Cybersecurity for Business Executives

An NTT publication for top management

In October 2015, we published the Japanese edition of *Cybersecurity for Business Executives*. This booklet is a preliminary version of a simplified English translation.

Target readers of the book are C-suite business leaders who are not familiar with technology. The key message is that we should reposition cybersecurity from an IT challenge to a business challenge. The book also argues that the cybersecurity workforce has a diversified profile and that companies need to define their required employee profiles based on their specific business needs. In addressing these messages, we introduce 14 NTT employees who work on cybersecurity in 10 subject areas. (In the English version, NTT employee profiles are introduced in one to two pages per subject area in Chapter 2). Learnings from NTT's experience in the US and the international public policy space are also shared to argue for the importance of a multi-stakeholders approach.

We developed this English translated version for readers in both the public and private sectors. We would like to share our thoughts on cybersecurity challenges from a business management point of view. We also want to share information about our public advocacy activities so that we can discuss collaborative public advocacy that aligns with international norms and practices.

We are happy to receive any feedback and comments on this preliminary version so that we can further improve it.

March 2016

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

Table of Contents

Introduction

Hiromichi Shinohara, Senior Executive Vice President, NTT Corporation

NTT has been named the gold partner in telecommunication services for the Tokyo 2020 Olympic and Paralympic Games. We at NTT will contribute fully to the successful operation of each competition at these games.

Unfortunately, attempted cyber attacks are virtually inevitable at such a large world-scale event. For example, the 2012 London experienced online frauds in accommodations and tickets to the games, and denial of service (DOS) attacks took place at the websites for these games.

Looking ahead to the Tokyo games, we see that information and communication technology (ICT) will clearly play a more vital role in operational infrastructure than at the London or Rio de Janeiro games; therefore, ensuring cybersecurity is a critical task. As a gold partner, NTT will do its best, but ensuring cybersecurity by efforts from telecommunication carriers alone could be difficult in today's world in which "everything is connected to everything else." It is therefore indispensable to have the efforts and cooperation of everyone engaged in the operations of the Olympic games.

This example pertains to the Tokyo Olympic and Paralympic games, but it is becoming a broader social requirement that cybersecurity requires every player's cooperation in this fully connected era. This is our motivation for publishing a book that appeals broadly to society.

Business people outside of ICT can find it difficult to understand well the topic of cybersecurity due to its highly technical nature. Most books that are available target the staff of the information system division or information and communication engineers. To challenge this situation, this book is directed at people with business management responsibilities or business executives outside of ICT. We hope to provide provocative ideas that will lead readers to think about answers, if not the exact answers themselves, to simple questions such as, "what is cybersecurity?," "how can we position it?" or "in what way and how far should we initiate cybersecurity?" In this book, we would like to convey three key messages.

Message 1: "Cybersecurity is a business management issue"

Cybersecurity is considered to be difficult to understand because it is very technical. Indeed, technical progress in this area has advanced greatly, including rapid advances in attack techniques and protection technology. For this reason, people will often take the position that they have to leave the responsibility to an internal information system department or an external technology company. Even if they recognize current issues as a "clear and present danger," they do not understand well what they should do and how much they should do it. They feel as if any efforts would go nowhere even though they need to do something. The reality is that people find it difficult to discuss the issue directly. As a result, cybersecurity issues are tasked to specialized staff only, and it becomes difficult for the company to have open discussions and initiate solutions. We suspect many companies are in such a situation.

Today, essentially all information is digitalized. Cybersecurity is an activity to protect trust in the information that a company handles or distributes. We need to initiate cybersecurity across the company by positioning it as a central topic among top management issues. We should reposition cybersecurity from an IT issue to a business management issue. This is our first message.

Having responses taken only by designated experts means that the company is unable to take appropriate measures to meet its company-wide needs; neither an internal expert department such as an information department nor external professionals such as at a technology company can respond adequately. This is because cybersecurity covers the corporate activities where digital information exists and is utilized over the entire company. As a result, a company is inevitably required to prioritize its tasks because there are limits to the size of the budget and amount of staffing resources for cybersecurity. The company needs to adopt a viewpoint of company-wide optimization.

Moreover, because cybersecurity is a new issue, most companies do not have prior experience in deciding what and how much they should do, even if they want to take action by prioritizing tasks from a company-wide point of view. Judgment plays an important role because it is difficult for companies to derive an answer based upon past experience or experiment. Therefore, top management needs to be

proactively engaged.

Message 2: "A cybersecurity workforce is key, but a staff with a diversity of capabilities is required. The first step is to define the requirements at each company".

It is often said that the key to effective cybersecurity measures is the workforce and that we need to build capabilities In Japan, it is said that we have a shortage of around 240-thousand security engineers. But what kind of workforce are we talking about?

An academic field called "cybersecurity studies" does not exist. Cybersecurity relates to a large number of topics and fields such as communications or computers and expands other areas in the social and human sciences such as international law and privacy protection. Even we at NTT say that the required profile for a "cybersecurity workforce" will vary depending on what we expect to have for resources. A hacker with advanced and specialized technical expertise in computer science isn't the only profile for a member of the cybersecurity workforce.

For example, a company may not need staffing resources who are familiar with the latest cyberattack techniques or defense technologies used against them. Instead, it may be important to have staff who can identify "which assets and information need to be protected" in the first place in reasonable consideration of their business characteristics from a corporate planning or risk assessment perspective. Or companies may need engineers who can talk accurately with people from technology companies and decide upon appropriate cybersecurity products or services and who have ability to implement and operate these products and services within an information system department. Moreover, a company may also need a certain number of employees who can take responsibility to provide training to general staff at general workplaces such as a sales or accounting department or who can be responsible for incident management when an attack occurs.

We would like to show you the diversity of front-line operations and required skill sets among cybersecurity workers by introducing some of NTT's employees in Chapter 2. At the same time, we will show you that the personalities and thoughts among these workers are also diverse. We hope that this book will give readers a chance to start discussion on the type of cybersecurity workforce that is needed in

their own companies.

Message 3: "The work on cybersecurity must be done by the entire industry and not left to the government or technology companies."

News coverage of cyberattacks often focuses on attacks by a foreign government or state-supported group that could be engaging in espionage. It is difficult both technically and financially for an individual company to respond to these types of attacks, which require multinational legal action or efforts such as diplomacy. We therefore expect that government will play a vital role. We have no other choice but to pin our hopes on research and development by technology companies while new attack techniques are developed one after another. Thus, it is understandable that companies largely look towards efforts from governments or technology companies.

But these expectations for initiatives from the government or technology companies does not mean that a company does not have to do anything. Regardless of what type of cyberattack occurs or whether the attack comes from a foreign government or an international crime organization, the company and its information are attacked and it is the company's responsibility to minimize the damage. Companies cannot shun their cybersecurity responsibilities as they operate their businesses. This is true for every business operating entity, for example, in shops such as restaurant chains or retail stores, or in production sites at general manufacturers, and especially in critical infrastructure industries such as electric power companies or financial institutions.

We would like to give you an example case. Suppose that someone is invading a company's systems by using malware and causes a breach of internal information. What would a law enforcement team do if they rushed to the crime scene and the criminal was not there. What should be done is to stop the data leakage and minimize the damage. The only party that can do this is the company, the owner and operator of the information system and information that is about to be stolen.

Furthermore in this age in which "everything is connected to everything else," there is great merit not only in an individual company's effort but also in cooperation. There is some movement towards information-sharing among companies on such matters as what type of attacks they have experienced, but such cases are still exceptional at the moment. However, progress towards universal cooperation in

cybersecurity creates great synergy and returns to society on time scales such as 5 or 10 years. We hope the number of companies that agree to universal cooperation increases step by step even if it starts small.

This book consists of three chapters.

In Chapter 1, "Cybersecurity for business executives," we provide an overview of the change in the quality of cyberattacks and analyze structural challenges that we face in preventing or recovering from them. We then describe how cybersecurity is a relevant issue for businesses and business executives. Based on this discussion, we suggest some principles and specific actions that we recommend business executives take.

In Chapter 2, "Professionals at NTT," we introduce 14 employees engaged in cybersecurity at NTT. We describe their profiles, how they work, and their passions for their jobs. Examples include a researcher who is called an ethical (white hat) hacker, engineers who work in security around the clock, consultants who pursue a balance between business and security, and engineers who volunteer to help build a workforce outside of NTT. Our intent is to describe the kind of people we are talking about when we say cybersecurity workforce. We would be happy if you thought about "whether candidates for these roles may be around you."

In Chapter 3, "Initiating a game change," we describe the movement to establish the new realm that is starting right now 20 years after the internet started spreading to the world. One such global change is that Japanese companies are expected as global citizens to participate in the establishment of a new information-economy social system. We would also like to refer to the possibility that Japan's contribution can make use of its strength in quality assurance operations. We also suggest that cybersecurity be included as an attribute of "high quality" in the building of high-quality infrastructure, the demand for which is increasing globally. Lastly, as an advanced case for reference, we share the essential details of the public-private initiatives in the US.

We do not believe that NTT's abilities in cybersecurity are perfect. We need to improve both in protecting ourselves against cyber threats and providing cybersecurity services to our clients. Hence, we were a bit reluctant to publish this

book that makes an appeal to society on the importance of cybersecurity even though our own situation is not perfect.

However, we thought it would be fine to publish if sharing our ideas and revealing the profiles of some of our internal workforce could contribute to an increased awareness of cybersecurity for all of society, particularly among business leaders. We also thought we could improve ourselves by accepting opinions on NTT's cybersecurity from readers. From these considerations, we reached our decision to publish this book. We would be grateful if you could understand the context behind the decision to publish and give us your feedback and opinions after reading this book.

Chapter 1: Cybersecurity for business executives

1-1: Cybersecurity is a business management issue

Cybersecurity attacks are changing in quality.

The number of cybersecurity attacks continues to increase. Using a system to observe and analyze cyber attacks against the Japanese government and corporations, the National Institute of Information and Communications Technology reports that the total number of attacks in 2014 reached 25.66 billion, twice the number of the previous year. This number equates to over 800 attacks per second.

The change in the quality of the attacks is more serious than the increase in number. In 2000, attacks were generally conducted by criminals who enjoyed watching how people reacted to what they had done. Starting around 2003 or 2004, however, the number of attacks by economic criminals with the purpose of obtaining money or intellectual property has been increasing. Recently attacks have become multi-layered as the number of attacks with political intentions increases. The typical image of the cybercriminals has also changed. Previously, the instigators were major criminals who wanted to boast about their computer prowess in an era of crime for pleasure. Today, the number of attacks with economic purposes, which are thought to come from organized groups, has increased as have attacks with political intentions, which are assumed to have the support of national actors.

There are no official statistics on the amount of damage by these cyber attacks, but the June 2014 research report *Net Losses: Estimating the Global Cost of Cybercrime*, a collaboration between the Center for Strategic and International Studies (CSIS), a US think tank, and Intel Security, an American security corporation, estimated the worldwide cost of cybersecurity damage at 400 billion US dollars (equivalent to 48 trillion yen at a yen-dollar exchange rate of 120) or about 0.6% of world GDP. The report also describes variations in the ratio of damage to GDP, ranging from 0.02% in Japan (about 100 billion yen assuming GDP of 500 trillion yen) to 0.64% in the US and 1.6% in Germany. The ratio to GDP is generally higher in developed countries such as the G20 members. Japan's ratio is the lowest among the G20 member countries but the cost of damage could be underestimated

What is cybersecurity?

Under these circumstances, the Japanese government in November 2014 enacted the Basic Act on Cybersecurity; the act went into effect in January 2015. The act defines cybersecurity as follows.

Definition (Article 2)

For the purposes of this Act, the term "Cybersecurity" means that necessary measures are taken: to safely manage information, such as prevent against the leakage, disappearance, or damage of information which is stored, sent, in transmission, or received by electronic, magnetic, or other means unrecognizable by natural perceptive function …; and to guarantee the safety and reliability of information systems and information and telecommunications networks….

In short, it means “to prevent electromagnetic information from leakage, loss or damage and to protect the safety and reliability of information systems and networks.

Although the law refers to the reliability of information systems and networks, the applicable target for reliability is not limited to traditional computer systems, but also covers the recent emergence of the Internet of Things: information systems and communication functions that are embedded in various devices in such forms as IC chips. Applicable devices have widened to almost every type of device, including not only consumer electronics and rate meters but also wearable devices such as eye glasses, watches, and certain medical devices, in addition to social infrastructure such as streetlights, traffic lights, crossing signals as well as transportation systems including automobiles and airplanes.

For this reason, the Basic Act on Cybersecurity in Article 1 defines its broad purpose as “to enhance economic and social vitality, sustainable development and realizing social conditions where citizens can live with a sense of safety and security, and contributing to the protection of international peace and security as well as national security.” The Cybersecurity Strategy decided upon by the Cabinet in September 2015 also described the field of cybersecurity as “a frontier for producing limitless value” which has become “an indispensable activity at the foundation of the economy”

The essence of cybersecurity is to protect trust

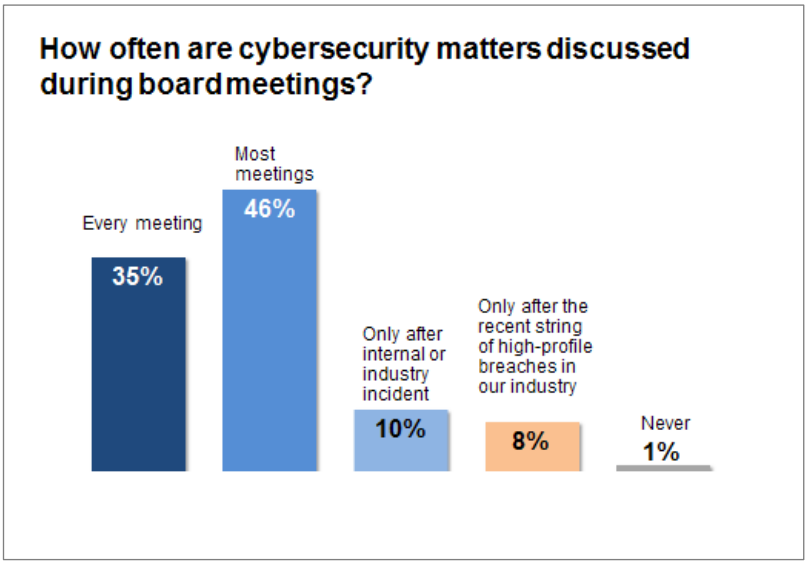
Now, we would like to consider the essential nature of cybersecurity. As described in the Basic Act on Cybersecurity, the purpose of security measures is to prevent leakage, loss, or damage of electronic information, which needs to be prevented because information integrity is a basic precondition for all social and economic activity.

We may say that our social and business activities are established under the assumption that all information is accurate. This assumption applies to factory operations and to device controls such as those for automobile driving and airplane operations. Under such circumstances, an organization that loses confidence in the information it sends or in the equipment it handles, would also lose trust in the organization's business development by its stakeholders such as business partners, customers, and society. Thus, the essence of cybersecurity is not only to protect the accuracy of information an organization sends or the equipment and devices it handles but also to protect the trust by others in their own businesses.

Positioning cybersecurity as a business management issue

If we consider cybersecurity as a management issue, its positioning changes. The traditional arrangement consisted of implementing systems for business, computerizing information as part of the process, and taking cybersecurity measures to protect this information. In short, the process went idea → business → information system → cybersecurity . But if we recast cybersecurity as protecting trust, we need to address cybersecurity as the twin management issues of protecting the information and equipment handled by our business and of ensuring others' trust in us as a business entity.

Ownership is different between the first issue and the second. For the first issue of protecting information and equipment, ownership belongs to a single group, the information system department. However, for the latter issue of ensuring trust in the business entity, all senior executive members are assumed to have ownership. A research bulletin published by NYSE Governance Services in May 2015 found that 35% of organizations discuss cybersecurity issue at every board of directors meeting and an additional 46% do so at most board meetings. In other words, over 80% of organizations discuss cybersecurity issues at every or almost every board meeting.



1-2: Cybersecurity has structural challenges

"Cybercrime is a growth industry." So states the report by CSIS and Intel Security, cited above. They see it as a field where "return is great and risk is low" and thus becoming an industry with high growth potential.

Cyber attackers have a structural advantage.

Cyber attackers have a structural advantage over defenders such as organizations at work or security companies. Once attackers find security holes at a target they can set a trap for a later attack; in contrast, defenders need to understand all security holes and take measures in response. Plugging every single hole would be impossible. Attackers can use a variety of techniques to target countless instances of software or hardware vulnerabilities. Once they find just one hole, they win—which gives them an asymmetrical advantage.

Black markets are out there.

Cybercrime has accelerated by the presence of two black markets. One is the market for personal information with high monetary value such as credit card numbers. The other market is that for cyber attack tools such as malware development kits.

Although there are no statistical data on these black markets due in part to their home in the underground economy, there is strong evidence that the black market for

personal information has grown dramatically over the past 10 years. According to the Trendlabs Security Intelligence Blog by Trend Micro, a prominent security company, credit card information is traded in the Russian black market at a few dollars per card number and online service account information is traded at 50 to 100 dollars per account. The black market in cyber attack tools is also rapidly maturing, even to the extent that markets for software support and training similar to the ones found in above-ground businesses have been established for beginners in cybercrime.

1-3: Key principles to follow

Although cybersecurity is a management issue, it is one in which the attackers unfortunately have a structural advantage, making it impossible for business executives to protect their organizations completely. In this situation, how should senior executives initiate policy for cybersecurity?

NIST Framework – a corner stone of US cybersecurity policy

Those who need to consider cybersecurity measures can refer to the *Framework for Improving Critical Infrastructure Cybersecurity* published in February 2014 by the National Institute of Standards and Technology (NIST), an agency of the United States Department of Commerce. The guidelines, known as the NIST Framework, lay out a framework for cybersecurity measures that was developed through a year-long process of soliciting opinions and comments from private sector organizations in response to Executive Order 13636 issued by President Obama in February 2013.

The NIST Framework was originally designed for organizations responsible for critical infrastructure but NIST soon realized that other organizations could benefit from the framework and broaden its scope to become the primary resource for cybersecurity policy within the federal government. Adoption of this framework is voluntary, but the government encourages its use by industry. Use cases have already been published by organizations and industry associations in finance, telecommunications, IT, and oil, et al.

The essential ideas can be summarized by the following three points.

1) Definition of measures before and after the protect function.

The NIST Framework defines cybersecurity measures to include not only protection against attacks but also to cover the periods before and after the protection is applied. Specifically, it enumerates five functions: identify, protect, detect, respond, and recover. In the NIST Framework, identify does not mean initiatives to identify attacks (which corresponds to detect) but rather means to identify assets or information for an organization to protect and define priorities for. This is considered to be the most important of the five functions.

2) A tool to promote continuous activity, not a certification standard.

The framework is a tool that uses the five functions to assess the current state of cybersecurity and to determine how much further each function needs to be strengthened to fill any shortfalls. In short, it is not a certification standard to obtain public endorsement but a live document to promote continuous activity.

3) An intentionally high level of abstraction with process and application depending on status.

In order to enable the framework to be modified or applied according to the state of cybersecurity at a given organization, it was intentionally designed to have a high level of abstraction. Those who are accustomed to the International Organization for Standardization (ISO) standards or the Information Security Management System (ISMS) tend to feel that this framework is too abstract to be useful, but in fact this is intentional in order to be flexible. This design is based on the assumption that users can advance their own customized efforts depending on their status or level of cybersecurity, rather than to have all organizations apply the same measures in accordance with a uniform set of standards.

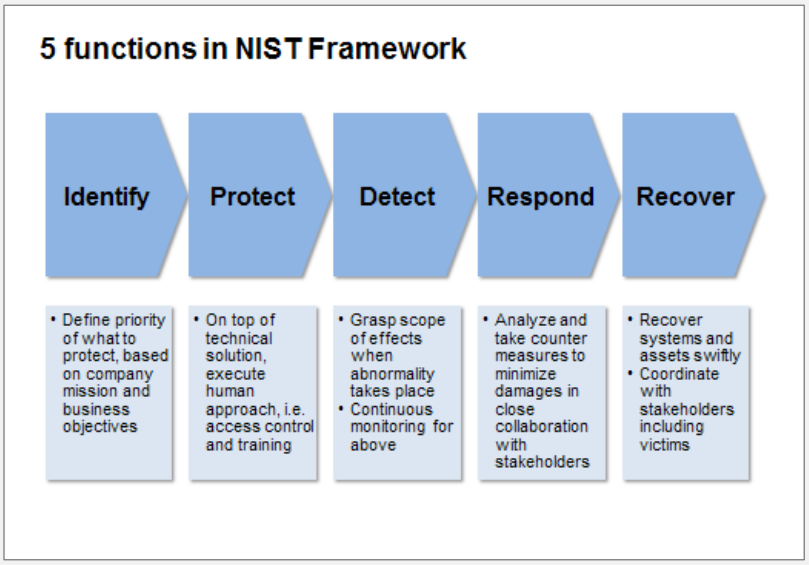
On the NIST Framework

On February 12, 2013, President Obama issued Executive Order 13636, *Improving Critical Infrastructure Cybersecurity.* Section 1 states, "It is the policy of the United States to enhance the security and resilience of the Nation's critical infrastructure and to maintain a cyber environment that encourages efficiency, innovation, and economic prosperity while promoting safety, security, business confidentiality, privacy, and civil liberties."

This order directed NIST to lead the development of a framework for reducing cybersecurity risks to critical infrastructure. Accordingly, NIST conducted five

public workshops and solicited opinions from industries, standard bodies, academia, and other parties. After taking these opinions into account, NIST then issued the framework in February 2014. A Japanese translation is available on the web site of the Information-technology Promotion Agency, Japan.

- The framework specifies five functions: identify, protect, detect, respond, and recover. Under these five functions are 22 categories and 98 sub-categories that define what activities need to be undertaken.



- Users are not expected to take all described actions or to execute them perfectly. Rather, each organization should first define on its own what it wishes to achieve and to what extent and then compare these goals to the current status. To reduce any gaps, the organization will then take actions to increase its organizational capabilities in cybersecurity.
- In the US, it is recommended that the NIST Framework be implemented by each industry. Companies and associations in such fields as finance, telecommunications, IT, and oil have announced use cases, and many say that the NIST Framework was useful as a common language within their organizations.
- Global corporations also participated in the process of developing the framework and requested that it be aligned with international practices and requirements. In response to these requests, NIST is working on international dissemination such as holding workshops and seminars in Europe, Japan, and China. In Japan, seminars were held in May and October 2014 with a NIST officers in attendance.

- The framework was originally developed for critical infrastructure players. However, people started to realize that the framework could be useful for industries not involved in critical infrastructure; the framework now plays a central role in the cybersecurity policy of the US government. The *FACT SHEET US-Japan Cooperation for a More Prosperous and Stable World*, issued after the April 2015 summit between President Obama and Prime Minister Abe, makes reference to the NIST Framework.

From the ideas of the NIST Framework, we here extract four principles that senior executives can refer to when initiating cybersecurity enhancements.

Principle 1: Initiatives should originate from the entire senior management.

If senior executives want to apply the essential ideas of the framework, they first need to gather support from the entire company and all departments. This is because the first step for this task is to determine what kinds of assets or information to protect and prioritize them. Although cybersecurity is a technical issue, it is not enough to leave the responsibility to the IT department alone. All senior executives must raise issues and initiate responses in their role as stakeholders and not leave the responsibility to the Chief Information Officer (CIO). For example, the CIO is not able to consider what the potential risks for their organization are; to identify the assets to protect and their locations, given the risks; and to determine which assets deserve top priority. This responsibility cannot be left to the CEO either. Every senior executive must help build common awareness across the company.

Principle 2: Consider each initiative as an activity in the continuous enhancement of organizational capability.

Cybersecurity measures should aim for continuous improvement in the ability to respond, not for perfect protection. The second function, protect, is important, but we should consider complete protection as something impossible to achieve given the current state in which the attackers enjoy a structural advantage. What is more important is how to **detect** after an intrusion from outside occurs, and then to react quickly to **respond** and **recover**.

For example, if an employee realizes that he or she has opened a file infected by malware, the employee needs to communicate the incident immediately within the organization in order to minimize the damage. Naturally the response capability not only by the department in charge of IT systems but also by the full participation of

other departments is put to test. Once recovery is complete, feedback is important to learn from this experience by applying the five functions starting with identify. By doing so, we do not consider damage by a cybersecurity attack as taboo, but rather an opportunity to enhance organizational capability to minimize damage from future cyber attacks.

Principle 3: Human resources development and employee training are imperative.

The NIST Framework is a tool that is easy to understand but it does not explain about the humans who actually operate this tool. Training responsible employees is very important to improving actual cybersecurity capability. It is not necessary for general organizations to have employees with highly advanced skills in security technology, and it would be reasonable to leave the responsibility for such skills to a technology company.

Three types of human resources and skills are required within an organization.

1) Risk analysts who can understand the characteristics of the organization and analyze and identify the assets and information to protect.
2) Information security engineers who can comprehend advice from professionals at a technology company and then implement this advice.
3) General employees with basic knowledge of cybersecurity.

We need to start developing these resources and improve their skills as stated above.

Principle 4: Actively engage in initiating information-sharing.

Because the NIST Framework is designed for a response by a single organization, it does not much refer to a cooperation with external organizations. Cyber attack methods have advanced rapidly, making it beneficial to exchange information with other organizations as much as possible instead of having the response come from only one organization. For instance, other organizations can share information about what type of attacks they have experienced or what kind of responses were effective.

Companies face the dilemma that they do not want to disclose their own information even though they seek information from others. One realistic way to overcome this dilemma is to create a members-only group with a mutually beneficial system to exchange information among members. Of course, in this case participants will also need understanding and direction from their senior executives because

these participants will exchange information on their attack experience with organizations outside the company.

1-4: Action items

What specifically should be done by senior executives who think about enforcing their own response capability for cyber security. The actions for them to take are different from those of an individual company depending on their situation, but here are some pointers.

Prioritize which assets and information to protect.

This action corresponds to the identify function in the NIST Framework. It is important for executives to understand that they need to start this action from a wide perspective, given what kind of management risks exist, rather than taking the point of view of asset and information management, which involves such matters as what kind of assets and information they need to protect. Executives need to review the details for management risks first. For example, how long will the company's competitive disadvantage last if technical information that is in the middle of its R&D phase is stolen, how large would the impact on delivery to customers be if production lines are stopped at manufacturing sites, and how much will earnings on sales for the whole company become negative if e-commerce websites fail to operate? After that, management will review which assets need internal protection and where they are located. They will then decide which ones need to be protected and determine their priority.

As an example of setting priorities, one organization would categorize the four levels of S, A, B, and C depending on what the impact would be if they suffer damage in a cyber attack such as leaked or destroyed data. For example, customer credit card information is categorized as S whereas publically available information about customers is categorized as C. With this categorization, the organization can maintain a balance between protection and detection and then proceed quickly to the next steps, response and recovery, as fits their business needs in case they do suffer damage.

Of course, it is not easy for an organization to determine priorities from a company-wide viewpoint. Probably few organizations can understand where and

what assets they possess or business risks they face. In such a situation, they need common standards within the organization to set priorities, but we believe that few organizations have such standards.

Such organizations need to conduct an asset and information inventory, originating with business risks, that involves departments that have not thought about cybersecurity so far. The top priority is to have common awareness, for instance, of what kinds of assets and information need to be protected in connection with their business risks. Creating a common language within an organization is very important for determining priorities. The NIST Framework is described in very simple words and is useful for an organization as an internal common language.

In addition, because electromagnetic data can be falsified, regardless of whether it can be accessed through the internet, it does not make any difference whether systems are connected to the internet when the identification function is performed. Plugging a USB memory stick into a control system at a factory is an example of a type of attack that frequently occurs. Or the attacker can drop a USB memory stick with the sticker “HR classified” in the company parking lot and wait until any employee at the organization plugs it into his or her own PC. This method has actually been used.

Prepare under the assumption that a breach will occur.

Perfect protection is impossible for an organization to achieve; realistically they are not able to completely protect themselves from cyber attack. Therefore, the organization must prepare for the detect step and the next steps, respond and recover, and conduct a drill as well. It is also important to determine an initial response, such as the information disclosure policy or a decision standard for suspension of service before technical initiatives are started. Then the organization must establish a structure for implementing these initiatives.

A Computer Security Incident Response Team (CSIRT), sometimes called the Computer Emergency Response Team (CERT), plays an important role in the technical aspect of implementation. The CSIRT is a professional team for cybersecurity measures whose members are assigned within an organization. The team detects cyberattacks against an organization and, in the event of a cyber attack, also assumes the role of an “internal control tower.” In addition, they are sometimes

responsible for researching the cause of the attack and its range of impact, or even for carrying out the task of damage recovery. The CSIRT is also in charge of exchanging the latest information on cybersecurity with external professional organizations.

In Japan, until recently only a few organizations had established a CSIRT; as awareness of their necessity has increased, one organization after another has established one. Advanced Japanese organizations that are using a CSIRT have established the Nippon Computer Security Incident Response Team Association (also known as the Nippon CSIRT Association or NCA), which has been offering advice to organizations that are planning to establish a CSIRT.

Receive risk analysis advisory (including tests by ethical (white hat) hackers).

An organization can receive a risk analysis advisory conducted from an external viewpoint to evaluate their business risks and analysis, and then assess whether their policy measures are appropriate. This is the first step to ensuring that their security measures fit their risk management policy and priorities.

In one approach, the organization can have an ethical hacker (a "white hat hacker") attempt to break their cybersecurity as a test to understand the current technical state of their cybersecurity. Submitting a company's security to a hacking test may seem absurd, but in Japan we have an expression that "if you know the enemy and know yourself, you need not fear the result of a hundred battles." Understanding how someone would attack and break into your systems is a very effective way to know how to protect and respond after an attack. This may sound indiscreet but it is similar to the approach police use to study how a thief commits a crime in order to reinforce their security and investigation skills.

Some people think that they are not able to prevent an attack because an attack may come from a group with advanced technology and sometimes support from a national government. But for most real attacks, the attackers use methods known in the past. Therefore, even if an organization submits its security to a test by an ethical hacker who is familiar with existing methods, it will be able to avoid a considerable number of attacks just by formulating a response based upon the results.

Initiate human resources development by building external personal connections.

An organization needs employees who can understand cybersecurity practices and determine the validity of applying it to their organization and who can take responsibility for the implementation and operation of a cyber defense. But it is difficult for people to learn by self-study. We believe that one realistic solution is to send employees to a corporate graduate school program where most of the instructors have practical experience and are not academic researchers.

Students would come from many different industries, which would foster an environment that helps them establish informal personal connections. After graduation, these connections will mainly help each student share information or work together with other organizations at their actual task. Even if it is not so easy for some students to exchange information officially, they will be able to get the latest information at a grass-roots level once they start to communicate with each other as trusted individuals. The important thing is that the organization should communicate well with trained personnel to explain how they can choose a career path that enables them to play active roles within the organization and ensure that they become indispensable resources for management.

One more important matter in human resource development and training is to involve everyone from senior executives to employees at work sites in raising the skill level and knowledge of cybersecurity and to have safe operations as much as possible, while also ensuring that an appropriate initial response will be taken when an actual cyber attack occurs. No matter how technologically advanced response may be implemented; vital information could be leaked if some employees have low awareness of cybersecurity.

The most vulnerable security hole is people. Measures must be in place, for instance, to acquaint all employees with basic knowledge of cybersecurity issues in internal training; in addition, there should be cybersecurity “fire drills” to verify that contact information, contact networks, and the means of response after a cyber attack are all in order.

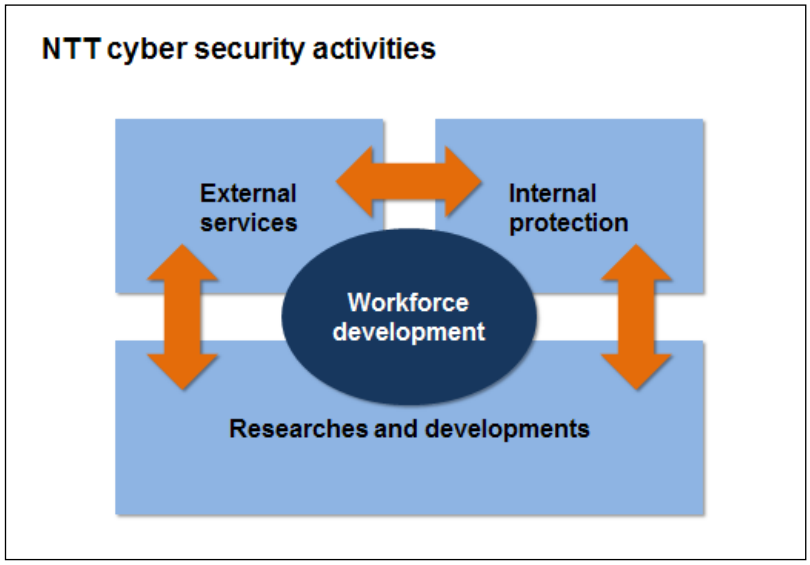
Chapter 2: Professionals at NTT

2-1: NTT's security activity connected by its workforce

NTT has three main cybersecurity activities. First, we provide security services to our customers to protect their assets and information; this is part of our business. Second, we protect NTT itself; when we provide ICT service to our customers, we do so with a high level of security by protecting our own information systems and networks. Third, we build our capability to support the first and second activities through research and service development at our labs and operating companies.

These three activities—customer protection, self-protection, and research and service development—are organically intertwined. The number of outputs from research activities that are put to immediate use in the market has increased in pace with rapid advances in technology. For example, knowledge about new types of malware or their countermeasures are immediately incorporated into our service technology for our customers and our technology to protect ourselves. Also, our service and self-protection technologies share much in common. This makes it easy at any time for us to leverage our knowledge and know-how developed for our own self-protection and employ it in services for our customers. Naturally this works just as well in the opposite direction.

The workforce plays an important role in forming the organic connections between these three activities. To begin with, we regularly rotate the workforce between the departments involved in each of these activities. Moreover, these organic connections between departments can be made more effective if those who provide external services to customers, those in charge of internal self-protection, and R&D personnel all know each other through connections formed by informal personal networks.



In this chapter, we will introduce 14 people in 4 categories of work keeping the above in our mind. To start, we introduce the activities and profiles of three ethical hackers. These three concentrate in different areas—malware, hacking contests, and talent scout—and have been active in other areas beyond their official roles and responsibilities. They sometimes extend their professional activities outside of the NTT group.

Next we introduce six members of our workforce who provide external services to our customers, along with their work areas of consulting, operations management, and security for financial services. The six have different backgrounds, including one person with previous sales experience, one who studied humanities and social science, and an American, but we would like to focus on how they feel and think about initiating security improvements for their customers.

Thirdly we would like to introduce several of our workers who provide internal protection to NTT itself. We inquired into efforts by three people who work on the frontlines of the company to strengthen its cybersecurity based upon their experiences when a part of NTT was under cyber attack and its cybersecurity was breached.

Lastly we would like to introduce the initiatives of three people in research and service development who work on developing the following initiatives: a project to leverage the capabilities of the entire NTT group as it becomes increasingly global; a new field of security for hardware and cyber physics; and encryption.

2-2: Ethical (White Hat) Hackers

Defending against malware - Aiming for a world of zero cyber-damage

Makoto Iwamura
Distinguished Researcher,
Senior Research Engineer, Cyber Security Project
NTT Secure Platform Laboratories

Many people, upon hearing the word "hacker," will conjure up an image of a cyber attacker who is attempting to gain unauthorized access. Originally, however, the term meant a person who has deep knowledge and excellent technical skills on a computer. Actually many ethical hackers work at NTT. These workers exhibit a strong motivation to cooperate with others outside of their organizations and initiate activities beyond the realm of NTT.

One ethical hacker who represents NTT is Makoto Iwamura, a leading person in making remarkable improvements in defenses against malware proliferation on the internet.

"My ultimate goal is that my job will disappear. If the world is rid of all vulnerabilities, then malware created by attackers to target a computer and then cause it to malfunction or destroy it loses its meaning. My dream is by my retirement to establish systems with security that cannot be exploited by attackers for making money."

"I entered NTT because this is one of the biggest organizations in Japan that provides a full-stack of services from network to IT systems and which has conducted research on security."

"Attackers have the upper hand in a cyberattack. If the defenders stop or yield, then attackers can gain whatever they want. If attackers are allowed to do whatever they want, then trust in ICT will fall and the market could stop growing. I will never let such a thing happen."

Hacking contest - Improving our skills on the world stage.

Hiroki Hada
Senior Analyst,
Operation & Consulting Dept.
NTT Com Security

In early August of every year, a large number of top class security technologists gather at the DEF CON convention in Las Vegas. Hada has aimed for three years to participate at DEF CON in the world's toughest hacker contest with volunteers from the NTT group. Regrettably he has lost in the preliminaries in all three years, but he now attends a classroom program to win in the preliminaries next year and qualify for the final. Hada realizes that he has matured technically and personally through the study sessions. As he increases his concentration not to miss any word of the instructor, he thinks, "we will qualify next year."

"I can view my ability objectively by competing with professionals from all over the world. My ability as an engineer will not grow anymore if I keep a narrow-mind and only defend my territory. Security technology is always advancing. The challenge of DEF CON is that it gives me a great opportunity when I think about my skill level and what I need to do to improve my skill."

"Working with dozens of NTT people with expertise in different areas is very stimulating for me as I work in a small team. We try to solve issues for DEF CON by thinking of all possibilities of attacks and vulnerabilities at the same time. We can expand the breadth and depth of our skills if we engage in many issues."

"I feel that a wide variety of talented individuals is represented in the NTT group and we study hard by accepting the challenge of competing at DEF CON. We hold a study session after office hours, and many participants even cancel their other appointments in order to attend. We have strong motivation and a sense of exploration, which enables us to improve our skills by working with our colleagues. This is a great opportunity.

Talent scout - Scouting prospects we can entrust our future to.

Kunio Miyamoto, PhD
Senior Expert
NTT Data-CERT
Information Security Office, Quality Assurance Dept.
NTT Data

Around 265,000 workers are employed in information security in Japan, About 160,000 do not have the required skills and more importantly about 80,000 more workers are potentially needed. There is one person at NTT Data who can make a great contribution to building a cybersecurity workforce in Japan: his name is Kunio Miyamoto. Miyamoto has been devoting his energy to a "talent scout camp" project for young engineers to whom we can entrust our future, not only at NTT but throughout Japan.

"It is not enough if engineers just improve their skills. It is more important to judge calmly when they should put their abilities to use."

"Current cyber attackers can do their work with a higher return on investment; for example they can make a 1,000 yen profit on a cost of only 10 yen. But if defenders improve their skills and attackers require greater costs, the number of attacks must decrease. No one wants to try if for instance they have to pay 200 yen to make a 100-yen profit."

"I believe there is no cybersecurity field in academia. There are various technical fields such as operating systems or networks and component technologies, which are connected vertically by security. Workers with various fields of expertise gather and explore what to do to avoid being attacked. So when we learn about security, we can learn about technology outside of our areas. As an engineer, I really enjoy this."

"I want graduates of the camp to surpass me in their skills and take responsibility for future security. That is all right—I believe this is the desire of every instructor. I believe the future created by such young people will be a bright one."

2-3: External services

Consulting - Security measures with a business perspective.

Chris Lincoln
Senior Manager
Managed Security Services Taskforce,
Corporate Planning
NTT Communications

Misa Nakada
Chief Engineer
Security Business Unit,
Cloud and Security Business Dept.
NTT Software

We suspect that lots of companies have not done the basic part of security planning, for example by identifying “what they should protect” or “what kind of risks they have.” Chris Lincoln, a security consultant at NTT Communications tries to address these issues by building a consulting group.

At the same time, there is an accelerating trend towards companies trying to bring out new services or strengthen existing businesses by utilizing the large volume of data accumulated within a company, known as big data. But if they take a false step in handling this information, they may be criticized by society because big data sometimes includes personal information. Misa Nakada of NTT Software, who consults on big data, is exploring the way to success by utilizing big data with her clients while trying to encourage her clients to mitigate risks.

“Strength in overseas networks is a differentiating factor for our company over competitors. Many of our clients have both domestic and international bases. We provide support to these clients by cooperating with our foreign bases and head office. I play the role of ‘hub’.”(Chris Lincoln)

“I like being thanked by clients, ‘Thank you very much. You really helped us.’ over being praised ‘well done’ by my boss when submitting paper work. I would like to make use of my knowledge for the benefit of others and society.” (Chris Lincoln)

“My duty is to make our clients feel safe and focus on their business while the gap between regulations and reality expands.” (Misa Nakada)

“There are many experts at NTT Group and if we ask them to present their expertise in a technical lecture they are happy to accept. My target audience is business executives. I do not communicate well with them just by describing the details of the technology. I talk instead of how security has a business effect and a return on cost. My role is to connect clients and technology as a person who can speak on such a topic.” (Misa Nakada)

Operation center – People should protect cybersecurity since attackers are also people

Shinji Abe
Senior Analyst
Operation & Consulting Dept.
NTT Com Security

Hiroki Hada
Senior Analyst
Operation & Consulting Dept.
NTT Com Security

A massive wave of cyber attacks is upon us. Attackers outsmart defenders and pursue further attacks until they slip through protections. One NTT organization on the frontlines of fighting this wave is the Security Operation Center (SOC). The center analyzes attack information and attempts to restore normal conditions if they discover an attack. “Who will protect clients if we don’t?,” ask the two young leaders of SOC, who devote themselves to improving their skills at perceiving the nature of attacks.

“The security business in essence does not sell or create things. The thing providers sell is safety and the thing customers buy is a sense of security. Then let’s provide the best safety.” (Shinji Abe)

“The idea that we can automatically protect ourselves from advanced and persistent threats only by machine is not correct. Human knowledge and experience is needed to confront attackers who check up on our skills and think up methods to outsmart us. Then they implement them and keep attacking until they actually slip through.” (Shinji Abe)

“Ten years from now? As a team, we want to strengthen our ability so that people can say the security team of NTT Com has the best technology in the world. We also want to focus on building up our subordinates. If we build a good workforce, we can provide good services. If our profit goes up as a result, we can strengthen our team. It is a virtuous cycle. To do this, I want to continually improve my skills as a security engineer.” (Hiroki Hada)

Security in financial services - Responding to customers' need for trust

Shuuichi Yoshida
Manager,
e-Business Promotion Group, e-Business Division,
Second Financial Sector
NTT Data

Satoomi Nabeshima
Senior Consultant
Security Business Division, Security Consulting Section, Consulting Support Group
NTT Data Intellink

The cyber attacks that most affect daily life or business activities are the ones that target money. Damage is serious: according to the National Police Agency of Japan the amount of damage suffered by internet banking users was in 2014 twice that of the previous year at 2.91 billion yen and the number of financial institutions that suffered damages has increased to 102 from 32.

Further security measures are being necessitated by the expanding range of uses for online payments, which is making them indispensable. The challenge will only increases the government is encouraging greater convenience for the growing number of foreign tourists who use credit cards or debit cards for everyday shopping as the Tokyo 2020 Olympics approaches.

Financial service systems take first priority in ensuring public trust. Two people who make great efforts everyday to protect security and improve convenience of these systems are Shuuichi Yoshida of NTT Data, who calls himself "a translator of security," and Satoomi Nabeshima of NTT Data Intellink who established a foundation for avoiding leaking of credit card information in Japan.

"My job is to clearly inform our customers about what is happening now. I provide information by thinking how much security threats affect our customers, and not just by telling about threats. As I was in charge of system development and sales

for financial systems for almost 20 years, I can understand the viewpoint of customers who worry upon hearing threat information."(Shuuichi Yoshida)

"I was glad to hear our customers' state their appreciation by saying they were able to reduce damage as a result of reading my report. However, at the same time I strongly realized the importance of routine work and the sophistication of attackers' techniques, and I was really motivated." (Shuuichi Yoshida)

"If the customers of more and more shops can use credit cards, it will improve users' convenience. But this increases the chances that cyber attackers will strike. Unfortunately, in the recent past, many cyberattacks have taken place in the Olympics' host countries. Many retailers currently understand the importance of security measures but are not sure how they need to do so specifically." (Satoomi Nabeshima)

"Ideas or solutions to protect credit card information have mainly come from overseas. We need to propose more ideas and solutions from Japan." (Satoomi Nabeshima)

2-4: Internal defense - Protecting NTT from the inside.

Junichiro Saito
Staff,
Cybersecurity Group, IT Innovation Dept.,
NTT East

Katsuhiko Eguchi
Security Engineer,
Cyber Security Operation Center,
Network Headquarters
NTT Neomeit

Naoko Chiba
Manager,
Information Security Dept.,
NTT Docomo

NTT group companies have also come under cyber attacks. There are people who make great efforts to provide safe and secure ICT services and increase protection capability inside the company every day.

Threats from attackers have breached the wall of protection in the past. Junichiro Saito of NTT East and Masahiko Eguchi of NTT Neomeit have developed their skills in security measures by making use of their experiences in being attacked by new types of cyber threats. Naoko Chiba of NTT Docomo makes every effort to improve security measures for several thousand information systems.

“Some parts of our work can be automated by software. However, talking with the people responsible for operation sites is a conventional but very important task. This is the most basic procedure but indispensable to ensuring security.” (Junichiro Saito)

“We do not need lots of praise. I am filled with a sense of mission that I can’t explain during my response to incidents. I dare to say that it is enough to hear thank

you. Those affected are glad to have us here when we resolve incidents. Hero without a name? Maybe it is too good." (Katsuhiko Eguchi)

"Technology such as encryption or authentication that prevent unauthorized persons from reading data is indispensable, but in the end, management issues concerning the people that handle information are more important." (Naoko Chiba)

"We can deal with security as familiar things like our meals or a bath. If the number of people who pay attention to and understand both business and security from these points of view increases, they will use our services more safely and confidently." (Naoko Chiba)

2-5: Research and development

Global service development - Enabling world-best services.

Hiroko Matsuoka
Manager,
Managed Security Service Taskforce, Corporate Planning
NTT Communications

"I would like to do my job both domestically and internationally." Hiroko Matsuoka joined NTT Communications in 2001 with such thoughts. She spent most of her career overseas and is now the leader of a project to achieve global unification of managed security services (MSS).

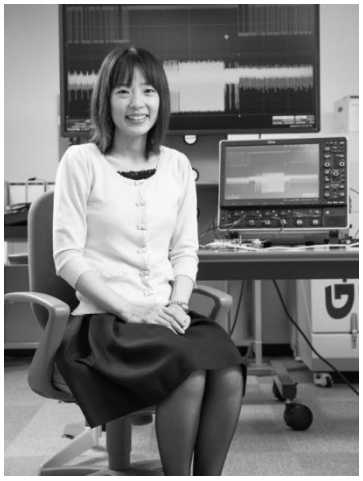
Why is global unification important? With it, we can collect threat information from all over the world by utilizing NTT's far-reaching global networks. It also enables us to provide global standard MSS to our customers that have developed their business globally. Moreover, global unification makes it possible for us to detect attacks earlier than anyone else and protect our customers by introducing the latest analytical approaches. This is our MSS strategy at NTT.

"We organize product development systems on a global scale in order to create products with the same quality at any location in the world. We do this for the benefit of our customers but it eventually benefits us as well."

"I want to do as much as I can to make the world of security more open through our services. In the interim, our profits may go down temporarily. We provide the minimum required services only by confirming our customers' actual security risks. Such a situation must be ideal for our customers."

"Conflict occurs mostly if people with different personalities work together. This tends to be uncomfortable but a more interesting result is created once we get over any personal conflicts The reason I want to do work in the global area is that I want to always be in a situation like this."

Hardware security - From smart cards and automobiles to the Internet of Things



Junko Takahashi, Ph.D.
Research Engineer
Security Platform Group, Data Security Project
NTT Secure Platform Laboratories

The metal strip on a credit card often has an embedded IC chip that contains personal information or card information. Certain cyber attackers will try to steal this information without even touching the card. Protecting the security "things" or "hardware" is taking on greater importance as the time is approaching when any device can be connected to the internet. Junko Takahashi, a research engineer at NTT Secure Platform Laboratories, initiated security for smart cards and other hardware.

"We use a different part of the brain for dealing with research than we do for business. I have productive days with both research and business even with heavy responsibility and difficult subjects."

"In the concept of safety, a different axis from security is established for an automobile from old times. I wonder if we can strengthen an automobile's security by combining safety with conventional security technologies."

"I expect my research on how to avoid cyber attacks upon hardware will make a solid contribution to our customers with advanced IoT businesses. I want to propose a level of security that fits specific business requirement and contributes to security architecture by utilizing my knowledge gained through implementation of cryptographic defenses against cyber attack."

Cryptographic technology – Invisible social infrastructure

Masayuki Kanda
Senior Research Engineer
Secure Architecture Project
NTT Secure Platform Laboratories

Cryptography is indispensable to using the internet. In fact it is so indispensable to security that the encryption to make communications unreadable by a third party was once treated like many weapons and prohibited for export. Despite this critical importance, users are often not conscious of cryptography at all. The main reason for this is that cryptographic technology has been very well designed—users do not have to pay it any mind because it doesn't cause any problems. Masayuki Kanda is a leading person in support of this advanced technology.

A boy who was fascinated by mystery novels, Kanda studied cryptography in college and graduate school because he wanted to find a way to thwart the increasing number of crimes aided by computers and computer networks. He has pursued this interest ever since he joined NTT.

"It is very important to consider encryption in terms of lifecycle management. Ideally, we should think about having an encryption replacement plan that goes into effect after a 5- to 10-year span by switching over to a new encryption regime, taking the timing into consideration when systems are updated."

"There is a big gap between cryptographic researchers and business people who use cryptography. The words used by cryptography researchers are completely different from the ones that touch consumers. I want to take on the role of the bridge that connects the two."

"My activity at Information-technology Promotion Agency (IPA; a Japanese government-affiliated organization) will probably not have many advantages or benefits for a private company like NTT. But the work is necessary for the future of cryptography in Japan. People around the world recognized that NTT Research

Laboratories is a center of excellence in the fields of security and cryptography. We are proud to leverage Japanese cryptographic technology for its merits for all of Japan, and not just its merits for one company. I suppose it is something only NTT can pursue”

Chapter 3: Initiating a game change

3-1: Changing the game with everybody's participation.

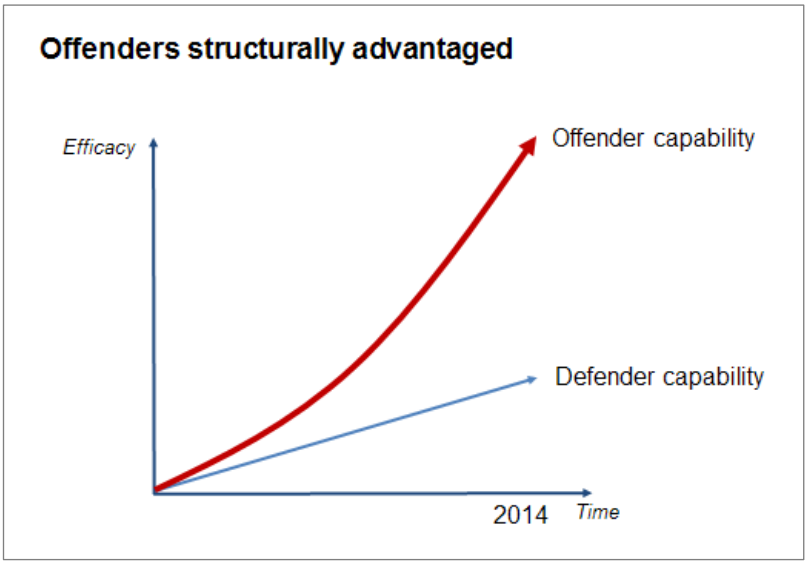
Necessity of a game change

"There are defenders (who protect your network from cyber attacks) and attackers (who attempt cyber attacks) in the world. Our skills as defenders have advanced but attackers' skills have advanced with much faster speed than those of defenders because attackers have a structural advantage. If we leave such a situation as it is, we are not able to maintain an internet as a system."

These remarks were given in August 2014 in Las Vegas by Jason Healey, an influential person in the cybersecurity industry, at Black Hat USA 2014, a leading international conference on cybersecurity. For hackers, participating in this conference is their dream. Black Hat attracts so much attention that it is called an annual festival.

Healey is a cybersecurity expert who has been working as the director of the Cyber Statecraft Initiative at the Atlantic Council, a US think tank. In his career, he has taken on a succession of roles, including engagements in actual cybersecurity work in the US Air Force and at Goldman Sachs and in cybersecurity policy at the White House and as the Vice Chairman of the Financial Services Information Sharing and Analysis Center (ISAC), which is described later in this report.

Because the internet is now a part of the social infrastructure, it is obvious that society and the economy would suffer critical damage if the internet could not be maintained as a functioning system. As described in Chapter 1, attackers have a structural advantage over defenders. If we do not change this structure, we will not be able to secure our safety in society or the economy in the future. This is the point that Healey wishes to emphasize.



Vincent Cerf, an internet evangelist at Google who is often referred to as "the father of the internet," is similarly aware of this issue. In April 2014, at the Global Conference on Cyberspace 2015 (GCCS) in The Hague, the Netherlands, he stated, "The internet resembles urban development. If we consider packets (a minimum unit of data going around network) as vehicles, networks are roads and computers are buildings. As we need traffic rules in a secure city, we need rules in each area such as information generation, transmission, and consumption. People seek security."

The number of cyberattacks has been constantly rising and taking countermeasures against them has become an important international issue that needs to be solved in order to keep the internet working and enable it to achieve stable development as a core part of our social infrastructure.

Establishing global rules starts now.

The delivery of Windows 95 in 1995 probably created the opportunity for internet usage to spread across general businesses and consumers. In the 20 years since, the technologies, products, and services that use the internet have made great steps forward. But the establishment of social rules has not kept fully apace with the advancement of technologies, products, and services. The internet is thus sometimes compared to "the wild west," an open world where everyone can get a chance but also a space where law and order is not easily maintained.

As a result of its wide penetration, the internet is no longer a completely virtual

space separated from the real world. Rather, it has become a part of real life, and a world that brings together the cyber world and the real world is about to appear. If this happens, the internet should not remain a wild west. Establishing systems and rules is necessary for a world that brings together the real and the virtual. Progress on this matter is relatively easy if the internet is a closed system confined to each country. But the internet has no borders limiting where it can be used; indeed, it has become a social foundation spanning all of the world's countries. For this reason, there has been little progress in establishing global rules. The entire internet faces a serious crisis forced upon it by cyber attacks, making now the time to establish rules on a global scale.

A combination of physical technology (science and engineering) and social technology (humanities and social sciences technology) is required.

Maintaining cybersecurity necessitates technological advancement in computer science including such fields as personal authentication, encryption, and malware detection. Moreover, security technology in its current state is hard to use—a problem that requires assistance from studies such as ergonomics. We choose to call these science and engineering as “physical technology”. In addition to “physical technology”, there are humanities and social sciences which we choose to call “scale technology”.

To take strides forward in cybersecurity, we need to advance social technology as well as physical technology. Social mechanisms need to be improved and advanced first in a process in which current society moves to a true information utilization society where trust in digitized information can be secured. Specifically, we need to include the viewpoints of privacy protection, ethical education, cooperative transnational systems to pursue cross-border criminal activities, and each country’s legal system. If the world cooperates to advance these efforts, it can establish social rules combining the real and virtual worlds. But it is only after we can set a pair of wheels in motion—physical and social technology—that we can initiate a game change.

Examples in physical technology (science and engineering).

- Authentication such as using biometric authentication as an alternative to passwords.
- Malware detection methods.

・Network technology to selectively control suspicious communications.
・Forensics.
・Software development and technology to hinder intrusions.
・User-friendly interfaces utilizing human engineering principles.

Examples in social technology (humanities and social science)
・Privacy law.
・Cybersecurity requirements in company audits.
・Childhood education.
・Cooperation to pursue criminal activities across borders
・Support for building capabilities in developing countries.

Companies also need proactive measures.

So how should companies participate in a game change? Would it be fine if companies leave their responsibilities of technology development to technology companies or social system changes to the government? We suppose not. Companies are places where cyberattacks happen. They need to protect themselves and continue to work on minimizing the damage if they are attacked. As the owners and operators of sites where cyber incidents occur, they have an important role in initiating a game change.

One example is information-sharing. Companies share information with others on their experiences with cyber attacks. An individual company's protection and response skills are developed by mutually sharing information with other companies. Eventually, this leads to advancement of protection ability in all of society. Suppose a given company's network is attacked by cyber criminals using a new technique. If the company makes known the details of its attack experience, other companies can take measures against this technique. The result is that protection skills are advanced throughout society. Such an initiative has already started in the US with the Information Sharing and Analysis Center (ISAC) that fosters the sharing of information within an industry.

We can also think of activities in which educational institutions and companies work together to build and recruit a cybersecurity workface. Their plans and efforts are required to seamlessly connect companies' work sites and educational sites. For instance, companies can describe required profiles for their security workforces for

undergraduate and graduate schools, provide students with opportunities for on-the-job training, provide guidance on career paths to these students after hiring, and then continually maintain their skills so that they can keep current with technical advancement—a role they share with educational sites that take responsibility for corporate training.

It is also important to raise basic knowledge about security and promote proper security practices to society at large through general staff training. In the future, the number of people working at home will increase as work styles diversify, and the number of opportunities for employees' work to engage in Bring Your Own Device (BYOD) will also increase. These circumstances will make it important for companies to convey basic knowledge of security not only to their employees but also their families. Perhaps companies may initiate training and educational programs on security that involve employees' families as well, so that their employees can work in a safe and secure environment.

Aim to strengthen cooperation of private sector companies with cross-industry forum among volunteer companies.

In June 2015, NTT convened a cross-industry cybersecurity forum for the purpose of providing a chance to strengthen corporate security activities by having volunteer companies work together with other leading companies. Around 40 companies from 15 industries participate in this group, with emphasis on industries responsible for critical infrastructure such as finance, electric power, railways, and chemicals. Another purpose of this group is to provide a place where participating companies regularly consult with each other or ask for advice on issues they are not able to speak about publically We expect that participants will be able to bring back the knowledge they obtain and utilize it to improve their own cybersecurity skills, and also be able to create an information-sharing system like ISAC in their own industry. The forum currently plans to conduct activities focusing on three topics: 1) building an internal cybersecurity workforce, 2) building a workforce for the next generation, and 3) sharing information through cooperation among private sector companies.

3-2: Learning from the US as an advanced case.

Since May 1998, when President Clinton issued Presidential Decision Directive

(PDD) 63, stating that the "level of dependency on infrastructure and information systems in both fields, economy and military have increased," initiatives in the US to strengthen cybersecurity involving industry, government, and academia have been undertaken. We would like to introduce some practices and reference points concerning what NTT obtained from its activities in the US. Please note that the range of activities is limited to the civilian field; the military field, including intelligence, is not touched upon.

Activities to share information by industry.

The PDD 63 also established ISAC, an organization connected by mutual trust for the collection, analysis, and sharing of information on security by industries responsible for critical infrastructure. In order that the nation be prepared for possible cyber attacks on critical infrastructure, this PDD recommended the clarification of responsibilities among government agencies and the establishment of professional organizations for information-sharing. The directive also requested the sharing of information on any cyber threats to national security in each area and vulnerabilities that indicate defects in the nation's infrastructure. ISAC was established in response to this request.

The National Council of ISACs (NCI) was established in 2003, five years after the directive, with the mission of mutual cooperation among the ISACs from individual industries. The primary members at the start were public infrastructure industries such as utilities, gas, finance, and telecommunications, but since then participation has been extended to other industries. As of June 2015, 19 ISAC members participate to NCI.

According to the documents published by the Asia Pacific & Japan 2014 - RSA Conference, the ISACs have the following mission:

- To serve as an organization established upon mutual trust by the operators of critical infrastructure.
- To share comprehensive analysis and results of a whole industry, either within the industry or with other industries and the government, while protecting the anonymity of information sources.
- To cover all threats, including natural disasters as well as cybersecurity.
- To identify the threat level for each industry.
- To emphasize operations at the incident sites by taking timely and

appropriate actions.

Leaders participate proactively.

On February 12 and 13, 2015, the Summit on Cybersecurity and Consumer Protection was held at Stanford University and hosted by the White House. Executives from the government and major companies gathered at this summit and issued a call to action concerning the cybersecurity threat. Panelists at the first panel discussion on the theme of "Public-Private Collaboration on Cybersecurity" included the CEOs of major private companies and non-profit organizations, such as American Express, Pacific Gas & Electric, Palo Alto Networks, and Kaiser Permanente as well as the Deputy Secretary of the Department of Energy. Jeh Johnson, the Secretary of Homeland Security, served as moderator. The theme of the second panel discussion was "Improving Cybersecurity Practices at Consumer Oriented Businesses and Organizations." The panel was moderated by Secretary of Commerce Penny Pritzker and featured CEOs from Master Card, AIG, Bank of America, the Center for Democracy & Technology, and Intel, who presented their organizations' initiatives and commitments.

President Obama appeared on the second day, following the panel discussions. In his remarks he pointed that the only way to protect our country from cyber attack threat is to have the cooperation of public and private sectors. As the leader of the country, he emphasized the need for cooperation between public and private sectors. President Obama illustrated one of the topics of the summit, improving the security of password authentication, by describing how he had used a simple password in his school days. He showed how vulnerable a simple password could be by talking about his experience in using "PASSWORD" and "123457," which drew laughter from the audience.

With the president talking about his experience, the cabinet members serving as moderators, and CEOs from major organizations that represent the country participating as panelists, leaders from all sectors, public, private, and non-profit, participated proactively in cybersecurity and promoted the importance of initiatives.

Private sector takes the lead, while the public sector supports.

"We are under cyberattack every week. It is an embarrassment that you are asking for our support 18 months in advance!"

This remark from the representative of the supply chain ISAC, consisting mainly of retail industry members, was uttered in a room at the North American Electricity Reliability Corporation in Washington, D.C., during a morning session of National ISAC Committee Meeting, held once every three months. It was directed at the Cyber Exercises Officer of the Department of Homeland Security when the officer requested support for a cyber exercise planned for 18 months later.

"It was hard for us to prepare for the previous exercise. Did you review it? How can you leverage the results?"

The representative of the supply chain ISAC asked questions to inquire about further situations. The DHS officer replied, "I will explain next time." This is probably the best that the officer could do because he had not prepared sufficiently.

This conversation clearly demonstrates the sense of ownership of cybersecurity that private sector companies have in the US. As the company's own issue, an idea spreads widely and the company initiates a solution by itself at first before coming to the government. The government considers their attitude as something to be expected and sees its role as supporting private sector companies. This idea of the private sector companies taking the lead adheres to the theme of the previous conversation.

"We cannot hope to keep up if we adopt a prescriptive regulatory approach. We must harness the dynamism and innovation of competitive markets to fulfill our policy and develop solutions."

This was a part of remarks on cybersecurity measures made in June 2014 by Tom Wheeler, the Chairman of the Federal Communications Commission, a regulatory agency of the telecommunications industry in the US government. The head of a regulatory agency stated publicly that it is impossible to protect cybersecurity by prescriptive regulations.

In an era in which technology advances rapidly, the moment the government decides on compliance requirements, attack methods to outsmart them are generated. This makes it is impossible to secure cybersecurity if we only depend on regulations

or guidelines by the government. The only way to make cybersecurity effective is to utilize market mechanisms and continue to innovate, something which should be absolutely led by the private sector. Both the US government and the private sector companies have consistently thought this way. This common philosophy lies at the base of US cybersecurity policy. The idea is to completely initiate cybersecurity measures by a company's own efforts and not by regulations.

Close cooperation between operating sites and policymakers

"A person from the government shouts and asks 'what's happening?' and we reply 'please relax!'. This kind of conversation occurs almost every day."

This remark was made at the Department of Homeland Security by the executive of a major telecommunication company, a main member of the telecommunication ISAC. NTT representatives visited there to learn about the structure of the US National Cybersecurity and Communications Integration Center (NCCIC), which maintains the security of the federal government's communication networks, at a meeting with an officer of the Department of Homeland Security. This remark comes from another attendee at the meeting who is a key person of the telecommunications ISAC in response to our query about cooperation between the government and the private sector.

The officer of the Department of Homeland Security replied to her remark saying, "it is best for us to trust what they say because it is telecommunication companies who operate the communication networks after all. We ask questions persistently as we have the responsibility, but we need to respond by facing reality calmly. For doing so, it is important for us to respect opinions from the operating sites of telecommunication companies." She explained further that "we have repeated this argument for over 20 years. Trust obtained through this approach is our foundation." The building where NCCIC is located has private rooms for responsible officers from four major US carriers (Verizon, AT&T, Centurylink, and Sprint) with their company logo on each of their doors; this close proximity facilitates measures to deal with actual situations through close connections between operators at operating sites and policy makers.

3-3: Japan's proactive participation as a global citizen

The Office of Management and Budget, a branch of the Executive Office of the President of the United States, described the policy that stipulates that the federal government procurement guidelines include companies' cybersecurity measures.

Under this policy, companies need to fully implement their cybersecurity measures when they accept outsourcing of frontline operations for handling sensitive information from the federal government. Draft guidelines for public comment were issued in August 2015. For instance, one guideline stipulates that the deadline be specified in the contract for reporting an incident observed by the company from the contractor to a government agency. The Office of Management and Budget has stated its intention to announce the final guideline by the fall of 2015. We expect it to have been announced by the time this book is published.

A similar movement has already taken hold in the UK, where the government announced the Cyber Essentials authentication system in June 2014. This system is an illustration of the basic activities for cybersecurity protection at private companies. As of October 2014, companies are required to obtain certification when they want to submit bids for government procurement contracts involving the handling of sensitive information.

These international trends show that the development of cybersecurity measures is not only needed to protect the organization's own information but is about to become a precondition for business development. In this current situation, we have no time to wait before taking measures.

Comparing the situation in the US and the UK to Japan, we suppose that the sense of urgency is not high for Japan. We often hear chief information officers of Japanese companies say, "We, as a company consider cybersecurity to be an important issue. But we are not sure how far we should take measures. There is no common sense rule as to what extent measures should be taken, and that causes us problems." The impossibility of providing 100% protection even if cybersecurity measures are taken means that these officers need to judge through discussion with top management whether "the measures agreed upon so far are fine." Nevertheless, the current lack of such standards is a genuine problem. The result is the common

complaint from CIOs that “senior executives of our company ask us to ‘target measures with zero-risk.’”

There are no perfect protection measures we wonder if top management of Japanese companies tends to avoid discussing cybersecurity or considers it taboo for this reason. We also wonder if they leave their responsibilities to certain departments and thereby avoid this issue in top management discussion. The time has already come when business executives need to position cybersecurity at the center of the management agenda and tackle it squarely.

Acting as a member of global community.

At the Global Conference on CyberSpace (GCCS) held on April 16–17, 2015 in The Hague, the Netherlands, participants from various positions in government, corporations, and civil organizations gathered to discuss what should be done for a free and secure cyberspace. This fourth edition of the conference, which followed previous ones in London, Budapest, and Seoul, was well-attended with nearly 100 countries represented. The big theme for this edition was improvement in cybersecurity for the several billion people in developing regions such as Africa where many people will soon be connected to the internet.

Around 30 people from Japan participated including Yasuhide Nakayama, the Senior Vice-Minister for Foreign Affairs. NTT also participated and during the panel discussion described their protection measures based on network technology. This could be an example of how Japanese companies do not hesitate to show what they can do themselves and that they recognize the need to participate in a game change as a member of the global community. Now that cybersecurity has become a social issue in which people around the world need to cooperate, it would not be an exaggeration to say that the potential development of all humanity will be endangered if the damages caused by cyber attacks continue to spread at their current speed. Cybersecurity is an issue comparable it its gravity to global warming; solutions necessitate cooperative structures that transcend borders. Japanese companies should engage in this issue proactively and think about ideas and forward-looking initiatives to reach solutions together with others.

Utilizing Japan’s strengths.

Japan needs to tout its unique strengths when it participates in the global

community. An example that reflects well on Japan is when its men's soccer team regrettably lost its final match in the preliminary round of the 2014 FIFA World Cup tournament in Brazil. Despite this setback, it was Japanese supporters who picked up the trash at the stadium after the loss and were highly praised all over the world for their actions. In another example, following the Great East Japan Earthquake of 2011, large crowds of people continued to wait in disciplined lines for their suspended train service to resume. For actions like these, people from around the world have developed high expectations of the earnestness and honesty of Japanese people.

Operational quality assurance is an area of original strength for Japanese companies in services as well as manufacturing. It is said that "the most vulnerable security hole in cybersecurity is people." All of an organization's members must improve their skills in order for there to be improvement in the organization's cybersecurity. We can say that initiating cybersecurity improvement is equivalent to how quality assurance leads to business trust at operating sites. This is an area of strength for Japanese companies, as exhibited by their work on quality circles.

Contributing to the provision of high-quality infrastructure.

In order to respond rapidly to future increases in the demand for infrastructure, Japan will put in place high-quality infrastructure overseas, particularly in the country's economic development partners in Southeast Asia. Here, "high-quality" means environmentally friendly and hard to destroy. How about incorporating "being cyber secure" in this term as well? Japanese companies can play an important role in this type of development.

Cooperation with local infrastructure operators is essential for local infrastructure development, and Japan could make a unique contribution by including cybersecurity through the utilization of the workplace skills that Japanese companies have strengths in.

There is an expression called "social capital," which is often translated into Japanese as *shakai kankei shihon* (social-related capital). The term encompasses hard infrastructure such as electricity, water, and roads, but is also extended to mean trustful relationships or principles among members of society. Social capital can then be used as an indicator of the maturity of an individual society. Japan has excellent social capital; it is what the Japanese people have built little by little over their long

history. Creating a game change is nothing more than building social capital in the true information utilization society. We propose that Japanese companies actively initiate cybersecurity by utilizing their strengths in building social capital.

Closing

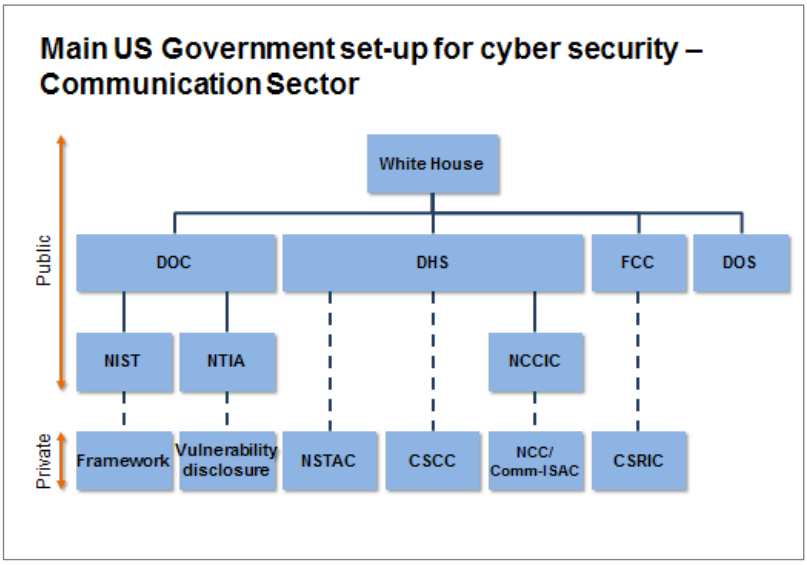
Shinichi Yokohama, Head, Cyber Security Integration, NTT Corporation

Public advocacy in cybersecurity.

In July 2014, NTT established the position of external spokesperson on cybersecurity at its holding company; I accepted this position. The NTT group intends to advance its cybersecurity activities both domestically and internationally under the theme of transcending international borders, as the current awareness of NTT's overseas activities in this regard is not high enough. A major element of my mission is to take part of the responsibility in solving this issue. For this reason, we are promoting our activities by focusing on two matters. One is to have policymakers, industry organizations, and external partners in the cybersecurity field understand the profiles and capabilities of all elements of NTT; the other is to play a leading role in proactively shaping the market for cybersecurity, which is still in its infancy globally.

We started our first activity in the US, which lies at the center of the world both in being targeted by cyber attacks, and in taking countermeasures and establishing and implementing policies. As stated in the introduction, our motivation to publish this book is that "we would like to make a broad appeal to everyone that cooperation by every player is required in cybersecurity measures in a time when everything is connected to everything else." Our fundamental idea is to introduce what we have learned or discovered through our activities in the US to the Japanese business community.

The US government has a complex cybersecurity organization that involves the Department of Defense and intelligence agencies, among many others, but we have focused our activities in the civilian area. We here introduce four activities that NTT has undertaken so far. The chart of US government cybersecurity activities looks as follows, after making certain simplifications, for collaboration through public–private partnerships in the communications sector.



1) Participating in the Communications Sector Coordinating Council (CSCC), led by the Department of Homeland Security.

CSCC is a council where the government explains its policies, programs, and requests for support and where companies exchange information and otherwise engage in mutual cooperation between the government and other communications sector stakeholders NTT has participated in the council since December 2012 and is the only company among its 40 members whose head office is not located in North America. Sample agenda items, addressed in monthly teleconferences and semi-yearly face-to-face meetings, include feedback on the result of participation in cybersecurity drills organized by the government, and consultation on collaborative policies with other industries such as finance and electric power. By participating in CSCC, we can understand the latest actions in US cybersecurity policies.

2) Participating in the Communications Security, Reliability and Interoperability Council (CSRIC), led by the Federal Communications Commission.

CSRIC is a council where major players in the telecommunications sector discuss measures to be taken to protect safety and trust in communications, including technical opinions. NTT has participated in one of the cybersecurity working groups since December 2014. Specific discussion topics include measures to implement the NIST Framework, information-sharing, and workforce development. Whereas CSCC is affiliated with the Department of Homeland Security, a non-regulatory agency, CSRIC is affiliated with the Federal Communications Commission, a regulatory agency. Through our participation, we can understand the

regulatory views of the US government.

3) Creating a use case from the NIST Framework

In March 2015, we held an internal meeting in Washington, D.C., attended by practitioners of cybersecurity from NTT group companies all over the world. An officer of NIST was invited as a special guest. After the officer's presentation on the NIST Framework, we conducted a workshop where we used this framework to review cybersecurity services at all NTT group companies.

4) Presenting our opinions and introducing our technologies at international conferences.

We attended the White House Summit on Cybersecurity and Consumer Protection, held at Stanford University on February 12–13, 2015. NTT was the only non-US company represented at the panel discussion, where we presented our views on issues faced by the private sector. We also attended the Global Conference on Cyberspace 2015, held in The Hague, the Netherlands, on April 16–17 (described in Chapter 3), where at the at plenary panel meeting we introduced attendees to our network technology to isolate and deroute attack traffic.

These activities are called "public advocacy" in English. As advocacy means "protect" or "support" and public advocacy means "an activity to present our opinions publicly and contribute to opinion formation in the process of planning, decision and achievement of public policy," we can say that this is "advocacy activity based upon the public interest viewpoint." This activity is not the same as lobbying. Whereas lobbying means to achieve one's own interests through public policies or obtaining approval or denial from government public advocacy has a more public tone. Public advocacy is more public-spirited because it uses public forums to propose policies to make the world better (although such advocacy may in the end deliver economic benefits to the advocator).

Respecting the multi-stakeholder spirit

In Chapter 3, we described the essence of US cybersecurity policy which we learned about through public advocacy activities. From my view, the encompassing concept is "the spirit of the multi-stakeholder."

Multi-stakeholder literally means a diverse (multi) group of related individuals

and organizations (stakeholders). Cybersecurity is a theme that really needs such a spirit. A diverse set of stakeholders participate in cybersecurity, for example regular companies, consumers who use the internet, and technology companies that provide technologies or protection measures. In addition to these, there is a wide span of stakeholders that covers law enforcement and judicial organizations; regulatory agencies; organizations dedicated to the protection of civil rights, particularly those who deal with privacy issues; lawyers; universities; intelligence agencies; the military; and international organizations. Participation by every stakeholder to solve such complicated issues embodies the spirit and approach of multi-stakeholder.

I felt this way for the first time when I attended a workshop by NIST in October 2014 in Tampa, Florida. That was the sixth workshop on the NIST Framework. The workshop was held for the purpose of having companies, industry organizations, and standards bodies present their experiences in applying the NIST Framework, which had evolved through the previous five workshops. A second purpose was to clarify what participants needed to spread the use of framework.

Around 300 attendees took part in open discussions over two days and not a few participants mentioned their skeptical view or questions on the effectiveness of the NIST Framework. In response, the effectiveness of the NIST Framework was defended not by NIST staff, but by participants from other private sector companies. In particular, we often saw a group of around 50 “six-timers” who attended all workshops explain backgrounds of framework development and their intentions to use it proactively.

I told a participant I met after ending the first day of the workshop, “participants who attended in the previous workshops behaved like missionaries.” The participant replied “this is the effect of the fact that NIST has advanced discussions involving all participants to develop the framework.” The participant continued, “NIST proposed the framework which can be accepted as the consensus of many people listening to and accepting various opinions or thoughts, not just the enforcing of a certain viewpoint. We have reached this point through such a process. I suppose this approach or the process itself is innovation.”

All attendees concerned took part in open discussion and expressed their opinions and exchanged views with others because cybersecurity is a complicated

theme. The participants have ownership for the output of the process regardless of whether or not their opinions are reflected in the final outcome. As a result, the conclusion compiled by NIST includes agreement from numerous stakeholders, and this helps to increase effectiveness.

It surely takes time and effort to have open discussion, since different people have different opinions. But as a result, the knowledge of all participants can be collected to reach an appropriate conclusion. This is because the approach enables them to share their trust and beliefs in open discussions.

Cybersecurity and NTT's evolution into a global ICT company

Lastly, I would like to explain the background behind why NTT started to initiate public advocacy on cybersecurity.

NTT is changing itself from “a telecommunications company in Japan” to “a global ICT company” as demonstrated by several specific indicators. First there are only four telecommunications companies in the world with sales of over 100 billion US dollars—AT&T and Verizon in the US, China Mobile in China, and NTT. We are not able to compare sales exactly as each company discloses information in a different format, but among these four companies NTT has the highest ratio of sales in IT. Our sales ratio is nearly 20% and about twice that of the other companies, which run around 10%.

We would like to examine NTT’s high sales ratio in the IT field from a different point of view. The NTT group has several companies which provide IT services, including NTT Data, NTT Communications, and Dimension Data. If we sum up sales of IT services at these group companies, the amount would come to around 20 billion dollars, which would put us near the top five companies in the global ranking of IT service companies published by various marketing research companies. In other words, we are in the top five globally in both network and IT services. This is NTT’s most recent status, and we may say that our business characteristics are globally unique.

NTT has promoted growth in overseas markets, especially IT, at a time when the domestic market is maturing and huge growth cannot be expected in the future. The result is that NTT is on the verge of establishing a unique global presence as an

integrated telecommunications and IT company. We currently position cloud computing and cybersecurity as two important areas for growth in the overseas market.

Within these two growth areas, cybersecurity stands out as having as dual missions to protect both our customers and ourselves. To achieve the dual missions, NTT advances technology development, the accumulation of operation expertise, and workforce development including an aggressive collaboration program with external partners. Through these activities, we can increase our capability in cybersecurity and plan to incorporate this capability into our organizational skills. In other words, NTT aims to become a security company.

The global cybersecurity market is growing at close to 10% annually but makes up only 5% or so of the entire ICT market. The aim of positioning cybersecurity as one of our two main growth engines is to seek expansion in the cybersecurity business itself and also to reinforce our competitive ability in other services. Specifically we plan to achieve differentiation by embedding cybersecurity capabilities and technologies into network services, cloud services, provisioning of infrastructure services, and IT application services.

NTT is growing in the global market and positions cybersecurity as a differentiating factor in its growth. To achieve cybersecurity, the group is raising its global capabilities. We have much room for progress in all of these skills, but we believe we can contribute to the game change described in Chapter 3 if we advance these skills by increasing the number of “fellow workmates” who appreciate our efforts towards the achievement. We will continue our efforts to become a security company without losing this aspiration.