

When You Think You Are About to Hesitate, Step Forward. Increase Freedom and Trust People in the Field



Shinichi Yokohama
Chief Executive Officer,
NTT Security Holdings

Abstract

In today's connected society, ensuring safety and security in cyberspace is an extremely tough challenge. NTT Security Holdings provides security services to clients on the basis of its proprietary cyber intelligence and threat-detection-and-response capabilities. We asked Shinichi Yokohama, chief executive officer of NTT Security Holdings and chief information security officer of the NTT Group, about the company's mission and strategy as well as his attitude as a top management.

Keywords: cybersecurity, security operations center, trust

The strengths of NTT Security Holdings—NTT's only company specializing in security

—Could you tell us how NTT Security Holdings was established and what are its features?

NTT Security Holdings is the only company in the NTT Group that specializes in security. Our mission is twofold: first, to maintain the security of the NTT Group's companies and support their activities and second, to provide security services to our clients.

NTT Security Corporation was established in 2016 and was temporarily a division of NTT Ltd. In 2022, on the recognition that security will become even more important to the business strategy of the entire NTT Group, it was reorganized as a direct subsidiary of the holding company and renamed NTT Security Holdings.

I believe that NTT Security Holdings has five unique strengths. The first strength is NTT's scale. Since NTT operates a huge information and commu-

nications infrastructure, it is the target of numerous cyberattacks at any moment. Therefore, we are able to learn about the world's most-cutting-edge cyberattack methods.

The second strength is our advanced technologies for promptly detecting cyberattacks and rapidly responding to and recovering from them. Cyberattacks have become so complex and sophisticated that 100% protection is no longer possible. Accordingly, we assume that an intrusion (cyberattack) from outside will occur, and we are required to detect it quickly, respond to and recover from it, and minimize the damage it causes. To meet those requirements, the NTT Group operates a security information and event management (SIEM) engine—which also uses artificial intelligence—to collect activity and log data from security devices and automatically detect, visualize, and notify threats. To make this SIEM engine function even more effectively, we have a global partnership for collecting and sharing threat information with highly skilled analysis engineers present at



our globally linked security operations center (SOC). Therefore, a virtuous cycle is created in which the input threat information is analyzed by our talented engineers and knowledge is accumulated, which allows us to provide fast and effective services.

—The above-described environment based on a huge global information technology (IT) infrastructure and excellent technical capabilities alone are of competitive advantage.

Our third strength is an abundance of human resources. Employees of the domestic NTT Group companies are required to take cybersecurity-related training. Approximately 3% of its employees in Japan, or about 4500 people, have obtained the certificate of “intermediate level,” which recognizes them as people who can play an active role in the cybersecurity field. NTT also employs approximately 100 experts having industry-leading achievements recognized by outside experts. Since NTT operates a huge information and communications infrastructure, we can develop those talent in our own cybersecurity field.

Our fourth strength is expertise backed by a wealth of experience. As a partner of the international sporting event held in Tokyo in 2021, we were able to play

a part in the defense against cyberattacks and other threats to that event. We have also accumulated experience in handling major international events such as the G7 and G20 Summits. Global events are held every year in Japan, and every time a VIP from around the world visits Japan, such as when Ukraine’s President Zelensky visited the G7 Hiroshima Summit, it attracts the world’s attention. Such a stage is ideal for those who want to launch cyberattacks. I believe that our strength lies in the expertise we have acquired from our experience for cyber defense in these situations.

Teaming up with clients and partners to build a more secure society

—With both the organization and knowledge in place, your company has a solid foundation. You have recently authored a book, correct?

Yes, the book is called “Towards World-Class Cybersecurity Practice” and its publication is an example of thought leadership, which is our fifth strength. Efforts in cybersecurity are generally not disclosed because of concerns that doing so could provide attackers with hints on how to attack. In my role as the chief information security officer (CISO)

of the NTT Group, I exchange opinions on cybersecurity and other topics with various companies and organizations, and I meet many people who have problems in handling cybersecurity issues. Having the desire to help them, I decided to disseminate information about our cybersecurity efforts. We have a team dedicated to publicizing cybersecurity information. We have also set up a presentation room where our clients and partners can see the operational state of our SOC.

When we first started to disseminate cybersecurity information, we heard concerns that doing so might be handing an advantage to attackers; however, we are already being targeted enough by attackers. Since NTT aspires to become a truly globalized digital company, hiding is not an option for us. We changed our way of thinking and decided to team up with clients and partners instead of hiding. We live in the era of Internet of Things, where everything is digitally connected. I believe that it is important to protect not only our own company but also the entire supply chain, including electric-power companies and other companies on which NTT relies, as well as our clients in a manner that makes society as a whole more secure.



—Many cybersecurity-related incidents have recently been reported. How do you view this situation?

I am actually very positive about the cybersecurity being the focus of attention. When I first started working in the cybersecurity field ten years ago, I felt that awareness of cybersecurity in society as a whole was low. For example, the cybersecurity incident at a large international media company 10 years ago was covered by the media, but for many people and companies, it may have been perceived as “someone else’s problem.” However, it is now widely known that cybersecurity incidents occur frequently both domestically and internationally and that responding to them requires much effort and expense. I think there is a growing awareness that cybersecurity incidents are no longer “someone else’s problem” but a “crisis happening right now” and “a threat to our company that could occur at any time.” In other words, society is becoming more aware of the importance of cybersecurity. There is also a growing awareness that cybersecurity is not an IT issue but a management issue.

Even if companies recognize that cybersecurity is a management issue, many do not know what they should do and to what extent they should take measures. In many situations, therefore, a security officer is appointed and security matters are left to them, and those security officers are troubled about what they should do and to what extent they should take measures.

The NTT Group consists of both large companies and small companies, such as startups with around ten employees. Such diversity of companies is what characterizes the NTT Group. We have a wealth of expertise in cybersecurity in regard to both large and small companies, and we want to offer that expertise to our clients.

The NTT Group also experienced a major data breach due to internal fraud at NTT WEST. We profoundly regret that the incident lasted 10 years. To regain the public’s trust, we intend to raise the level of our internal security.

External services and internal defense for the NTT Group are two wheels of the same cart for fulfilling our responsibilities. Regarding external services, our diverse clients range from domestic companies to multinational corporations of all sizes. For all of these clients, we leverage our five above-mentioned strengths to provide consulting, knowledge provision, system integration, and other security-related services that are tailored to their needs and environments.



In regard to internal defense for the NTT Group, we will ensure that the so-called Three Lines of Defense Model of governance and risk management (defined by the Institute of Internal Auditors) is fully functional, and the incident that we experienced is an opportunity for us to go back to basics and reaffirm our commitment to security. While it is fundamental that each operating company takes the initiative, NTT Security Holdings, under the direction of the NTT holding company, will promote complementary initiatives to enhance the collective strength of the NTT Group. For example, since security is not only a technical issue but also a management issue, NTT Security Holdings will provide training to the presidents of domestic NTT Group companies.

Trust each other and become a reliable presence

—The pressure of being the head of security for the NTT Group seems considerable. What attitude do you have towards your daily work?

I sleep with my smartphone next to my pillow, and since I receive reports of security incidents that occur for the NTT Group both in Japan and abroad and respond to them 24 hours a day, I would be lying if I said I feel no pressure. When an incident occurs, the

most-important task is to minimize the damage it causes. To minimize the damage, it is important to give freedom to the people in the field who understand the situation better than anyone else, including the incident that has occurred.

It doesn't matter if there is a slight delay in reporting a security incident to me, the CISO of the NTT Group. To be honest, it can be frustrating if the situation is not reported to me immediately, but I try to think that it is because the people in the field are busy doing everything in their power to minimize the damage. I think it is important to increase the freedom of those in the field and trust them.

I joined NTT after working at the Ministry of International Trade and Industry (now the Ministry of Economy, Trade and Industry) and at a consulting firm. When I worked as a consultant for a major beverage company, I would sometimes ride with the company's delivery truck drivers as they drove around town to think about measures to improve the sales capabilities of the company. One time, a driver told me about the things you won't get to hear unless you are in the field, including a delicious local Chinese restaurant at which drivers would eat between shifts. Listening to their voices, I became convinced that leveraging their strengths, namely, knowing the overall situation and environment in the field, would lead

to good work. This experience was the starting point of my desire to trust the people in the field.

It is also important to communicate my belief to the people in the field. Therefore, at my first meeting as the chief executive officer (CEO) of NTT Security Holdings, I told the participants that my belief in my work is “When you think you are about to hesitate, step forward.” I’m not sure if this belief always produces the right results, but if we proceed and find that we are wrong, we can correct mistakes immediately.

—Employees must be reassured to know that the CEO has confidence in their work. What are your future aspirations and what would you say to readers?

A good corporate culture cannot be created overnight, but I want to make it a priority to maintain unwavering trust in those in the field. To that end, I focus on the things that only I can do, and I want each and every employee to focus on the things that only they can do. This way of working is important not only for gaining my trust but also for employees to gain the trust of each other in a manner that enables us to all to be a reliable presence and say, “I can leave it to them.”

Although NTT’s security business is still in the development stage, we aim to be a world-class security company. Achieving this aim does not mean being the best in the world; it means being proud to sit at the same table as top-class companies. I have said that external services and internal defense for the NTT Group are two wheels of the same cart, but it is

important that NTT Security Holdings becomes the “security hub” of the entire NTT Group, and I believe that if NTT can pool all its strengths, we will be able to win trust externally.

I want all of you involved in research and development to approach your work with pride. Expectations from around the world concerning the security capability of Japan and NTT are growing. In that sense, NTT has an enormous opportunity to excel. I want you to conduct research and development with pride in building security practices in your field. To our clients and partners. We will disclose as much of our knowledge and expertise as possible, so please join us in building a more secure society.

Interviewee profile

■ Career highlights

Shinichi Yokohama joined the Ministry of International Trade and Industry (now the Ministry of Economy, Trade and Industry) in 1984 and McKinsey & Company, Inc. in 1992. He became the head of the Business Integration Department at the Global Business Headquarters of NTT DATA in 2011 and a special advisor to NTT, responsible for increasing the external presence of cybersecurity, in 2014. He has been the CISO of the NTT Group since 2018 and CEO of NTT Security Holdings since June 2023.