Cybersecurity R&D to Counter Global Threats

Takeshi Nakatsuru, Yoshiaki Nakajima, Jun Miyoshi, and Katsumi Takahashi

Abstract

New cybersecurity threats are continuing to expand on a global scale, and Japan is expected to become the target of cyber-attacks in the run up to 2020. In these Feature Articles, we discuss the key points of resisting global cybersecurity threats and introduce our research and development strategy for dealing with them.

Keywords: security, global, R&D strategy

1. Introduction

The NTT Group has aggressively expanded into the global business sector to establish global cloud services as a cornerstone of our business. To this end, we are establishing stronger systems to offer to the world by responding to the needs of our customers who are developing diverse information and communication technology (ICT) services on a global scale. In the global business arena, ICT is an essential component that is used by a wide range of businesses in diverse fields. Incidents of cyber-attacks on these businesses can cause serious damage such as service interruptions or information leaks. In recent years, many cases of cyber-attacks directly aimed at exploiting business secrets or financial assets have been reported, and the financial impact of these attacks is also increasing.

NTT Group's managed security service provider companies are expanding their services in order to address these issues in the global business arena. Cyber-attacks on global businesses raise various concerns, including the risk of theft of business secrets through industrial espionage and the disruption of key infrastructures such as electricity, gas, and communications.

Broadly speaking, there are three points that global businesses must follow to protect themselves from the latest security threats and new threats accompanying the latest technological developments. We describe them here and explain our efforts to address them in section 2.

1.1 Technology and security operations are both important when responding to targeted attacks

The NTT Group's Global Threat Intelligence Report (GTIR) analyzed common factors in businesses that had suffered losses and found that although unknown threats that instigate targeted attacks against businesses and other organizations do exist, most attacks exploit known vulnerabilities that are sometimes several years old. To deal with these incidents, it is essential not only to use advanced techniques such as attack detection, but also to implement operations to pre-empt attacks by taking steps such as establishing patch management processes and incident response procedures, and by training people how to deal with attacks.

1.2 Making use of threat intelligence is essential to reduce the cost of security operations

Cyber-attacks are becoming more organized, with corporate spies and even state agencies among the perpetrators in some cases. In these cyber-attacks, there are clear profits to be made by the attackers, who may also have considerable financial resources at their disposal. When running a global business, it is

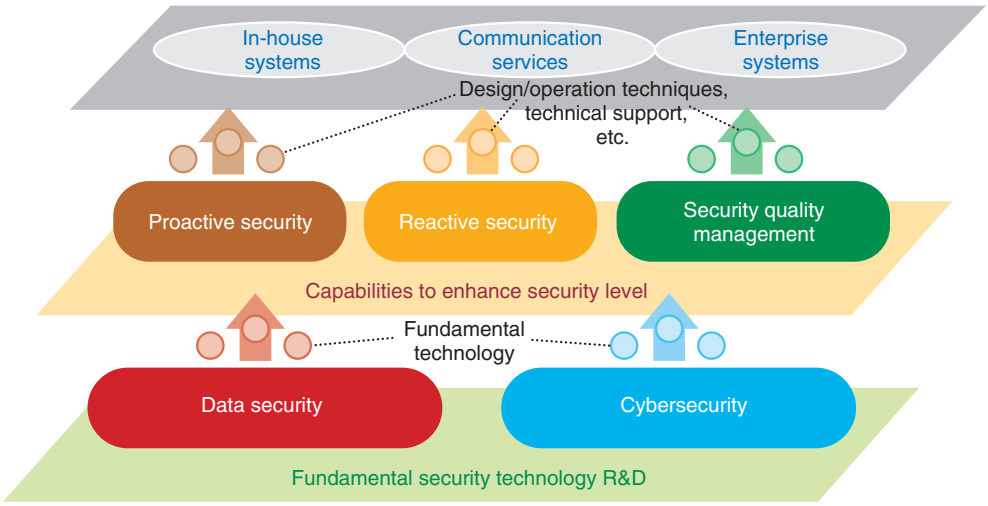

Fig. 1. R&D efforts focusing on security measures.

difficult to put a cost on security alone, so it is necessary to apply measures efficiently. It is also important to make use of threat intelligence such as that on new types of vulnerabilities and the places from where attacks are originating, which makes it possible to balance the cost of security measures by pre-emptively blocking access from attack sites and to increase the efficiency of business operations.

1.3 Integration of the real world and cyberspace is essential when applying security measures in the IoT era

As technology advances, we are fast approaching the Internet of Things (IoT) era, where all sorts of things will be connected to the Internet. In some respects, this era has already started. For example, the use of IoT has been discussed for applications such as self-driving automobiles and the optimal distribution of electric power. In this sort of world, cyber-attacks are considered as a possible cause when there is an incident such as a widespread power outage in one area. In dealing with such cases, it is first necessary to clarify the relationships between incidents that occur in the real world (physical accidents) and those that occur in cyberspace. To respond to these incidents, it is essential to implement a response that takes both real-world and cyberspace factors into consideration.

2. R&D efforts to respond to global cybersecurity threats

At NTT Secure Platform Laboratories, we are engaged in research and development (R&D) in order to implement security measures to keep up with changes in the latest threats and the latest technologies (**Fig. 1**).

Regarding the first point mentioned in section 1, we are not only studying fundamental security technology aimed at creating the world's most advanced systems, but we are also studying how fundamental security technologies can be used to provide enhanced security for in-house systems, communication services, and enterprise systems. We are working to enhance the level of security by not only researching and developing ways of dealing with incidents before and after they have occurred, but also investigating security designs that can be easily operated.

Regarding the second point, we have launched initiatives for sharing threat intelligence with global Group companies including NTT Innovation Institute, Inc. (NTT I^3), which was founded in 2013 as a North American base for R&D.

Regarding the third point, we are researching and developing integrated risk management solutions that combine the know-how of NTT Secure Platform Laboratories on disaster response systems, and the know-how of NTT-CERT* in handling incidents in

* NTT-CERT: NTT Computer Security Incident Response and Readiness Coordination Team

response to cyber-attacks.

In these Feature Articles, we first present some case studies of cybersecurity threats in the global arena [1], and then we discuss two of our activities associated with threat intelligence [2, 3]. Finally, we introduce our efforts aimed at integrated risk management [4].

References

[1] Y. Aragane, K. Ogura, H. Endoh, and K. Takahashi, "Trends in Global Security Threats," NTT Technical Review, Vol. 13, No. 12, 2015.
https://www.ntt-review.jp/archive/ntttechnical.php?contents=ntr201512fa2.html

[2] T. Hariu, K. Yokoyama, M. Hatada, T. Yada, T. Yagi, M. Akiyama, T. Ikuse, Y. Takata, D. Chiba, and Y. Tanaka, "Security Intelligence for Malware Countermeasures to Support NTT Group's Security Business," NTT Technical Review, Vol. 13, No. 12, 2015.
https://www.ntt-review.jp/archive/ntttechnical.php?contents=ntr201512fa3.html

[3] T. Koyama, B. Hu, Y. Nagafuchi, E. Shioji, and K. Takahashi, "Security Orchestration with a Global Threat Intelligence Platform," NTT Technical Review, Vol. 13, No. 12, 2015.
https://www.ntt-review.jp/archive/ntttechnical.php?contents=ntr201512fa4.html

[4] T. Kokogawa, N. Kosaka, A. Koyama, F. Ichinose, F. Tanemo, and Y. Maeda, "Efforts to Achieve a Joint Risk Management Support System," NTT Technical Review, Vol. 13, No. 12, 2015.
https://www.ntt-review.jp/archive/ntttechnical.php?contents=ntr201512fa5.html

Takeshi Nakatsuru
Senior Research Engineer, Planning Section, NTT Secure Platform Laboratories.

He received a B.S and M.S. in computer science and system engineering from Yamaguchi University in 1998 and 2000. In 2000, he joined NTT Information Sharing Platform Laboratories, where he worked on R&D of VOIP (voice over Internet protocol), location awareness systems, and NGN (Next Generation Network) subscriber session control servers. In 2008, he joined NTT WEST and developed high speed (200M and 1G) optic network services for consumers. He joined the R&D planning section in 2012 and was involved in launching NTT I^3 as the North American R&D base.

Yoshiaki Nakajima
Senior Research Engineer, Supervisor, Planning Section, NTT Secure Platform Laboratories.

He received a B.S. in information science and an M.S. in mathematical and computing science from Tokyo Institute of Technology in 1995 and 1997. He joined NTT Information and Communication Systems Laboratories in 1997, where he worked on R&D of information security. From 2009 to 2013, he was with the Security Strategy Section of the Technology Planning Department. He has been involved in R&D of information and communication platforms, security platforms, and other areas.

Jun Miyoshi
Senior Research Engineer, Planning Section, NTT Secure Platform Laboratories.

He received a B.E. and M.E. in system engineering from Kyoto University in 1993 and 1995. Since joining NTT Telecommunication Networks Laboratories in 1995, he has been researching and developing IP networking technologies. From 2006 to 2011, he was engaged in developing FLET'S Hikari networks at NTT and NTT WEST. He has been involved in security R&D management since 2011. He is a member of the Institute of Electronics, Information and Communication Engineers.

Katsumi Takahashi
Executive Research Scientist, Senior Manager of Planning Section, NTT Secure Platform Laboratories.

He received a B.S. in mathematics from Tokyo Institute of Technology and a Ph.D. in information science and technology from the University of Tokyo in 1988 and 2006. He joined NTT in 1988 and has studied information retrieval, data mining, location information processing, information security sociology, privacy preserving techniques, and cryptographic techniques. He has developed several commercial systems including i-Townpage, Mobile Info Search, and privango.