sensitive information on surveys and previous countermeasures, information on finance and decision-making, most of which involve shared experiences.
- Threat actors: Information on individuals who perpetrate attacks and incidents with ill intent.
- TPP (tactics, techniques, and procedures): Information pertaining to the actions of attackers. Specific attack methods and tools, as well as vulnerabilities that invite attack.
- Campaigns: Wide-ranging information including attack targets and tools, attacker profiles, and related incidents.
- Analytical reports: Reports supporting rapid and strategic decision-making as well as information on individual incidents.
- Threat intelligence reports: Reports detailing current cyber threats from security companies, public organizations, NPOs, etc. Also includes detailed analyses of specific incidents and documents providing predictive insights.
- Security advisories and alerts: Newly-confirmed major vulnerabilities and other information provided by the key international group CSIRT, and by software companies, security companies, and other organizations. In Japan, such information is primarily issued by JPCERT/CC.
- Operational practices: Records of effective and ineffective practices and measures used by members in security systems as solutions to specific issues. Includes cases involving personnel deployment as well.

5. Trust is the key to success

What is the key to success in information sharing? Trust is the answer most often given. For example, Finance ISAC management uses various methods to garner fond attachment from its 320 corporate members and works hard to instill a feeling of unity and communication within the group.

I moderated a panel discussion on critical infrastructure protection sponsored by the Japanese government for the 10 ASEAN member nations (Association of Southeast Asian Nations). The members all agreed that a relationship of trust was the key to information sharing initiatives in their countries. The Western participants nodded and agreed, indicating global recognition that trust is indeed the key to success.

This is a bit of a digression, but the representative from one of those ASEAN nations compared "the volume of beer enjoyed with a colleague to a relationship of trust. Simply sharing a beer gets things started." While drinking beer together is a fun way to facilitate mutual trust, instead of gathering strangers to create a group for information sharing, a more practical approach would be to leverage an existing group in which trust is already present. As we saw in section three highlighting ISACs and related organizations in Japan, creation of a WG for information sharing on cybersecurity within an existing industry organization is a practical and smooth approach.

If there is no existing group or organization providing such a foundation, a careful approach is required in establishing new information-sharing initiatives. For instance, as the abovementioned Cross-sectoral Committee for Cybersecurity Human Resources Development was a new group, they adopted a slow and detailed approach to build trust among corporate members. Specifically, they invited courageous volunteers from the 30 original corporate members to discuss their initiatives. Initially, one or two members at each meeting provided a company-approved description of their cybersecurity system and history. Over the course of about a year and a half, participating management leaders grew acquainted, and executives from each company began to meet and further their relationship of trust.

ISAO 100-2: Guidelines for Establishing an Information Sharing and Analysis Organization (ISAO), published by the ISAO-SO, also emphasize the importance of establishing a relationship of trust. The Guidelines offer specific hints for achieving that relationship, listed here in brief:

- Identify a leader for the group.
- Launch the group with a small number of companies.

- Ensure that membership is comprised of interested people who share common needs.
- Launch the group with members from trusted organizations and corporate entities.
- Aim for a group with shared empathy and support, one that others will be tempted to join.
- Periodically reiterate rules to protect trust among members.
- Track and measure the mutual levels of trust over time to assess how they impact member actions, periodically sharing the results with members.
- Make any rule infringements transparently known and take corrective action. Never deny any such infringement.

Whenever information sharing is discussed with another company, acknowledge that there will be occasions when mutually-important information is shared and occasions when it is not. Discussion should probe how shared information will be utilized. If the other company requires differing information, it might be proceeding with cybersecurity initiatives in a different manner from one's own company. Pursuing why the other company needs that information and how it will be used may spotlight a new initiative not yet taken by one's own company. Improving oneself through shared partnerships is one benefit of information sharing. Maintaining a spirit of mutual betterment among participants contributes greatly to a relationship of trust.

6. The importance of collaboration in capacity building

While the importance of cybersecurity is clear, the shortage of human resources is a shared concern of most companies. Survey results published by METI in June 2016 indicate that as of that year, there were only 280,000 individuals available to fill some 410,000 security positions, revealing a shortage of 130,000 persons. Moreover, the shortage was expected to increase to 190,000 individuals by 2020.

Capacity building is something that individual companies need to work on for themselves. However, many of these concerns shared by firms can generate solutions through inter-company collaboration. In security, for example, establishing a human resource network transcending individual corporate frameworks proves extremely useful in the normal business environment as well as in emergencies. In the information-sharing initiative mentioned above, participants not only enjoy information disseminated among all participants in the group, they also benefit from shared private insights resulting from a relationship of trust. Such

personalized information and the human relationships supporting it come in handy in times of trouble. There is a great benefit for companies proactively supporting security personnel willing to foster external human networks—support which can be manifested both financially and through modified working conditions. Sharing workforce development study materials and curricula, and sharing educational and training opportunities for general employees, may also answer mutual needs.

Furthermore, Japan's personnel system is structured such that many individuals without security experience are undoubtedly transferred into the security department, causing worry about how to prepare for the job. They can always ask senior departmental members for help, but for in the industry at large, others have overcome similar concerns in the past. Having individuals with similar experience from various companies contribute toward a booklet to help train individuals newly assigned to the cybersecurity field might be effective. Topics could include neophyte mistakes and how to overcome them along with a list of introductory learning material. The title of the booklet could be: "For executives suddenly assigned to a security position despite little experience."

Going a step further, companies must facilitate personnel exchanges and active nationwide training of what is now a deficient workforce. This can also illuminate a security path and future growth for security professionals in the industries.

An increasing number of students are interested in cybersecurity, as evidenced by establishment of the security department at the National Institute of Technology, Tokyo College and other developments. Once they see the various career paths available when they graduate and enter the security profession (remaining with a single company or experiencing a progressive career with multiple transfers), they will surely find increased appeal in the security field. With this long-term view in mind, companies should indeed focus on interactive experiences for the corporate security workforce. Personnel exchange will allow returning employees who experienced other companies to benefit from the external human networks mentioned earlier.

The government is keenly aware of the nationwide shortage in human resources within the security field and has developed policies geared toward capacity building. These will be discussed in Chapter 6, which deals with Collaboration with Government. However, the workforce development policies created in each government ministry, the human resources cultivated by universities and other educational institutions, and the needs of industries may not necessarily harmonize. The single concept of "security personnel" accommodates various occupational

categories and personnel profiles. Corporate personnel needs also differ based on business content and the specified “objectives for protection.” One important topic is the need for a definition of the human resource profile sought by each company, and corporate cooperation to give a clearer picture of the specific workforce deficiency faced by the industry.

7. Specific capacity building sites

Let us examine some security human resource development initiatives involving industry cooperation and which may be effective in capacity building. First, I recommend utilization of industry-specific ISACs. For example, one of the ICT-ISAC’s stated goals in sponsoring training exercises was capacity building. The outreach sought to cover the three existing shortages (personnel, development opportunities, and trainer resources) through table-top exercises with participants from other firms, with the focus on incidents not arising during normal security operations. Assuming a large-scale cyberattack impossible for a single company to stage allows for liaising between colleagues, fulfilling participant needs, sharing know-how among participants, and improving individuals’ skills, all of which contributes to capacity building based on practical experience.

Even ISACs which do have no direct capacity building outreach (as do ICT-ISAC and Finance ISAC) can expand their network of known professionals when corporate representatives meet and can learn from each other through repeated information exchange. As we saw with the JFTC ISAC example, ISACs are forums for capacity building as well as for information sharing.

I recommend taking advantage of the capacity building program sponsored by Nippon CSIRT Association (NCA), which was introduced in Chapter 3. The organization offers a two-night, three-day training retreat twice a year, built around the four parts of organization, operation, technology, and law, for those interested in establishing a new CSIRT or helping an existing one to mature. Even those who are not members of the NCA may take part in the event, which includes role playing in pseudo incident responses, group debate, and networking among participants. A friend of mine who participated in a past retreat commented that he still sees individuals he met during the event some years ago. Offering individuals who normally stay close to home the opportunity to develop extra-corporate relationships and broaden their scope for sharing advice is another important aspect of capacity building.

It is also effective to send human resources to universities for additional higher-

level education. In the cybersecurity field, the Institute of Information Security (IIS) can be described as a trailblazing post-graduate university. Its adult-education courses either comprise a master's degree program or form a set of intensive courses, often leading to a certificate. Master's degree courses offer night and Saturday classes which enable the students to continue their day job. As a result, over 80% of the 40 or so students entering each year are working adults, a third of whom come from the government, and two-thirds from private companies. The latter include not only ICT companies, but also a broad range of firms representing manufacturers, finance, logistics, and media. Some 40% of the students are in their 30s, and 20% in their 40s or beyond, mostly representing mid-level positions in their respective organizations.

Intensive adult courses cover topics such as establishing a CSIRT, security-by-design, practical cyber range (virtual environment for cyber defense) training, and other specific, hands-on, short and intensive courses typically offered over two to four days. Whether through a master's program or an intensive course, students find the opportunity to network with fellow participants, with lecturers also representing the forefront of corporate cybersecurity. These valuable connections made outside the company can be solidified even after individuals complete their courses and return to their firms.

8. Cross-Sectoral Committee for Cybersecurity Human Resources Development

I would like to conclude this chapter by touching briefly on the Cross-Sectoral Committee for Cybersecurity Human Resources Development mentioned earlier. This entity was formed in June 2015 by members representing critical infrastructure companies across the industry to help solve the cybersecurity workforce development problem recognized by the entire field. It is currently a general incorporated association and welcomes new members who agree with the spirit and purpose of mutual aid and the membership fee.

As mentioned earlier, the simple term "cybersecurity personnel" embraces many types of profiles, and profiles sought by individual companies vary even further. The Cross-Sectoral Committee sought to define the profile of individuals sought by companies as its initial goal. At that time, it took into consideration unique traits in Japanese personnel practices, such as the fact that many individuals given supervisory roles or appointed by CISO may experience a job transfer every few years or may lack experience in the cybersecurity field, and the committee tried to

emphasize that ideal capacity building methods should incorporate these traits.

Many Western corporate capacity building policies focus on the individual, questioning what skills the individuals need to have. Japanese companies, on the other hand, strongly focus on the skills of the team or organization. The Cross-Sectoral Committee thus takes a different approach from similar groups in Western countries, with an initial focus on the definition of organizational requirements common among each company's information system division.

"Organizational Requirements Definition" is a phrase we do not often hear. This specifically refers to each organizational unit handling corporate information security (IT project and system development, infrastructure operations, etc.), and the clearly-defined security-related tasks handled by each, thus defining individual missions. There are more than 50 such business tasks, and each is quite specific. For example, tasks for IT Planning would include considering how to implement cybersecurity insurance, while a System Development task would include a secure design for the requirements definition and basic design.

To execute each of the 50 or so security-related functions, the Cross-Sectoral Committee then defined function implementation roles, with the organization's management and supervisors clarifying what skills and abilities were required in terms of function classification and knowledge. For example, the function of considering the purchase of cybersecurity insurance requires responsible decision-making based on knowledge of the companywide system status quo. Through this process, the grouping of organizational unit – function – role (supervisor) – function classification/required knowledge – skill set can be clearly documented. The outcome of this process is referred to as Organizational Requirements Definitions. The outcome of this initiative was published in the September 2016 as the Cross-Sectoral Definition and Reference of Cybersecurity Professionals Based on Functions and Missions. (See http://cyber-risk.or.jp/index.html)

Jointly creating the Organizational Requirements Definitions resulted in a foundation that allowed companies participating in the committee to share human resource images on a detailed level, describing a personnel profile in terms of which organization unit it belongs to, what its responsibilities include, and what skill set it requires. The challenge required steady and meticulous work, but the resulting effect is amazing. The labor pool which previously did not match the label of "cybersecurity personnel" can now be defined specifically in accordance with the Cross-Sectoral Committee's "Definition and Reference" guide, and as a result, the foundation for capacity building can be shared across industries.

External development training used by the Cross-Sectoral Committee member companies can now utilize common expressions for assessing personnel profiles during information exchange, such as: Training A will be useful as it teaches XX skill to the supervisor of XX function in XX department. Making use of this situation will allow for creation of databases for every type of training in the market. The Cross-Sectoral Committee is also promoting common use and exchange of curricula and programs maintained by each company for education and training.

The Cross-Sectoral Committee also stated that one of its major goals is to contribute to the cybersecurity capacity building pursued by member companies, and that as a medium-range goal it hopes to clarify specific needs of industries and strengthen industry-academia-government cooperation. In terms of government outreach, the Cross-Sectoral Committee hopes to recommend industry needs for inclusion in capacity building policies created by each government ministry, and similarly make recommendations for university curricula and endow university chairs. Finally, the Cross-Sectoral Committee aims to promote united and harmonized industry-academia-government capacity building initiatives in which the career path of cybersecurity personnel in education, recruiting, assigning, developing, and transferring creates a single cohesive ecosystem throughout Japan.

Chapter 5: Global Management

Dealing with cybersecurity from a global standpoint is necessary not only for multinational companies, but for industry as a whole. Global security governance of one's own company is essential. Moreover, it is important to strengthen the supply chain and contribute to international policy harmonization, as Western companies have done.

1. Hot topics among global CISOs

There is a group in the US designated "Security 50." It is a community of CISOs who gather from global corporations (representing finance, automobile manufacture, machinery, energy, pharmaceuticals, consumer goods, retail, IT, and telecommunications) to exchange insights. "Security 50" met in early 2017 to discuss topics they deemed important, and arrived at the following conclusions:

Point #1: Geopolitical risk response

As demonstrated by the new US government, uneasiness surrounds the question of how global political uncertainty and changing policy priorities will impact cybersecurity initiatives. For example, worries persist about whether cybersecurity initiatives will be mandated with tighter regulations among businesses from every nation. If they are, what form will they take? Furthermore, what effect will unpredictable nations such as North Korea, Iran, China, and Russia have on geopolitics, and how will that impact the global cybersecurity threats? These are some of the concerns.

Point #2: Enhancing information sharing

Major Western firms have already been sharing information on a volunteer basis through ISACs and other channels, and many have taken advantage of commercial information services offered by security companies. To ensure a multilayered approach, some proactively create cybersecurity initiatives jointly with an external partner. These partners may be rival firms, for example. The top strata from a specified few firms gather for deeper information exchange within intra-industry ISACs. They are also creating such relationships with their clients. In terms of the information exchange mentioned above, one CISO commented that information sharing is an essential component of fulfilling their mission, while

another said that half of his/her time was spent building relationships of trust.

Point #3: Handling the IoT and the supply chain

As many devices and components have latent vulnerabilities, companies must accept that their products and services have vulnerabilities which transcend corporate lines and national borders. Moreover, as new technology races forward, security threats are spreading into all industrial areas. CISOs of multinational corporations share this perception. One commented that while the threat to IoT is just now gaining awareness, it will spread explosively from here on out.

Point #4: Technology advancement "catch-up"

One sees dual sides to this issue: hope and worry. While CISOs see themselves as leaders producing and elevating in-house security to respond to maximized threats, they also realize that this will require constant innovation. CISOs thus embrace new technology, and many at the recent meeting said they look forward to putting it to proactive use. On the other hand, some CISOs said they would put the standard cybersecurity playbook to work, but that attackers would not similarly limit themselves, leaving CISOs nervous about how to stay one step ahead of ever-evolving offenders.

These were some of the concerns of CISOs at multinational Western firms expanding global business, and I presume their counterparts at globally-expanding Japanese firms feel much the same. Meanwhile, those at Japanese companies growing primarily in the domestic market certainly echo these fears. Most attacks are launched from outside Japan, as parts, material, and raw material procurement involves business with entities across the globe.

This chapter looks across national borders to introduce trends among foreign governments and businesses. That will enable us to see how Japanese businesses, which transcend the nation's boundary to participate in global management, should take on cybersecurity.

2. Policy trends in various governments

The US is said to receive more cyberattacks than any other nation on Earth. Similarly, more attacks reportedly originate from the US than from any other country. However, one supposes the latter, as more ICT assets (data centers, etc.) are located in the US than elsewhere (conveniently serving as stepping stones), and not

necessarily because more attackers themselves reside in the US. However you assess it, the US market is the center of cybersecurity action, both for attacks and protection. Let us therefore move directly to US government trends.

American cybersecurity policies really got off the ground during the Clinton presidency, when the Internet began to spread. Since then, policies have been driven in a bipartisan way involving Republicans and Democrats through the George W. Bush and Obama tenures. As a result, the Trump administration has not greatly rocked the boat. One reason is the Congressional elections paralleling the presidential election in the fall of 2016; as Congress shoulders the greatest cybersecurity policymaking burden, the reelection of most of its members who were on the ballot in 2016 kept those policies stable. On May 11, 2017, the Trump administration issued Executive Order 13800, retaining most of the Obama administration's cybersecurity policies.

Executive Order (EO) 13800 rests largely on three pillars. The first is strengthened protection of the federal government itself. Each department in the federal government is required to utilize the framework of NIST (the National Institute of Standards and Technology, introduced in Section 5 of Chapter 3, entitled The Role of the CISO, or Chief Information Security Officer), with each Secretary naming a departmental cybersecurity supervisor. Individual departmental initiatives must follow the presidential directive to create "one enterprise," a single unified defense policy. The executive order also specifies consolidating networks used by all departments and consideration of shifting ICT assets to the cloud.

The second pillar supporting EO 13800 is protection of critical infrastructure. The new administration specifically highlighted three ways this might be done, vowing first to continue support of efforts by businesses which the Obama administration defined as critical infrastructure companies. Secondly, the administration added it would seek international support for and continue to implement countermeasures against "bot" networks (or "botnets;" see section 5 of Chapter 2 - "Reason 1: Business continuity") and initiatives related to industrial interdependence, such as impacts on power systems and other aspects of social infrastructure. Thirdly, it would strengthen the protection of defense-based industries. In a seminar held after EO 13800 was signed, a senior White House officer commented that international botnet policies commanded the highest priority among the three goals.

The third pillar is international cooperation and capacity building. The former

targets formation of international norms, attributions, criminal investigations, and other new areas such as rules to be promoted in initiatives mostly adopted by allies. Meanwhile, the Department of Defense will liaise with other departments on capacity building, assessing conditions in the US and overseas, and devising cybersecurity resources development plans to accommodate the gap.

Reading through the details, the executive order seems to sustain Obama policies while infusing them with the Trump administration's priorities of "America First" and homeland security protection. Moreover, one notes appointments of individuals with military experience for cybersecurity oversight, a tendency expected to encourage adoption of military procedures in the civilian sector. In terms of emphasized cooperation with allies, I believe the US will likely ask Japan for greater contributions to, and cooperation with, cybersecurity within the context of the Japan-US relationship.

The European approach is to promote country-specific policies along with those of the European Commission (EC), which sets overarching strategy and directionality, followed by legislation and enforcement in individual countries. Along those lines, in 2013, the EC simultaneously announced dual policies—the Cybersecurity Strategy of the European Union and the Directive on the Security of Network and Information Systems (abbreviated as the "NIS Directive"). These are being turned into legislation in each country and are scheduled for implementation by May 2018. The latest development is the EC's September 2017 comprehensive strategy, abbreviated as the "Cybersecurity Package." Its three main pillars are: (1) building resilience to cyberattack, (2) creating effective cyber deterrence, and (3) strengthening international cooperation on cybersecurity.

The EC intends to achieve the first pillar, building resilience to cyberattacks, by identifying and strengthening the European Union Agency for Network and Information Security ("ENISA") as the core EU organization. ENISA (https://www.enisa.europa.eu/about-enisa) was originally a provisionary group within the EC, established in 2004 and directed to advise individual member nations and conduct research, somewhat like a research institute or think tank. The new strategy redefines ENISA with permanent EC status, reinforcing its budget and manpower, making it an EU advisor providing cybersecurity policymaking advice to each member nation and arranging a certification system, as described below.

"Building resilience to cyberattacks" will be realized through creation of a common certification framework of ICT product and service security. The plan is extremely ambitious. Countries with certification systems already established in

specific industries will see those systems incorporated into the new framework. Countries without such certification in certain industries should not create them, but rather adhere to the new shared certification framework. When I was in Europe and asked those involved about the plan shortly after it was announced, however, many seemed to doubt its feasibility.

The EC not only announced its new certification framework, it also targeted May 2018 for compulsory implementation of the Cybersecurity Strategy and the NIS Directive (the dual EC policies announced in 2013). Moreover, the EC plans embrace a new system for speedy, collaborative response to large-scale attacks in each country, continued promotion of the 450-million-euro investment into public/private sector R&D as announced in 2016, and workforce development and general consumer education, among other initiatives. The first pillar, then, essentially strengthens previous policies, proposes cooperation among European countries, emphasizes commonality and sharing whenever possible, and in a sense, follows the natural objective of the EU itself.

My own interest lies in the second pillar, "creating effective cyber deterrence." The key word is "deterrence." This term gained wide usage during the Cold War era, and its precise meaning varies with the many methods one might adopt to "deter." I will not go into the history of deterrence, as that would lead us astray from the purpose of this book. Glancing over the new strategy, one notes that key methods of deterrence include: identifying bad actors and strengthening law enforcement, political response, deterrence through defense capability of member nations, and the like. The nuances indicate a changed approach to deterrence—an emerging intent to discourage attackers with economic or political targets through a resolve for mutual cooperation.

The third pillar, strengthening international cooperation, advocates the use of international laws such as the UN Charter to govern cyberspace, and promotes partnership on both a bilateral and multilateral basis. It distinctively promotes collaboration with NATO.

Turning our attention to Asia, cybersecurity policies vary with the level of economic development of individual countries. Both Singapore and Australia (with a $50,000+ per capita GDP), which have similar political systems and policymaking structures as Western nations, have national cybersecurity strategies. Singapore, for example, unified its governmental cybersecurity agencies in 2015 into the Cyber Security Agency of Singapore (CSA) overseen by the Prime Minister's office. The nation's cybersecurity strategy focuses on four key areas: building a resilient

infrastructure, creating a safe cyberspace, developing a dynamic cyber ecosystem, and strengthening international partnerships. The strategy distinctively positions economic digitization as indispensable to Singapore's economic growth and underscores a cybersecure business environment as prerequisite to that growth. The cybersecurity industry itself is recognized as a growth industry, and its active efforts toward development and creation of an industrial environment designed to invite growth merit special mention.

On the other hand, in nations such as Malaysia, Thailand, Indonesia, the Philippines, and Vietnam, governmental policies revolved around defending the governments themselves. Efforts extended to creating systems for defense as well as to workforce development. Now, however, attention is gradually shifting from defending government systems to creating policies to defend their critical infrastructure. Many of the businesses supporting this critical infrastructure are state-run companies, and state-led efforts continue to be a feature of ASEAN.

The Japanese government is proactively cooperating in the protection of critical infrastructure for ASEAN nations, including the implementation of approaches introduced in Chapter 4—the key to success lies in building relationships of trust and relationships of trust are built over a shared beer. This cooperation includes hosting a workshop on critical infrastructures in the ten ASEAN nations in addition to an annual gathering of ASEAN leaders, not to mention joint work on forming guidelines for protecting critical infrastructure. In December 2017, ASEAN and Japan agreed to establish an ASEAN workforce development center in Thailand, with Japan lending its support. Of course, as an entity within the Southeast Asian community, ASEAN is not focusing solely on Japan for collaboration, but is creating opportunities to discuss cooperation with South Korea and China, and is learning from successful American and European precedent policies.

This book cannot delineate Russian and Chinese cybersecurity policies, but we can note that in defending policies safeguarding state control, the two nations cite improved security as the reason for restricting Internet usage, monitoring information channels, and the like. It is fair to say that these are far-reaching Internet policies rather than cybersecurity strategies.

This chapter has thus far outlined my understanding of cybersecurity policy in several nations, summarized by the following three points:

Point #1: The nations of the world have disparate cybersecurity policies. Some,

such as G7 and G20 countries/regions and the UN, for example, increasingly discuss cybersecurity issues on a multilateral basis, whereas others progressively engage on a bilateral basis, but cooperation is just now evolving.

Point #2: Countries pursuing economic development while championing so-called liberalism, have especially conditioned their digitized economy-based economic growth on cybersecurity. Those countries therefore share the ideology that private companies should drive cybersecurity.

Point #3: Initiatives involving private enterprise increasingly emphasize cooperation with the police, the military, and, above all, other nations. If you consider this together with Point #2, you see the huge significance for business. While businesses are independent entities dealing with cybersecurity, they are increasingly involved with law enforcement, the military, and—unavoidably at times—perhaps law enforcement and the military abroad. The exact implication is not very transparent, but it does seem clear that we must keep our eye on international developments and prepare ourselves accordingly.

From the next section forward, we will look at how individual companies can prepare to deal with cybersecurity amidst this complex backdrop, referencing several examples.

3. Global governance

Global cybersecurity policies are still in their infancy. Countries will evolve and change, and cooperation among them will undoubtedly take time. Companies developing business in multiple countries must therefore comply with differing laws in each country for the time being. The same may be said even of Japanese companies focusing only on domestic business; they will naturally be influenced by overseas policies as supply chains spread globally and business partners are overseas.

In other words, in-house cybersecurity governance of all companies must incorporate a global viewpoint. The first step is crafting a cybersecurity policy embracing a global perspective. A good example is the information security policy published by Toyota Motors which specifies that Toyota and its consolidated subsidiaries will systematically and continuously administer information security initiatives. The basic approach calls for (1) cooperation in the five areas of compliance, (2) maintenance of a stable business infrastructure, (3) provision of safe products and services, (4) contributions toward establishing a safe cyberspace, and (5) information security management. The policy's two characteristics are the fact

that it embraces a global approach (including its consolidated subsidiaries) and the inclusion of a maintained stable business infrastructure, provision of safe products and services, and establishment of a safe cyberspace in addition to the basics of compliance and information security management.

A corporation clarifying its universal philosophy as its shared policy must nevertheless establish rules (with a team to implement them) ensuring conformity to the laws of various countries and regions as it executes the plan. Businesses with overseas bases must consider appointing a CISO for global oversight, a CISO in each country or region, and one in each subsidiary, or some combination of the above. A Security 50 participant commented that "one size fits all" does not apply when it comes to the CISO format; each company must find what works best for it. Practicality suggests that each company determines CISO needs based on its global management system and human resources. Moreover, CISOs in each country/region and those assigned to individual subsidiaries may not directly report to the "global CISO," but more likely to their national/regional or subsidiary branch manager. The latter arrangement likely streamlines business operations. However, the individual CISOs participate in committee meetings sponsored by the global CISO, offering them a setting in which they can cooperate and collaborate in organizational management.

Establishment of such global governance allows corporations to abide by restrictions and demands varying by country and/or region. One example is response to the GDPR (General Data Protection Regulation) commencing in Europe in May 2018. The GDPR, as explained earlier, governs personal data management and export of that data to third nations and fines companies up to 4% of total global sales if they do not comply. As the GDPR itself has a global reach, the Regulation forces companies doing business within the EU to prove global conformance, which requires governance with a global scope.

Another example involves the CFIUS (Committee on Foreign Investments in the United States), a federal entity examining the impact of foreign investment in corporate America on US national security. If this interagency committee uncovers security concerns, it recommends that the President deny the foreign entity permission to invest. The CFIUS inspection elevates the importance of the investor's cybersecurity ability. Should a company with modest cybersecurity buy, or form a joint venture with, an American entity, the American side would theoretically fret about its information being leaked to a third nation. Just as the GDPR requires global preparedness of companies doing business within the EU, so is the CFIUS

showing increasing interest in whether entities investing in American companies have global cybersecurity readiness.

4. Supply chain cybersecurity readiness

Supply chain cybersecurity is a major issue. And supply chain readiness is a priority issue, reflected by the Japanese Ministry of Economy, Trade, and Industry's announced revision of its Cybersecurity Management Guidelines (Version 2) in November 2017, and the pending update of the US National Institute of Standards and Technology (NIST) cybersecurity framework scheduled for early 2018. Whether a supply chain transcends national borders has no fundamentally bearing on managing corporate impact from the cybersecurity level covering procured components and suppliers. However, as many supply chains do transcend national borders now, most companies debate bringing supply chain readiness under the global management umbrella. The NIST cybersecurity framework update shows awareness that businesses depend on a global supply chain and third-party provision of products and services, and that consequently, corporate risk assessment must consider risk generated by those third parties.

As consideration of supply chain cybersecurity readiness is in its global infancy, a formularized approach is yet to come. At present, companies are sharing their individual initiatives as they search for an ideal approach.

For example, the May 2017 suburban Washington, DC workshop supporting preparation of the NIST cybersecurity framework update, and the public comments preceding it dealt with supply chain initiatives for industries. One workshop panelist, a security officer from Royal Dutch Shell USA, commented that one index the company uses in considering a given supplier is whether the supplier's security risk has been assessed using the NIST framework. Her comment indicated that the security of supplier products is not considered item by item, but rather that the overall security of the supplier is evaluated. Also, written public comments such as the following received from specific companies seemed to indicate actual issues which they experienced:

- The supply chain issue is included the question, "What should our company be protecting?" (Note: This applies to Imperative Action #1 in Chapter 3)
- In terms of supply chain, we consider interdependence with other companies regardless of whether we have a contract with them.
- Sharing common terminology among companies within the supply chain is important.

It is becoming increasingly important for Japanese companies to have the opportunity to participate in global events to discuss supply chain readiness with overseas companies.

For major companies, small-to-medium-sized companies generally shoulder the supply chain, be it upstream or downstream. The prevailing opinion is that globally, these smaller companies have few human or financial resources to dedicate to cybersecurity, and lack technical know-how. Some Western companies are now starting to take this issue on collaboratively.

Specifically, the Cyber Readiness Institute (CRI), an NPO, was founded in the US in August 2017, spearheaded by former IBM CEO Samuel Palmisano, MasterCard CEO Ajay Banga, and former US Secretary of Commerce Penny Pritzker. The announcement indicated that the major companies joining the Institute were pooling their know-how and human resources to create study programs for the smaller supply chain companies as workforce development and training. As the Institute is new, a close watch is needed to see how it develops. Given the CRI's background and purpose, it is clearly not a commercial endeavor, but rather one seeking ambitious solutions to the far-reaching issue of cybersecurity enhancement for the supply chain and small-to-medium-sized firms. The fact that current and former corporate leaders, and a former US departmental secretary, are the standard-bearers proves that this is an important project which bears watching.

5. Public advocacy

Cybersecurity initiatives should be undertaken independently by companies, but they are also greatly influenced by governmental policy and regulations. As we saw in Section 2 of this chapter (Trends in overseas governments), cybersecurity policymaking by most global governments is still maturing. Multilateral and bilateral cooperation and collaboration is just now getting underway. Moreover, unknown geopolitical influences will likely also impact the situation.

We saw that US companies involved in public-private sector cooperation do not passively await governmental policy; rather, they proactively state their opinion and press for its realization. Industries' opinions and activities are not limited to one nation; they transcend borders. This is particularly true of multinational corporations which have expanded into many countries. At times, the actor is an individual corporation; at times it is an industry group, and on occasion, it is a corporate group spanning multiple industries which actively presses another government to heed its opinion.

In December 2015, for example, the EC asked for public opinion on public-private sector cooperation in a unified digital market, including the issue of strengthening cybersecurity. Since the public-private sector cooperation had somewhat favored European businesses, the EC request yielded an American Chamber of Commerce response signed by American trade associations from 13 industries, including automobiles, banking, chemicals, gas, hotels, petroleum, and electrical power.

In this example, American companies petitioned the EC, but there have also been reverse cases of European companies petitioning the US government. When NIST asked for public input as it updated its cybersecurity framework, European companies such as Germany's Siemens and the British Standards Institute responded. The NIST framework does not purport to serve only American interests, but rather to gain favor worldwide.

Western companies' motivation to participate in self-expression and promotion, hoping for favorable policies, may resemble so-called "lobbying." However, it exceeds that in my opinion. Convenience for one enterprise aside, industry's interest in finding policies to enhance cybersecurity—the advocacy viewpoint—is the dominant meaning.

Global companies must deal with each country's policies and rules, and costs run high. Moreover, differing policies in each country weakens security, delivering a negative outcome. Companies now seem interested in avoiding obligatory responses to prescribed rules, preferring dynamic incorporation of proven substantial and useful cybersecurity policies. Advanced Western companies use this universal principle and philosophy as the basis for public advocacy initiatives. (Figure 5-1)

Figure 5-1:
G7 ICT and Industry Ministerial Multi-stakeholder Conference (September 25, 2017)

Sandwiching the Atlantic Ocean as their respective governments craft cybersecurity policies, industries of the US and Europe transcend their borders to participate in the cybersecurity policymaking of other nations, engaging in mutual pressure. Few Japanese companies participate in public advocacy in international cybersecurity. However, the creation of international rules for cybersecurity is a sphere which will develop. Such rules are international public goods, and Japanese corporate participation in the process is awaited. Japanese companies should not approach the process as a profit/loss business expansion negotiation, but rather as an opportunity to create a foundation for the healthy development of the digital economy along with global peers.

When participating in creation of international rules, Japan is likely to formulate Japanese standards to share with the international community. However, this two-step approach lags behind international trends. Rather than create Japanese standards, Japan should join the international force creating global rules together.

6. The implication for Japanese companies

This chapter summarized Western multinational corporate security officers' issue awareness against the backdrop of overseas governments' cybersecurity policies, underscoring global governance, supply chain readiness, and public

advocacy as requisite corporate initiatives. These activities are part of global business management and factor into cybersecurity as a business issue.

Japanese companies generally trail their Western counterparts in cybersecurity initiatives. Most Japanese companies prioritize enhancing their domestic cybersecurity through independent efforts, and then through mutual support such as ISACs serving individual industries.

However, as cybersecurity transcends national boundaries, all companies must assume a global perspective when dealing with it. Businesses expanding globally must take the content of this chapter urgently to heart. One would like to think that advanced corporations will begin advancing global governance, supply chain response, pressure on overseas governments, and more. If ISAC and other domestic activity matures in each industry as leading companies advance global initiatives, international cooperation will grow beyond leading companies to become an effort by the entire business community before long.

Chapter 6: Collaboration with Government

Industry should not passively await government policy; rather, it must engage in proactive outreach and advocacy to ensure that its needs are met by government. Action is beginning in the capacity building sphere and should be augmented by information sharing and other means. Cybersecurity is a public good, and it is essential that industry plays a proactive role in its establishment and maintenance.

1. The respective roles of industry and government

Public-private partnerships (PPPs), as the phrase suggests, refer to a collaborative arrangement between the public and private sectors. In Western countries, one often hears that PPPs are essential to securing cybersecurity for society as a whole. However, overseas (particularly American) reference to "PPPs" and Japanese usage of "public-private cooperation/collaboration" feel substantially different.

To wit, as the motif of NCI meetings illustrated in Chapter 4, Section 2 ("ISAC initiatives in the US"), the US has many forums in which industry can actively and openly share its opinions with the government. Section 2 also noted the comments of a Department of Homeland Security official, in which he explains that it is "the private sector (industry) which safeguards and manages the telecommunications infrastructure. The government has no choice but to trust the word of the industry." This comment symbolizes the strong tendency for government to respect industry and incorporate its viewpoint. One senses that PPPs are spearheaded by US industry.

On the other hand, Japanese industry tends to be passive in interaction with the government. In Japan, the public-private relationship seems characterized by governmental dominance, with the government initiating a plan which industry accepts. The feeling is that industry expects government to assume the reins of leadership. Of course, all parties have input on policy and its formation process, and industry representatives participate in deliberations with expert opinions, so you could say that industry exerts both substantive and formal influence. However, in terms of overall dynamism, Japanese governmental leadership dominates in public-private endeavors.

As role-sharing depends on factors such as political climate, culture, and history, it is impossible to determine whether industry or government leadership is

preferable. With cybersecurity, however, it is appropriate for industry to take the initiative, as we concluded in Chapter 2 ("Why Cybersecurity is a Business Management Issue"). Attack targets and owners/managers of digital assets (targets for protection) are the best informed on new attack methods and patterns, deeply understand relevant concerns and issues, and are the most experienced in countermeasures. Managers overseeing daily security at operational sites possess the most up-to-date expertise on attack protection, detection, and response, and are most keenly afflicted by attacks. Industry must proactively communicate its needs, based on this on-site concern, expertise, and experience, requesting practical political support from the government. The key is to put government to work.

2. Public-private sector collaboration in capacity building

Capacity building is one area in which industry is speaking up and the government is beginning to respond. In Chapter 4, Section 8 ("Cross-Sectoral Committee for Cybersecurity Human Resources Development"), I explained how the Committee clarified required personnel profiles by establishing the Cross-Sectoral Definition and Reference of Cybersecurity Professionals Based on Functions and Missions. Member businesses are now incorporating those results into collaborative workforce development, but the data should also serve long-term unified industry-academia-government capacity building efforts.

In March 2017, the Cabinet Secretariat's National Center of Incident Readiness and Strategy for Cybersecurity (NISC) established the Cybersecurity Capacity Building Policy Collaborative Working Group in Japan. The Cross-Sectoral Committee secretariat participates in this working group, along with entities such as the National Institute of Information and Communications Technology (NICT), which is overseen by the Ministry of Internal Affairs and Communications, the Information-technology Promotion Agency (IPA) overseen by the Ministry of Economy, Trade, and Industry (METI), and technical colleges established by the Ministry of Education, Culture, Sports, Science, and Technology (MEXT), representing a true embodiment of an industry-academic-government organization. In its inaugural meeting in June 2017, the first working group sought shared basic awareness of nature and scope of personnel profiles before addressing its goal of establishing curricula for workforce development. The workshop will undoubtedly make good use of the Cross-Sectoral Committee's "Definition and Reference of Cybersecurity Professionals."

Workforce development policies are created by each governmental ministry,

including the Ministry of Education, Culture, Sports, Science, and Technology (MEXT), the Ministry of Internal Affairs and Communications, and the Financial Services Agency. In cybersecurity training, for example, the NICT sponsors CYDER (Cyber Defense Exercise with Recurrence) and Cyber Colosseo (aimed at 2020 Olympic readiness), the IPA runs a program for CISOs at its Industrial Cybersecurity Center of Excellence, the Financial Services Agency sponsors Delta Wall, the National Police Agency hosts joint countermeasure training for essential infrastructure companies, and NISC oversees its essential infrastructure sector-wide training.

Each initiative aims to train its own human resources which differ according to factors such as level and industry affiliation. However, it seems that an overarching, unified educational policy portfolio and organization is missing; we do not know how, or to what degree, Japan plans to train its security workforce. The NISC's Cybersecurity Capacity Building Policy Collaborative Working Group not only has a fundamentally shared personnel profile as its starting point, it also intends to coordinate the policies of the various government ministries. There are also plans for shared training exercises incorporating shared scenarios, as well as shared materials for educational programs, all based on industry needs.

Each ministry has its own workforce training programs promoting its own policies, and often asks industry to send lecturers to support these programs. Industry has limited development staff available for training and sparing them for dispatch to various ministries is inefficient. There is a strong sense—from that viewpoint—that the ministries should have a one-package policy as one government.

3. Public-private collaboration in information sharing

Capacity building is a field in which industry has communicated its needs, government has listened, and the ministries have coordinated and taken the first initiative. In Chapter 4 ("Collaboration with Other Companies"), we saw that intercorporate information sharing could be effective and noted the need for ISACs to be established in each industry. What sort of needs should businesses and operational sites proclaim to realize policy that supports and accelerates information sharing?

First, I suggest establishment of a set of rules for information sharing that are applicable internationally. They could include, for example, terminology and guidelines to apply when sharing and using information. Information sharing among Japanese companies is important, but in today's world of cyberattack threats

transcending national borders, utilizing information generated overseas is inevitable. The Japanese government should confer with other governments and settle on international "rules" enabling Japanese companies rapid acquisition and exploitation of threat warnings, solutions, and other information from overseas.

As it stands, there is vague common terminology at best within Japan, and less within individual industries, with little mutual understanding of what sort of "information sharing" is needed; in short, nobody seems to be on the same page. At the very least, sufficient common terminology is needed to discuss "shared information." Receipt and dispatch of shared information between Japan and overseas requires shared terminology used worldwide. One option is to adopt definitions proposed by ISAO-SO which we mentioned in "Types of shared information," the Special Focus article in Chapter 4, Section 4.

Guidelines governing information exchange and usage is a wide-ranging topic. For the recipient company, it involves rules overseeing re-disclosure to third parties, whereas for individuals and companies sharing information, it covers protection mechanisms against lawsuits, and issues such as measures protecting personal information. Creation of guidelines for domestic use and efforts to integrate them with international ones must progress in a parallel fashion.

My second suggestion is for speedy governmental intelligence on material and significant threats and courtesy delivery to industries. Following the December 2015 cyberattack on a power company causing a blackout in the Ukraine, the US Department of Homeland Security and the FBI co-sponsored a webinar offering industry information including the blackout chronology, the presumed cyberattack method, and recommendations for containing damage in the event of a similar cyberattack. Targets are not limited to power companies, but embrace other entities supporting critical infrastructure. After the May 2017 WannaCry incident which caused worldwide damage, the Department of Homeland Security streamed information during the weekend on the Homeland Security Information Network (HSIN), its portal site for essential infrastructure companies. Information procurement/sharing is primarily the business of companies themselves, but when unusually strong threats emerge, the government should amass information from foreign governments and elsewhere, and provide it to industry without delay.

A third suggestion is to develop and provide software and information systems that automate and accelerate information sharing from a global perspective. When we discussed activities of industry-specific ISACs in Chapter 4, Section 3 ("ISACs and related organizations in Japan"), we mentioned that Financials ISAC Japan

uses an information-sharing portal known as “Signal,” and that J-Auto-ISAC uses e-mail for information sharing. At present, methods and tools vary among ISACs in Japan. The key is information rather than tools, but the more information that is shared, the more laborious the methods and uses become. Development of an automated, labor-saving system for information sharing can eliminate that bottleneck from the outset. The Cyber-Security for Critical Infrastructure program (SIP-Cyber), under the umbrella of the Cross-ministerial Strategic Innovation Promotion Program (SIP) supported by the Cabinet Office, is now creating a foundation for information sharing on cyber threats. Japan must ensure interoperability of such information exchange programs with international sources.

Despite emphasis on how important awareness of information sharing is, companies seem reluctant to release information. Some argue that laws enforcing information sharing should be created. I feel that this argument mixes two approaches: reporting the cause, response, and future policies to a regulatory agency when incidents occur, and a broader sharing of threat warnings, possible countermeasures, and their efficacy. The former represents mandatory reporting to ensure stable business operations and services based on business laws and regulations according to industry, or business type. The latter is reciprocal corporate sharing of valuable information gained through hard work or purchase, and carefully developed countermeasures, with trusted business partners. We should keep in mind that the two abovementioned approaches have different intents.

It might be possible to introduce regulatory obligation to the latter. However, from the standpoint of those in the field, legally mandating information exchange with external sources seems fraught with problems. For example, when warnings are received voluntarily, they may include a given amount of uncertain information. For example, if it was mandated that known warnings must be reported to the government, who would verify the authenticity of those warnings? Furthermore, if information sharing were to be made compulsory, a precise definition of what constitutes information to be shared would become necessary. Information on cybersecurity is diversely spread and changes with rapid advancements. Defining the scope of mandatory shared information would be exceedingly difficult. It would also require compliance checks to confirm that companies were sharing information as mandated, an even harder task. If you consider actual activities on the ground, you can see that voluntary information sharing between companies would be preferable. What we need is an environment in which companies are incentivized to share information with each other.

4. The cyber environment: a public good

The research group headed by Katsunari Yoshioka, Associate Professor at the Yokohama National University Graduate School, examined the current Internet "pollution level" and published their findings in the summer of 2017. They selected seven clearly unsafe IoT devices such as security cameras and wireless routers, connecting them to the Internet, and measuring elapsed time until they became infected with malware. Repeated experimentation produced an average time to infection of an hour or less for six of the seven devices. The shortest time noted by Yoshioka's group was a mere 38 seconds.

The experimental results demonstrated that today, unprotected Internet connection results in infection in the twinkling of an eye due to the highly-polluted environment. Imagine walking defenseless into a crowd of people infested with a highly contagious influenza virus. Your likelihood of being infected would be quite high. You would be sure to protect yourself by putting on a surgical mask before going out (a common practice throughout Japan), and would wash your hands and gargle after coming home. Even so, that would not yield 100% protection; some individuals would get the flu regardless. If a fever or other flu symptoms appeared, you would quickly see a doctor and would receive treatment if necessary. You will see that the "Imperative Actions for Business Executives" described in Chapter 3, such as executing "prioritized layered defense " and "quick detection, response, and recovery," perfectly harmonize with commonly-accepted beliefs surrounding influenza infection.

Neither individuals nor lone companies can protect safe and secure usage of the cyber environment—the Internet and the "complex commingling of networked people and machines"—against the threat of new forms of malware; it requires countermeasures by society, supported by us all. This viewpoint highlights the many similarities between the fields of cybersecurity and medical/health care. For instance, when a new type of infectious virus emerges, the World Health Organization (WHO) depends on international cooperation to help treat the infected individuals, engage in widespread preventive measures in the endangered region, disseminate information on preventive measures, and develop and provide medications and vaccinations.

Unfortunately, the field of cybersecurity still lacks the mechanisms which are in place for medical care. A similar structure needs to be established, not only targeting the Internet, but also cyberspace itself, where life-forms and machines are

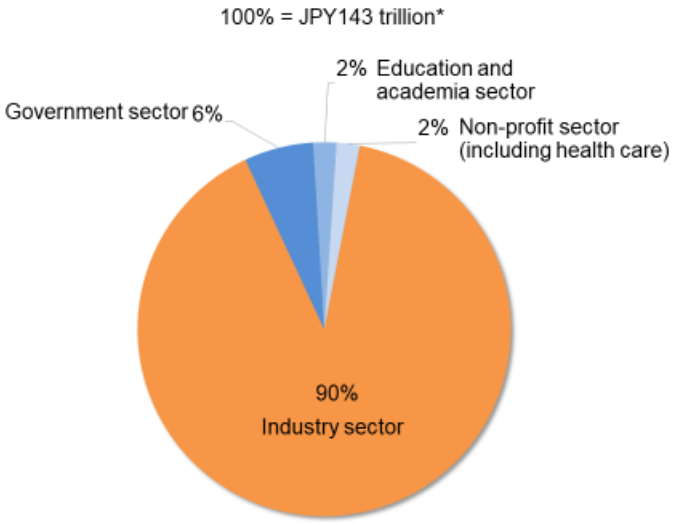
commingled in a networked condition. Safe and secure cyberspace usage is not for one individual, company, or even group; rather, it is for everyone. Cybersecurity has the pronounced characteristic of being a public good.

5. The need for a market mechanism

Let us examine the mechanism for establishing and protecting cyberspace as a secure public good. Normally, countless people benefit from public goods such as roads and parks, airports, and harbors, meaning that their so-called externalities are high. For that reason, there is little incentive for individual economic entities such as people or companies to invest or put effort into their establishment or maintenance. Thus, it is often left to local and national governments to invest in the establishment and maintenance of public goods as a community service.

It is therefore natural to expect that governments will assume a role with cybersecurity as it does with other public goods, becoming actively involved and investing to create and maintain a safe and secure environment. Unfortunately, however, I fear the governmental approach may not go well because maintaining cybersecurity will involve protection of things—ICT devices, for example—which are largely owned by private companies and households. An input-output table shows us that 90% of Japan's ICT assets (excluding household economies) are owned by industry. Educational and research institutions have 2%, government has 6%, and NPOs own 2% (Figure 6-1). As this book repeatedly stresses that industry should take the lead, the latter's ownership of most ICT assets is a prime reason why industry should independently lead its own initiatives.

Figure 6-1:
IT capital stock in Japan



** Price in 2000
Source: Input-output table

The distinctive characteristic—and challenging reality—of cybersecurity, then, is that although it is a public good, it must be the private sector which creates and sustains it. As we enter the IoT age, that which needs to be protected will expand beyond conventional ICT assets. The growing tendency is for the private sector to oversee creation of the public good of "cyber protection."

I believe that environmental improvements can offer a hint on how to proceed. Discrete companies, households, or individuals independently determine their activities, and as a result, we have created a social mechanism to preserve our surroundings with clean air and water and a safe natural environment. Though we may simply say "social mechanism," it goes without saying that the actual content and structure are extremely complex. There are regulations, machinery and equipment for implementation, underlying technology, capacity building/workforce development, awareness programs, international cooperation, and myriad other components which merge in a complex conversion of functions. We have spent 50 to 100 years of repeated trial and error to reach our current social mechanism for environmental protection, which is continuously being reconsidered. The important thing to remember is that if each economic entity behaves based on a rational assessment, a market mechanism of sorts is realized that generates and sustains the public good of clean air and water.

In Chapter 4, Section 1 ("The importance of information sharing"), we indicated

that the black market where attackers buy and sell information and attack tools consists of attackers (nation states, political offenders, etc. excepted) who behave based on economic rationality, representing a functioning market mechanism. Perhaps we can expect government to counter this black market by producing a larger market mechanism in which each entity acts following rational assessment, and as a result, produces a public good: a cybersecure environment.

We used the term “market,” when we really mean “market principle” here, and not the “market” where companies sell security as a business. The security business market is also one component of the market principle, but in this section, we are dealing with the broader issue of market principle.

The safe cyberspace with inherent high externality will be produced based on market principle. That social mechanism will not be created overnight. It will require a wide range of policies. Moreover, just as consumers choose eco-friendly products despite their higher cost, users will need to rethink their priorities to emphasize safety and security. We will also need technological development to reach that point. Moreover, cyberspace has no national boundaries. The nations of the world need to pitch in and participate in the creation of the new mechanism, but when we consider competing interests, we will surely be in it for the long haul.

The important thing for industry is to participate as a principal player. We usually equate the public domain with government, and the private domain with industry. If we categorize cybersecurity according to its beneficiaries, it belongs in the public domain, not in the private domain. Despite this logical classification, industry must act on its own initiative. As we have mentioned, government of course has an important role as well — to create what we can call the public domain through cooperation with industry.

Closing

Although the perception of cybersecurity as a management task is gradually expanding, it is still firmly perceived as a necessary cost. As being cyber-secure becomes the fountainhead of competitiveness amidst soaring business digitization, I suggest repositioning cybersecurity as a competitive edge linked to value creation instead of viewing it as a necessary cost.

The essence of cybersecurity

In the Introduction, we stated that cybersecurity is multifaceted, and that this book would provide a thorough examination of this multifaceted cybersecurity from a business executive's viewpoint. I will leave it to readers to determine the success of that elucidation; meanwhile, let us synthesize the chapters by revisiting my assessment of the essence of cybersecurity in business, comparing it to conventional views.

First, we saw that cybersecurity is not an issue which accompanies Internet usage, but rather one accompanying business digitization.

A new era is coming when our lifestyle and socio-economic activity will face multiple risks unrelated to the Internet, such as the challenges shadowing autonomous driving and the medical threat to insulin pump hacking. Devices and systems not normally connected to the Internet are already vulnerable to cybersecurity risks. The backdrop to all of this is the gradual permeation of digitization into our socio-economic activity—a trend which is irreversible.

Second, we emphasized that business continuity, more than data breaches, deserves our full attention in terms of preparedness and countermeasures.

When data breaches occur in Japan, there is a strong tendency for the public to censure companies and question management responsibility, especially when personal information is leaked. Of course, data breaches should be avoided to the best of our ability, but from a business management standpoint, the weightier task is avoiding threats to business continuity. We also discussed a new development: a recent upswing in cyberattacks using ransomware to take business continuity "hostage." This trend should spur senior management to prioritize dealing with business continuity.

Third, we pointed out that the private sector—in other words, companies, households, and individuals—must shoulder a primary role in dealing with this

issue, even though it also encompasses national security.

Discounting the household sector, industry owns some 90% of ICT assets in Japan. From a national security standpoint, Japan's cybersecurity cannot be improved without the proactive involvement of the companies, households, and individuals representing ICT asset ownership and usage. The private sector must act independently to help achieve the safety and security of cyberspace, strongly identified as a public good. What is needed, then, is for business executives to prioritize self-help measures (Chapter 3: "Imperative Actions for Business Executives"), followed by cooperative initiatives (Chapter 4: "Collaboration with Other Companies") and the expectation of public assistance (Chapter 6: "Collaboration with Government"), with companies addressing government on equal footing.

Lastly, we concluded with the point that managers should not seek perfection in cybersecurity, but should approach it with risk-based initiatives.

At present, cyberspace is a highly-polluted environment in which vulnerable and unprotected devices may become infected with malware in less than a minute. We are beset by the threat of targeted attacks, with attackers relentlessly and incessantly testing a variety of means to slip through safeguards. To that, we add the successive scattering of malware—especially, ransomware—which targets an unspecified victim. In such a climate, it is unrealistic to expect 100% protection. The importance of seeking safeguards goes without saying; meanwhile, the reality of protections being ripped away should be considered as tantamount to encountering a natural disaster. Organized measures for early detection and early response are needed to minimize damage, along with drills and training for readiness at the critical moment. Risk-based management is what underlies such an approach. Not only is it impractical to assume 100% risk avoidance, doing so excessively pressures the organization and worksites, conversely creating a great disadvantage for management. Part of management's responsibility is judging which risks should be minimized, which avoided, which transferred, and which accepted.

Cybersecurity ensures competitiveness

With the shift from tangible to intangible value-added assets, and their increasing digitization, the digitization of corporate value creation activities has become irreversible. This progressive reality has been a constant drumbeat throughout this book, as it has led every nook and cranny of businesses to become a

complex commingling of individuals and machines in a networked cyber-state. That cyber-state is spreading through interaction with business partners, thoroughly permeating the supply chain. Goods and services are marketed, purchased and used on a cyber-state platform. Questions are being posed regarding what responsibility companies bear for usage of these goods and services which they are producing and selling.

Business management equals risk management. It thus follows that digitization of risk management is now irreversible. As digitized risk is dynamic, it requires continuous management; as it has connectivity, it requires collaboration with outside entities; and as its speed of diffusion is high, rapid response is required. The issue cybersecurity poses for business management is how to advance management of this idiosyncratic new digital risk.

Digital risk management has just started to take root in business, and it appears that a standardized approach has yet to take shape. The conventional risk management methods of compliance checks and audits will probably not do the trick. A better way would be for each company to reconsider its business characteristics, create a fitting approach, and test it through trial and error.

If companies fail to manage digitized risk, their business planning and execution may be hindered. They may also encounter unexpected damage as a result. On the other hand, executing matured digitized risk management and appropriate cybersecurity measures ahead of other businesses positions a company to advance quickly with business planning and implementation. This will give the company an advantage when it comes to being selected by customers, clients, and business partners.

Even if executives are aware of cybersecurity as a business issue, the majority regard it as nothing more than a necessary cost. However, the vast potential for added-value creation introduced by a progressively digitized economy suggests that ensuring cybersecurity can be equated to the development of “value creation competitiveness” that generates and acquires added corporate value. Thus, I propose a paradigm shift from “necessary cost” to “value creation competitiveness.”

Imploring those involved in management

These days, I am often asked to address non-executive corporate directors who are interested in learning more about cybersecurity. After speaking, I sometimes enjoy the opportunity to hear what the participants expect of senior executives. I would like to share a few of those comments as we bring this book to a close. I

believe these are just a few of the expectations held of business executives everywhere.

- For business growth, executives cannot avoid including ICT in business initiatives. Moreover, we must learn to separate what we can protect from what we cannot, or we will be unable to proceed. This reality is not, however, limited to cybersecurity.
- Management must discuss the relative priority of its various crown jewels (protected assets), and not only from a cybersecurity standpoint.
- The all-encompassing view that "all cyber-damage must be eradicated" is nonsense. Each company needs to devise its cybersecurity based on its business and corporate characteristics.
- The Board of Directors should be debating in advance what to protect, and should not be debating what measures to take after an incident occurs. In addition, such discussions should be held regularly, reflecting the corporate mission.
- The most important factor is the consciousness of corporate officials. This is especially true in the new IoT era.
- A sense of balance is important. Business executives' antennae should remain alert to cyber-episodes even as they keep cybersecurity on the front burner.

The opinions in this book are solely those of the author, as is the responsibility for the content herein. Meanwhile, nothing would bring me more joy than for this book to be useful to business executives grappling with cybersecurity.

Acknowledgments

While writing this book, I received valuable advice from numerous individuals, including Masato Kimura, Hiroo Suzuki, and my innumerable other colleagues at NTT, as well as all those with whom I shared friendship at the Japan Business Federation and other forums outside my corporate sphere. Hideaki Inoue from Nikkei Business Publications, Inc. was greatly helpful in the editing of this effort, while my secretary, Chieko Tokano, kept me on schedule during the writing process. May I take this opportunity to thank all of you for your support. Finally, I would like to thank my wife, Nozomi Yokohama, for her tireless support in the face of my (nearly) monthly trips overseas.

English translation by MDK Translation Inc.