Measures for Corporate Cyber-attack Preparedness and Resilience

In May 2017, Hitachi became the victim of a worm-type virus called WannaCry that shut down in-house systems, creating an impact inside and outside the company. Responding to the rise in cybersecurity threats with the arrival of the IoT era, Hitachi has made information security governance its top management priority. Specifically, since October 2017, it has been promoting the governance and technical aspects of corporate preparedness and resilience, and created two specialized security divisions reporting to the Chief Information Security Officer. Looking ahead, it will continue working on security risk reduction activities for all its equipment. These activities will affect not only its office automation IT environments, but also extend to equipment in its product and service business areas (including IoT/OT systems) and its development and production equipment.

Toru Matsukawa
Hiroshi Nishihama
Daisuke Shibata
Akihiko Kawasaki
Hajime Nodaguchi

1. Introduction

Hitachi is responding to new threats such as rapid cyber-attacks by positioning information security as its single most important management priority. It is working to make the entire company more resilient in terms of both governance and technical aspects. This article looks at Hitachi's efforts to increase resilience against cyber-attacks.

2. Looking back on the WannaCry Cyber-attack

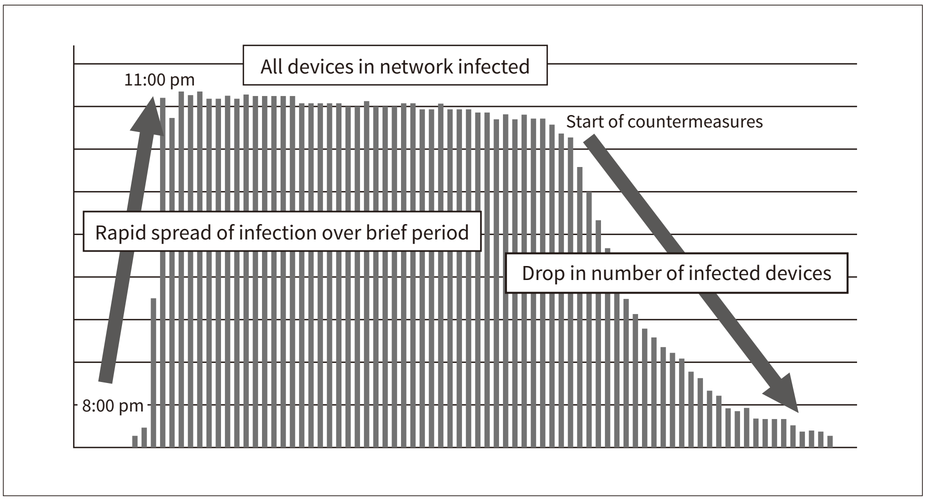
2. 1 Cyber-attack Overview

On May 12, 2017, a worm-type ransomware called WannaCry spread its infection from Europe to victims throughout the world. The virus exploited a Windows*1 vulnerability to spread itself to other

*1 Windows is a registered trademark of Microsoft Corporation in the United States and/or other countries.

Figure 1 — WannaCry Infection Rate

The use of a flat network configuration prioritizing convenience caused the infection to spread rapidly over a brief period until all devices with unprotected vulnerabilities were infected.



vulnerable Windows systems over networks. The virus encrypted the files of the infected systems and displayed a ransom letter demanding money in exchange for the decryption key. The virus infected Hitachi too, starting with inspection equipment at a local European affiliate, the infection spread to in-house network servers and other devices one after another causing global damage.

2. 2 Extent of Impact

The extent of the damage was widespread, ranging from devices connected to in-house networks (business system servers, PCs for office automation, and other devices managed by information system departments), to systems used by plants for applications such as manufacturing, production, control, warehouse operations, and facility access control systems.

Figure 1 shows the number of WannaCry-spreading packets discarded by external firewalls starting on May 12. The infection started around 8 pm and reached a near-saturation point 3 hours later. The spread of infection stopped once it had reached every device with an unprotected vulnerability. Antivirus software subsequently reduced the number of packets through quarantine and vulnerability countermeasures.

3. Lessons Learned from the WannaCry Cyber-attack

Four lessons have been learned from the WannaCry cyber-attack. The first lesson relates to network configurations. When in-house networks assume endpoint-based virus countermeasures and use wide-area Ethernet[*2] to eliminate segmentation, worm-type virus attacks can spread instantly if an endpoint becomes infected. Network connections made without knowing the state of an endpoint's security were also responsible for spreading the virus during the WannaCry attack. Implementing heightened security features and network monitoring functions designed to enable recovery are key requirements for improving these issues.

The second lesson comes from discovering inadequately implemented security measures in server systems that require round-the-clock operation to support worldwide use. Some systems were damaged because they could not receive patches for discovered vulnerabilities right away as they were not permitted down time. Installing patches was not considered necessary. Reforming this attitude to raise awareness about the vital necessity of patches will be a key issue for the entire Company to work on.

The third lesson is the difficulty of implementing security measures for Internet of things (IoT) devices. The WannaCry attack originated in an IoT device used for inspections, but many IoT devices are not designed for patch installation (despite being embedded Windows devices), and IoT device users often have little awareness of the need for system updates. These sorts of facts are keen reminders of how difficult it will be to implement responses for IoT devices in the future. Unlike office automation equipment, IoT

[*2] Ethernet is a registered trademark of Fuji Xerox Co., Ltd.

Figure 2 — Governance Work

Hitachi's work on governance in response to the WannaCry cyber-attack consists of Groupwide policies for creating more robust information security. These policies focus on six elements.

1. BCP designs for cyber-attack preparedness
   Designs incorporating cybersecurity and global responses as well as disasters
2. Countermeasures for IT informed by business risk analysis
   Countermeasures for IT incorporating information asset weightings
3. Patch management with mandatory security patch installation
   Creation of a structure enabling management of all site devices along with IoT devices and physical security
4. Creating a consolidated management structure by reviewing management scope/authority areas of IT managers
5. Global governance of security management
   Structure re-examination encompassing regions of every country
6. Creating IoT security guidelines

➡ Creating cross-Group specialized information security divisions

BCP: business continuity plan IoT: Internet of Things

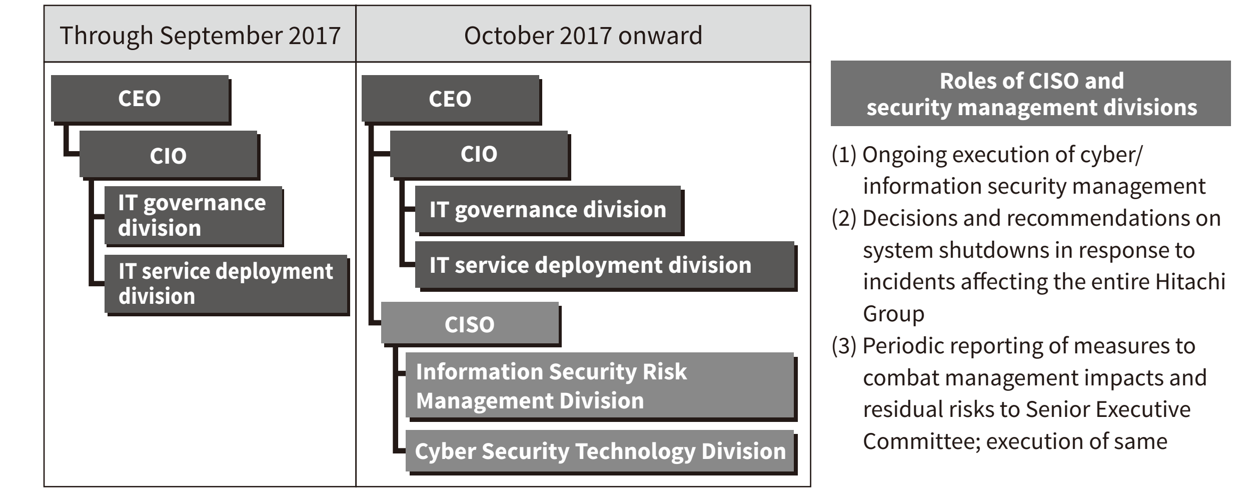
devices designs need to anticipate patch installation becoming impossible, and rely on the network for defense measures.

The fourth lesson comes from a renewed awareness of the stark difference between IT-business continuity plans (BCPs) for disaster preparedness and IT-BCPs for cybersecurity. Preparedness measures for disasters such as earthquakes called for continuous synchronization of data across geographically redundant locations with the aim of enabling rapid business recovery. But since encrypted files were also synchronized, redundant data that was destroyed had to be restored from the previous day's file, requiring a prolonged restoration process as a result. Preparedness measures for ransomware require rethinking the approach used by the data backup processes needed for business recovery. Like BCPs for disasters, BCPs for cyber-attacks need to specify actions that focus first and foremost on preserving lives and restoring business. Incident responders must always anticipate worst-case scenarios and be ready for the possibility of incidents leading to major damage.

To put these lessons learned into practice, it is important to create written procedures tailored to attack scenarios, provide training, and improve site capabilities. Work is being done on applying these lessons learned to increase the resilience of organizations, with the focus being put on the six governance elements shown in **Figure 2**. Hitachi has established cross-Group specialized information security divisions to implement these elements and create a more robust security governance structure.

Figure 3 — CISO Structure and Roles

Reflecting its efforts to approach cybersecurity as a management issue, Hitachi has created a new CISO position and two new specialized divisions tasked with managing security throughout the entire Hitachi Group.


Through September 2017
October 2017 onward
CEO
CIO
IT governance division
IT service deployment division
CEO
CIO
IT governance division
IT service deployment division
CISO
Information Security Risk Management Division
Cyber Security Technology Division
Roles of CISO and security management divisions

(1) Ongoing execution of cyber/information security management
(2) Decisions and recommendations on system shutdowns in response to incidents affecting the entire Hitachi Group
(3) Periodic reporting of measures to combat management impacts and residual risks to Senior Executive Committee; execution of same

CEO: Chief Executive Officer CIO: Chief Information Officer CISO: Chief Information Security Officer

4. Creating a More Robust Security Governance Structure

Hitachi has made information security governance its top management priority in response to the rise of the IoT and heightened cybersecurity threats. To enable consolidated information security governance for the entire Hitachi Group, it created the new position of Chief Information Security Officer (CISO) in October 2017. The CISO handles the areas of information security responsibility previously handled by its Chief Information Officer (CIO). Two specialized divisions reporting to the CISO were also created for managing the security of the entire Hitachi Group (see **Figure 3**).

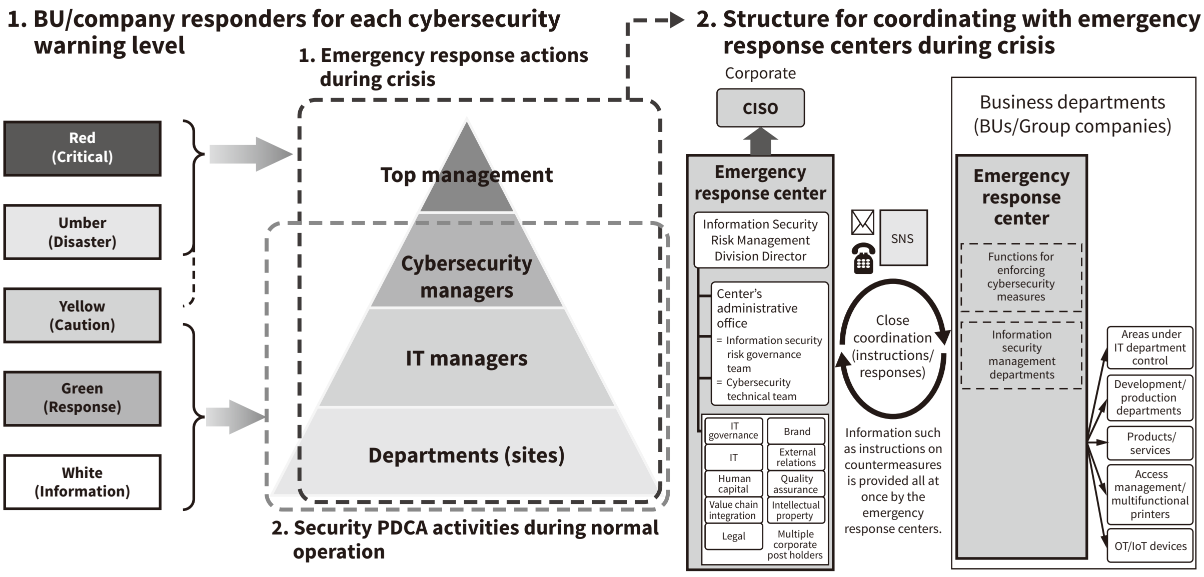
Security functions were previously handled by the CIO, but this reorganization has created a Groupwide governance structure that puts security first by creating a distinct separation between security governance functions and the IT governance areas they used to be part of.

The new specialized divisions reporting to the CISO manage cybersecurity and information security on an ongoing basis and make decisions and recommendations on system shutdowns in response to incidents that affect the entire Hitachi Group. These divisions also execute countermeasures to combat the management impacts and residual risks that they periodically report to the Senior Executive Committee.

Within the new specialized divisions, security operations centers (SOCs) also provide 24×7, 365-days-a-year monitoring and the Hitachi Incident Response Team (HIRT) provides more robust incident responses. As shown in **Figure 4**, Hitachi has created a structure that can set companywide cyber-attack

Figure 4 — Cybersecurity Warnings and Emergency Response Center Communication Structure

Threat information is gathered from around the world, and each threat's urgency and impact extent are evaluated to issue cybersecurity warnings with assigned threat levels. Hitachi has created a structure that brings the entire Group together to work on coordination/responses in times of crisis.


1. BU/company responders for each cybersecurity warning level
Red (Critical)
Umber (Disaster)
Yellow (Caution)
Green (Response)
White (Information)
1. Emergency response actions during crisis
Top management
Cybersecurity managers
IT managers
Departments (sites)
2. Security PDCA activities during normal operation
2. Structure for coordinating with emergency response centers during crisis
Corporate
CISO
Emergency response center
Information Security Risk Management Division Director
Center's administrative office
= Information security risk governance team
= Cybersecurity technical team
IT governance
Brand
IT
External relations
Human capital
Quality assurance
Value chain integration
Intellectual property
Legal
Multiple corporate post holders
SNS
Close coordination (instructions/ responses)
Information such as instructions on countermeasures is provided all at once by the emergency response centers.
Business departments (BUs/Group companies)
Emergency response center
Functions for enforcing cybersecurity measures
Information security management departments
Areas under IT department control
Development/ production departments
Products/ services
Access management/ multifunctional printers
OT/IoT devices

	Action category	Action description
1	Emergency response actions during crisis	• Creating emergency response centers • Deploying cyber BCP plans (system preservation activities) • Issuing instructions to employees on countermeasures
2	Security PDCA activities during normal operation	• Executing security management PDCA cycle for products and services, development and production, and OT/IoT devices • Vulnerability countermeasures • Resilience planning (working on resilience policies, assessing residual risks, assessing business impacts, then reporting to top management) • Security improvement/education activities for employees

For crises requiring deployment of cyber BCPs, a corporate-wide emergency response center is set up. It coordinates with functions for enforcing BU/Group company cybersecurity measures and works on responses.
The corporate departments implement the responses set by the emergency response center.

PDCA: plan-do-check-act BU: business unit OT: operational technology SNS: social networking service warnings, carry out consistent plan-do-check-act (PDCA) cycle activities during times of normal operation, and act to implement emergency countermeasures during a crisis. At times of crisis that require deployment of cyber BCPs, a corporate-wide emergency response center is set up to implement responses in coordination with the cybersecurity departments of the business units (BUs) and Group companies. The corporate departments team up with the new specialized divisions to function as an emergency response center that implements the predetermined responses (including responses to outside organizations such as law enforcement, the media, and government agencies).

5. Making the Technical Aspects of Corporate Preparedness and Resilience More Robust

In parallel with a more robust governance system, Hitachi Group is working to increase the robustness of monitoring and incident response in terms of technical aspects to ensure attacks are detected early and handled rapidly. With the need to prepare for attacks from WannaCry subspecies in the wake of the original WannaCry attack, Hitachi has responded by planning a phased approach to creating more robust security. This approach is designed to enable progressive and steady advances.

5. 1 Resilience-building Phase 1

The work done during resilience-building phase 1 focused on policies with immediate effects, using existing operations as a starting point to enable earlier detection and faster decisions and responses.

In-house networks and business systems were previously operated and managed autonomously by the departments in charge of them. Monitoring organizations were unable to adequately understand their configuration and details as a result, and neglected to monitor some of the logs gathered for operational purposes. But when monitoring in-house networks with flat configurations, every additional monitoring point helps enable early detection. Therefore, Hitachi has taken an inventory of the devices and systems managed by each department to identify and locate every component. It has enabled earlier detection by finding all the obtainable logs and expanding the scope of monitored logs to include items that are useful for threat detection.

The rapid pace at which threats have been changing recently has created the need for monitoring operations to respond flexibly to these changes. The operation manuals created by monitoring organizations were previously patchy documents with detailed information only for common procedures used for checks and countermeasures. Their content was abstract and written for knowledgeable responders. Realizing that WannaCry-like emergencies could occur when no knowledgeable responder was available and result in lengthy response times and spreading damage, organizations rewrote their emergency response manuals to enable rapid and confident decisions and responses by responders assumed to have limited knowledge.

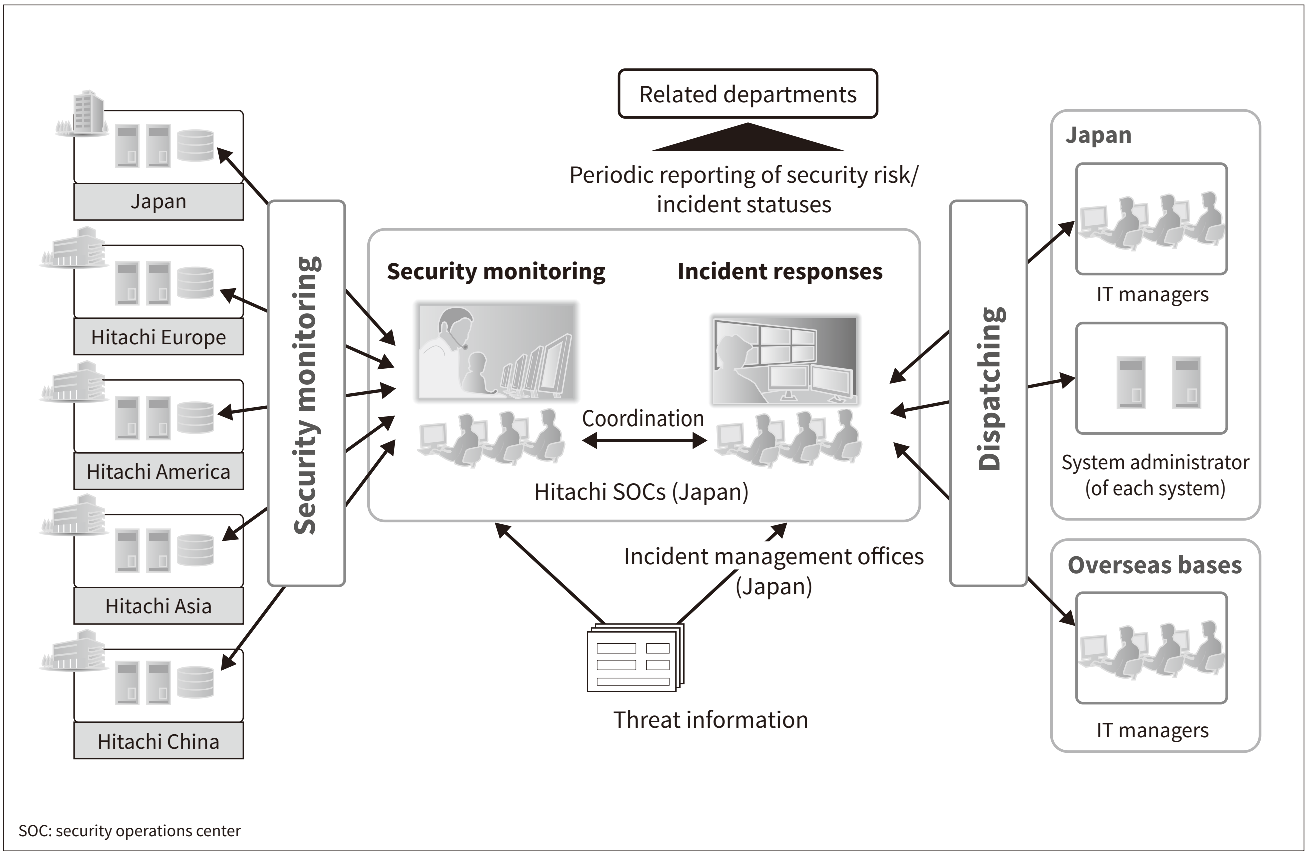
Monitoring previously focused on targeted attacks in Japan, so responses were handled separately for domestic and overseas organizations. But the WannaCry attack was an incident that originated overseas and caused major damage in Japan. The severity of this experience proved that responses designed for attacks in Japan also need to anticipate attacks from overseas, so a structure was put in place to enable 24×7, 365-days-a-year incident reporting and response that can respond rapidly to highly dangerous incidents.

5. 2 Resilience-building Phase 2

Resilience-building phase 2 involved creating more robust security monitoring. Hitachi started by looking into expanding its monitoring platforms to make monitoring more robust. It examined the in-house monitoring platform expansion work done independently in the past, but it did not address the need to quickly increase the robustness of both domestic and global monitoring in a cost-effectiveness manner. So, using the managed security services (MSS) of several companies as a screening pool, it selected the MSS of Hitachi Systems, Ltd. Hitachi Systems' MSS can provide security monitoring and also incident responses (IRs) when incidents occur, both in the form of services.

Figure 5 — Creating More Robust Security Monitoring Worldwide

The Hitachi Group's security monitoring is being made more robust throughout the world by monitoring in-house domestic/overseas networks 24×7, 365-days-a-year and responding to incidents.



SOC: security operations center

The next step was to achieve more robust global monitoring by setting the system and network points to be monitored, and making the adjustments needed to enable coordination/monitoring of system and network device logs from around the world (see **Figure 5**). In addition to Japan and Hitachi Europe, Hitachi America, Hitachi Asia, and Hitachi China were set as monitoring points.

Monitoring is done by using the MSS monitoring platform to aggregate and perform correlation analysis on the system and network device logs of the monitored bases. However, Europe's General Data Protection Regulation (GDPR) prohibits the transfer of data containing personal information outside of the European Union so, for each base subject to similar laws or regulations, correlation analysis is performed only within the base. The use of the MSS monitoring platform to gather, analyze, and monitor logs has enabled earlier detection of cyber-attacks on the Hitachi Group and faster IR-based countermeasures and recovery.

Hitachi will work on a number of issues in the future. The SOCs currently provide 24×7, 365-days-a-year monitoring, but the operation work done by IT managers and IT administrators varies from base to base, and some bases do not support 24×7, 365-days-a-year monitoring. Since time zone differences can create lags or discrepancies, Hitachi will work to minimize cyber-attack damage, ensuring rapid execution of everything from initial responses when incidents occur, to defensive countermeasures.

6. Conclusions

Hitachi Group is learning from the lessons of the WannaCry cyber-attack it suffered by promoting more robust corporate preparedness and resilience. This work is now centered on the IT systems used for office automation. In the future, the scope of these efforts will be expanded to include IoT/operational technology (OT) systems and all other devices directly or indirectly connected to networks. The Group will continue to expand its security risk management activities encompassing all domestic and overseas equipment, including in-house equipment for product/service business areas and applications such as development and production.

Authors

Toru Matsukawa
Cyber Risk Management Department, Information Security Risk Management Division, Hitachi, Ltd. *Current work and research:* Information security risk management of Hitachi Group Companies.

Hiroshi Nishihama
Cyber Risk Management Department, Information Security Risk Management Division, Hitachi, Ltd. *Current work and research:* Information security risk management of Hitachi Group Companies.

Daisuke Shibata
Hitachi Security Operation Center, Cyber Security Technology Operations, Security Businesses Division, Service Platform Business Division Group, Hitachi, Ltd. *Current work and research:* Security monitoring of Hitachi Group Companies and incident response.

Akihiko Kawasaki
Hitachi Security Operation Center, Cyber Security Technology Operations, Security Businesses Division, Service Platform Business Division Group, Hitachi, Ltd. *Current work and research:* Security monitoring of Hitachi Group Companies and incident response.

Hajime Nodaguchi
Hitachi Security Operation Center, Cyber Security Technology Operations, Security Businesses Division, Service Platform Business Division Group, Hitachi, Ltd. *Current work and research:* Security monitoring of Hitachi Group Companies and incident response.