Hitachi's Approach to the Skills Development Challenges Facing Social Infrastructure Security

Training for security human resources has become an area of concern in Japan and around the world in the wake of a recent rise in cyber-attacks and other security threats, combined with a shortage of security human resources who can respond to them effectively. As an infrastructure provider in the IoT era, Hitachi also has an urgent need for development programs designed to educate engineers who can provide secure products and services, and operate business systems. This article provides an overview of the challenges facing security human resources development. It looks at the Hitachi Group's security human resources initiatives made possible by collaborations among industry, academia, and government, and proposes providing security human resources development in collaboration with clients.

Yoshitaka Tsushima
Tatsuya Fujiyama
Manabu Natsume
Motoshi Sakakura
Ryo Nakano

1. Introduction

1. 1 Cybersecurity Trends

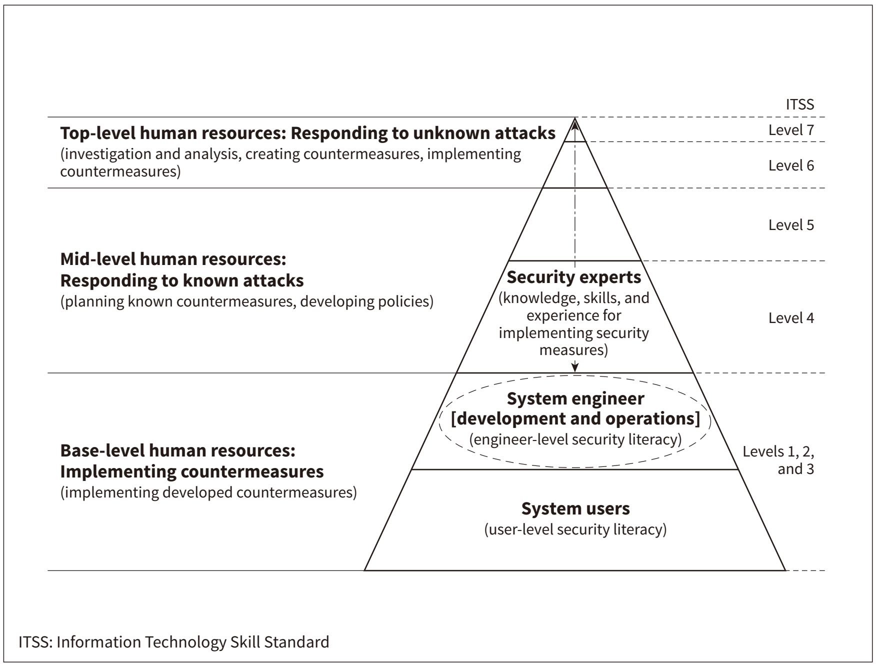
While cyber-attacks used to be mainly pranks carried out for fun, today's attacks are being mounted for clear monetary, espionage, or military objectives. Cyber-attack vectors have also become more sophisticated. Some attacks are large-scale indiscriminate types, while others are persistent attacks on specific targets.

Some recent cyber-attacks have used ransomware to destroy data on computers. In May 2017, the WannaCry attack damaged some victims in Japan, while in June the NotPetya attack wreaked havoc on mainly Eastern European victims. Damage from such attacks is not limited to IT systems. The control system operational technology (OT) of victims such as manufacturers and power providers has also been affected, creating major impacts on business.

Internet of Things (IoT) devices are coming into widespread use, and the security measures used for them are not always adequate. The damage caused by

Figure 1 — Security Human Resources Pyramid

Different levels of security knowledge need to be acquired for different roles.


ITSS
Level 7
Level 6
Level 5
Level 4
Levels 1, 2, and 3
Top-level human resources: Responding to unknown attacks
(investigation and analysis, creating countermeasures, implementing countermeasures)
Mid-level human resources: Responding to known attacks
(planning known countermeasures, developing policies)
Base-level human resources: Implementing countermeasures
(implementing developed countermeasures)
Security experts
(knowledge, skills, and experience for implementing security measures)
System engineer [development and operations]
(engineer-level security literacy)
System users
(user-level security literacy)

ITSS: Information Technology Skill Standard

the Mirai malware and its subspecies was caused by exploiting several IoT devices by using them as bots (attack springboards) to perform large-scale distributed denial of service (DDoS) attacks.

A very large number of attacks exploit vulnerabilities, and several attacks have been mounted on vulnerabilities in systems used by web servers such as WordPress*1 and Apache Struts 2*2. Vulnerabilities are not limited to software. Hardware vulnerabilities have also been announced and widely reported, such as the Meltdown and Spectre vulnerabilities in central processing units (CPUs) with speculative execution. Vulnerabilities are discovered over time, and measures for them need to be provided on a continuous basis.

IT is indispensable for carrying out business operations in a wide range of business areas today, and it is being used increasingly in new areas such as the IoT. But, because security design and management in these areas are not always handled properly, the risk of cyber-attacks continues to grow.

1. 2 Shortage of Security Human Resources

Despite the continued rise in the risk of cyber-attacks, human resources who can handle cybersecurity measures are reportedly in short supply.

A survey[(1)] released by Japan's Ministry of Economy, Trade and Industry (METI) in June 2016 has reported a growing shortage of security human resources. The shortfall grew from 82,000 in 2014 to 132,000 in 2016, and is predicted to rise to 193,000 in 2020.

The security human resources shortage can be included among the threats facing organizations today. In fact, a report compiled by the Information-technology Promotion Agency, Japan (IPA) entitled 10 Major Security Threats 2018 ranks the security human resources shortage at No. 5 among 10 major threats facing organizations[(2)].

The security human resources shortage is not limited to Japan. The same problem is found overseas. Developing security human resources is an urgent task needed for responding to recent cybersecurity trends.

1. 3 Security Human Resources Pyramid

Creating a separate team of security experts is not enough to ensure security in an organization. Each member of the organization needs to play a role in the aspects of security that affect his/her job duties (see **Figure 1**). Therefore, mindset is just as important as skill set.

System users must have the knowledge and motivation needed to use the system securely. System engineers must be able to implement indicated security

*1 WordPress is registered trademark of the WordPress Foundation.
*2 Apache Struts is a trademark of The Apache Software Foundation.

measures accurately, and should ideally be able to pursue security measures on their own initiative in response to system-specific risks. Security experts must be able to explain why security measures are needed, and be able to pitch and implement them.

1. 4 Security Human Resources Development Challenges and Approaches to Solutions

Since different jobs need different security capabilities, human resources development programs must be created in a way that provides the proper training and study method for each level and job.

Creating secure systems requires security human resources with a wide range of expertise in security, IT skills, and other areas. It is difficult to become familiar with the wide range of areas encompassed by security, so security human resources need to acquire overall security knowledge before increasing proficiency in particular areas of expertise.

While the points above should be considered when developing human resources, the ability of individual companies to respond will be limited due to the wide range of areas covered by security and their rapidly changing nature. Tackling common initiatives through cross-industry alliances and community-wide responses is therefore important.

2. Security Human Resources Development Programs Created Collaboratively by Industry, Academia, and Government

Ensuring a stable supply of security human resources requires human resources development policies for various fields, along with community-wide initiatives. This section looks at human resources development programs created collaboratively by industry, academia, and government.

2. 1 Development of Core Human Resources: Industrial Cyber Security Center of Excellence

Threats have arisen to the security of critical infrastructure and industrial platforms. To create more robust cybersecurity measures for these areas, an organization called the Industrial Cyber Security Center of Excellence has been created within IPA. Headed by Hiroaki Nakanishi, Chairman of the Board, Hitachi, Ltd., the Center works mainly on (1) human resources development projects, (2) verifying actual control system security and reliability, and (3) studying and analyzing threat information. Its work on the human resources development projects is described here.

Security measures for social infrastructure and industrial platforms call for skills in both information (IT) systems and control (OT) systems. Ensuring proper countermeasures requires human resources who are aware of the risks to their company's systems and who can make decisions on security measures. The Center has two programs designed to develop these human resources, the Core Human Resources Development Program and the short-term program.

The Core Human Resources Development Program is a long-term (one-year) program designed to produce bridging human resources who will serve as a link between management and field workforce in the future. The program teaches a comprehensive set of skills in the areas of technology, management, and business. The technology skills are taught through coursework, written drills, basic hands-on drills, and practical drills using simulated systems. The curriculum covers security theory, attack/intrusion vectors and incident responses. The management and business skills training prepares trainees for their role as bridging human resources by equipping them with a wide range of perspectives ranging from sites to management. Training is also provided in collaboration with overseas facilities to ensure that the curriculum provides both skills and top-level personal relationships across country and industry borders. Five trainees from Hitachi are taking part in this program.

The short-term program provides training over a few days based on either of two curricula. One covers knowledge common to multiple industries required by management-level security human resources such as Chief Information Security Officers (CISOs). The other covers industry-specific knowledge required by CISO assistants. The program aims to inform participants about domestic and overseas trends, and the issues facing their company. It also aims to foster personal relationships with other companies and security evangelists.

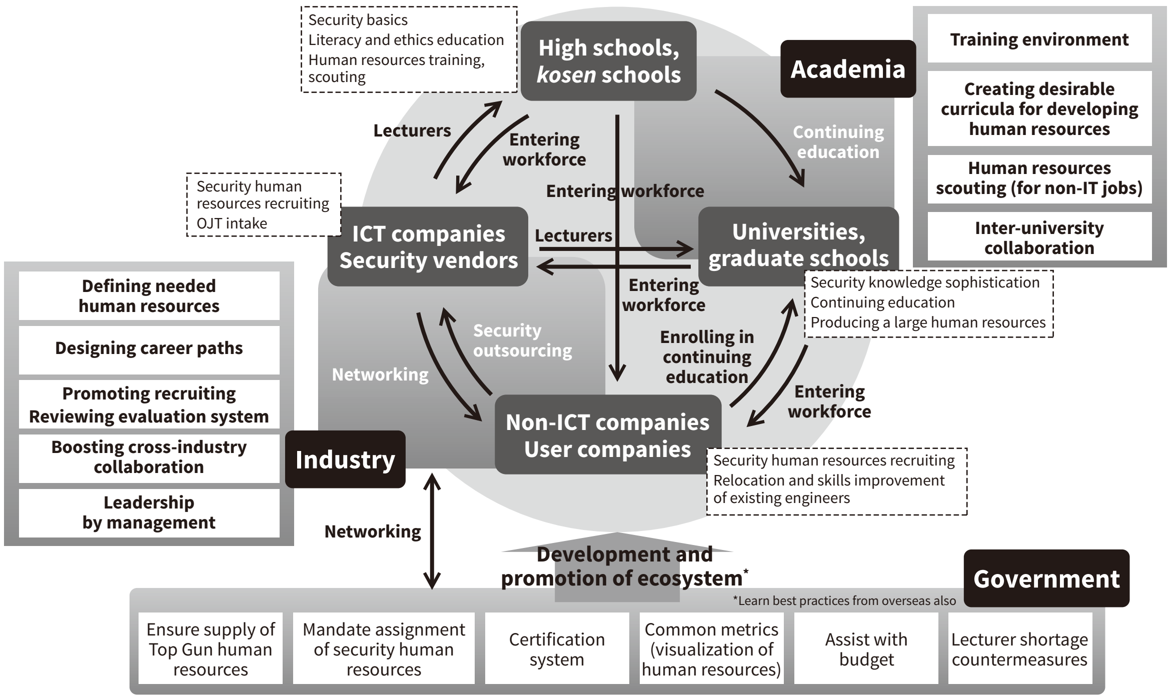


Figure 2 — Ecosystem for Developing/Maintaining Human Resources

Security talent development needs to be tailored to each job type. The Cyber Risk Intelligence Center-Cross Sectors Forum (CRIC CSF) is working on creating an ecosystem to develop/maintain human resources that will enable training and maintenance of cybersecurity talent in the future (an ongoing cycle of human resources training, recruiting, and utilization).

Security basics
Literacy and ethics education
Human resources training, scouting
High schools, *kosen* schools
Academia
Training environment
Creating desirable curricula for developing human resources
Human resources scouting (for non-IT jobs)
Inter-university collaboration
Lecturers
Entering workforce
Continuing education
Security human resources recruiting
OJT intake
Entering workforce
ICT companies Security vendors
Lecturers
Universities, graduate schools
Defining needed human resources
Designing career paths
Promoting recruiting
Reviewing evaluation system
Boosting cross-industry collaboration
Leadership by management
Entering workforce
Security knowledge sophistication
Continuing education
Producing a large human resources
Security outsourcing
Networking
Enrolling in continuing education
Entering workforce
Non-ICT companies User companies
Industry
Security human resources recruiting
Relocation and skills improvement of existing engineers
Networking
Development and promotion of ecosystem*
Government
*Learn best practices from overseas also
Ensure supply of Top Gun human resources
Mandate assignment of security human resources
Certification system
Common metrics (visualization of human resources)
Assist with budget
Lecturer shortage countermeasures

OJT: on-the-job training ICT: information and communication technology

2. 2

Creating a Human Resources Development Framework: Cyber Risk Intelligence Center-Cross Sectors Forum (CRIC CSF)

Ensuring cybersecurity is an important issue for maintaining trust and business continuity. It is relevant for all companies, and not just for those that work with critical infrastructure.

The Japan Business Federation (Keidanren) has created an organization known as the Cyber Security Working Group that has released a set of recommendations entitled the Proposal for Reinforcing Cybersecurity Measures. The recommendations include calls for initiatives such as human resources development, and deal with cybersecurity as a management issue affecting industry. The Cyber Risk Intelligence Center-Cross Sectors Forum (CRIC CSF) has been created in response, with Nippon Telegraph and Telephone, NEC Corporation, and Hitachi, Ltd. serving as the three co-founders and administrative offices.

CRIC CSF has brought together user companies mainly working with critical infrastructure to study issues such as industry approaches to security human resources development (training and recruiting).

Drawing on the findings of this study, CRIC CSF has created a framework for defining and visualizing the characteristics of human resources needed by industry. It takes the form of an ecosystem for developing/maintaining human resources that presupposes partnerships among industry, academia, and the government (see **Figure 2**). This framework has been released as an activity report. The study findings have been approved by Keidanren and referenced in recommendations released by Keidanren entitled A Call for Reinforcement of Cybersecurity to Realize Society 5.0[(3)].

CRIC CSF will continue holding discussions to determine how to bring about this ecosystem, while working on applying the activity results to industry. The ecosystem will be implemented through concrete human resources development policies tailored to the conditions currently facing companies. It is expected to help improve the overall standard of cybersecurity.

2. 3 Security Education for Students: Development of *Kosen* Human Resources

The human resources produced by Japan's *kosen* (technical college)*3 school system have recently been receiving attention for the solid specialist knowledge and technical skills they possess. The National Institute of Technology (NIT) operates 51 *kosen* schools throughout Japan. To help tackle the security human resources shortage, NIT has started an information security human resources development program called the Human Resource Education Project on Information (K-SEC) that accepts students as young as 15. Hitachi has partnered on the project, helping to develop teaching materials and setting the targets to attain for human resources from *kosen* schools.

One of the specific activity areas Hitachi is engaged in is providing classes directly at a *kosen* school. Drawing on knowledge gained from Hitachi's security education, it has developed new student-oriented teaching materials for use in seven security courses selected through discussion with NIT. Classes are being held at Ichinoseki College, one of the K-SEC base schools for academic year 2017. **Table 1** lists the course names for the classes that have been given at the school. Students have praised the classes as being "difficult, but worthwhile."

Another activity area is the internship program for *kosen* students. The program has been provided as part of the work on developing security human resources. Its aim is to produce educational materials covering countermeasures for attacks targeting vulnerabilities such as web applications for system engineers. Student participants have said the program gave them a visceral sense of just how frightening cyber-attacks are, along with a solid understanding of the importance of security. They have also credited the program's hands-on experience at security sites for giving them a better understanding of the capabilities demanded of human resources, making them more motivated to study than they were before joining the program.

These activities are laying the groundwork needed to produce security human resources. They should eventually help eliminate the security human resources shortage by giving students education that starts at a young age and covers security topics ranging from the basics to actual practices.

Table 1 — Courses at *Kosen* Schools

Hitachi has held the following classes at the Ichinoseki College *kosen* school.

No.	Course name
1	Information Security Risk Basics
2	Cryptography and its Applications
3	Hardware Security
4	Network Security
5	Software Security
6	Information Security and the Legal System
7	Information Security Management

3. Hitachi's Security Human Resources Development

To provide examples of industry security human resources development, this section looks at Hitachi's security human resources visualization (assessment) and development system.

3. 1 Human Resources Evaluations/Scouting: ITSS Level Assessments and CIP System

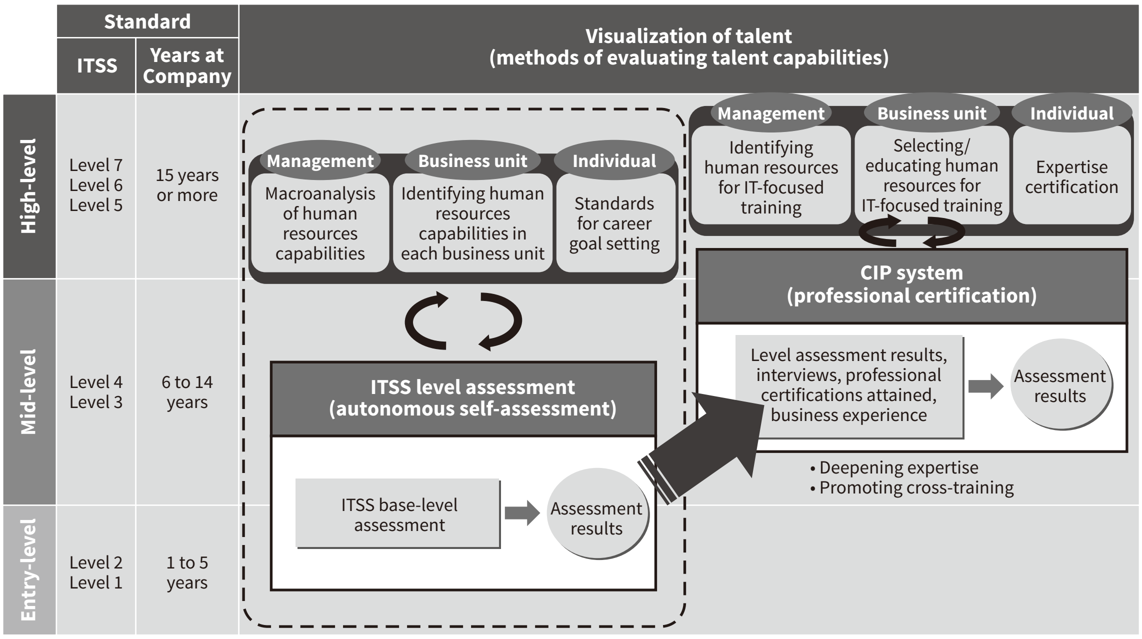
Hitachi has two methods that are used together to determine the competency of human resources: Information Technology Skill Standard (ITSS) level assessments and the Hitachi Certified IT Professional (CIP) system (see **Figure 3**).

ITSS is a METI-created indicator used to describe and systematize the practical work capabilities needed when providing IT-related services. It is a skill assessment indicator created from common IT market metrics, and defines achievement, skill, and proficiency for various areas of expertise on a 7-level scale(4). To determine ITSS levels, Hitachi administers ITSS level assessments that allow human resources to self-assess their own competency levels for various skill areas. Their responses are checked and approved by their supervisor. ITSS defines multiple job types such

*3 College of technology that offers five-year engineering education for student starting from 15 years old. In 1961, *kosen* was established in response to a strong demand from the industrial sector to foster engineers to support the high economic growth of Japan with their knowledge of science technology.

Figure 3 — Relationship Between ITSS Level Assessments and CIP System

ITSS level assessments are mainly done by self-assessment, while the CIP system uses third-party assessments covering skill elements such as professional certifications and career elements such as business experience.


Standard
ITSS
Years at Company
Visualization of talent
(methods of evaluating talent capabilities)
High-level
Level 7
Level 6
Level 5
15 years or more
Mid-level
Level 4
Level 3
6 to 14 years
Entry-level
Level 2
Level 1
1 to 5 years
Management
Business unit
Individual
Macroanalysis of human resources capabilities
Identifying human resources capabilities in each business unit
Standards for career goal setting
ITSS level assessment
(autonomous self-assessment)
ITSS base-level assessment
Assessment results
Management
Business unit
Individual
Identifying human resources for IT-focused training
Selecting/ educating human resources for IT-focused training
Expertise certification
CIP system
(professional certification)
Level assessment results, interviews, professional certifications attained, business experience
Assessment results
• Deepening expertise
• Promoting cross-training

CIP: Hitachi Certified IT Professional

as IT Specialist (Security). Hitachi uses the assessment results to identify IT engineer skill levels and to create the skill training plans needed for job assignment and execution.

The CIP system is a Hitachi in-house certification system used to certify high-level IT professionals (with ITSS level 4 or higher skills). Although CIP is an in-house system, it has been officially recognized as a corporate system equivalent to the Certified IT professional program provided by the Information Processing Society of Japan[5], making CIP certification equivalent to an official professional certification.

Becoming CIP-certified involves more than just skills assessment based on training courses and official professional certifications. The candidate's career is also assessed in areas such as work experience and professional contribution to the world. To be recognized as a high-level engineer, the candidate is required to help with the growth of others such as by training or educating junior engineers. A CIP certification is valid for 3 years, and the requirements for recertification include continuing professional education, internal/external contributions, and work experience. Like ITSS, the CIP system also defines multiple job types. The job type defined for security-related work is Hitachi-certified Information Security Specialist.

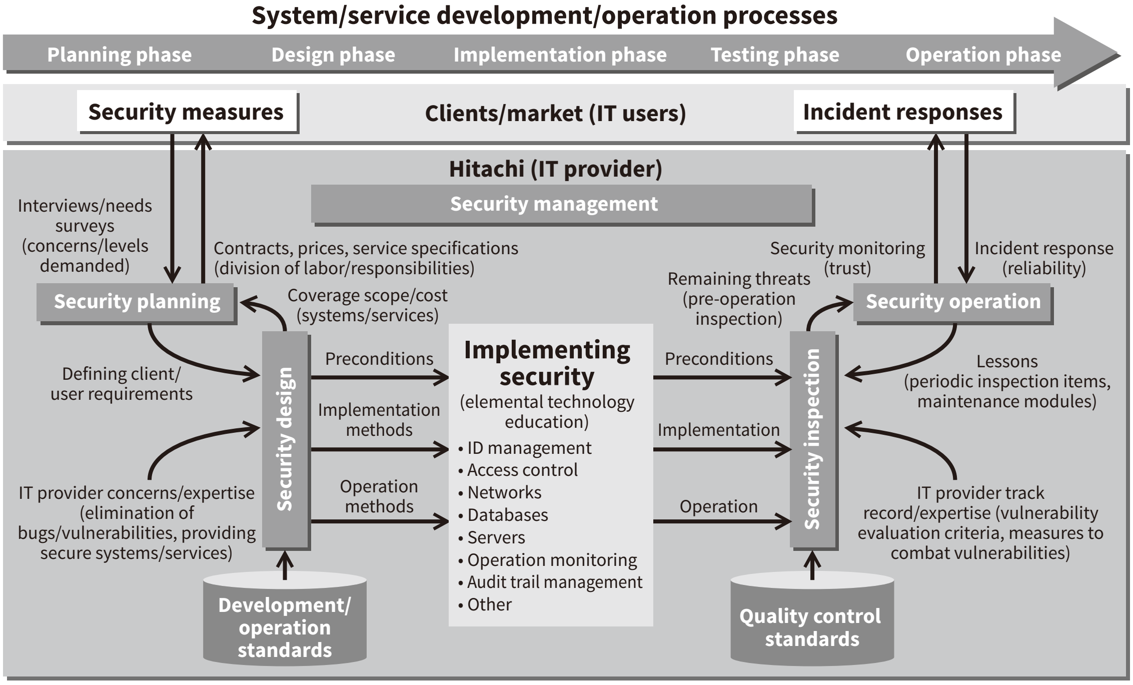
Hitachi uses ITSS to assess the skill levels of entry-level and mid-level human resources, and the CIP system to assess higher-level human resources. These methods are used to visualize, scout, and develop security human resources and other IT human resources in-house.

3. 2
Planning and Operation of In-house Security Training

Hitachi provides training on elemental security technologies and training corresponding to development and operation processes (see **Figure 4**). Since trends in security change rapidly, keeping up with these changes is a key requirement for ensuring that technical training remains relevant. Hitachi has therefore created a committee-based organization that plans and administers new and revised security technology training curricula, while reviewing the course system periodically.

The committee has been created by gathering experts from related departments in areas such as system engineering, development, control

Figure 4 — Development and Operation Processes and Security Technology Training
Hitachi provides security technology training corresponding to development and operation processes.


System/service development/operation processes
Planning phase
Design phase
Implementation phase
Testing phase
Operation phase
Security measures
Clients/market (IT users)
Incident responses
Hitachi (IT provider)
Security management
Interviews/needs surveys (concerns/levels demanded)
Contracts, prices, service specifications (division of labor/responsibilities)
Security monitoring (trust)
Incident response (reliability)
Remaining threats (pre-operation inspection)
Security planning
Coverage scope/cost (systems/services)
Security operation
Defining client/user requirements
Security design
Preconditions
Implementation methods
Operation methods
Implementing security
(elemental technology education)
• ID management
• Access control
• Networks
• Databases
• Servers
• Operation monitoring
• Audit trail management
• Other
Preconditions
Implementation
Operation
Security inspection
Lessons (periodic inspection items, maintenance modules)
IT provider concerns/expertise (elimination of bugs/vulnerabilities, providing secure systems/services)
IT provider track record/expertise (vulnerability evaluation criteria, measures to combat vulnerabilities)
Development/operation standards
Quality control standards

systems, security technology, and quality assurance. Information linked to security trends and required by sites is incorporated into training.

3. 3 Instructor Development and Continuing Professional Education: Practical Training, Community

Ensuring proper countermeasures in the rare event of a security incident requires training for the related departments, but training courses that teach security technology are limited in number and have limited course sizes. Different departments also have different work characteristics, and optimum training should ideally accommodate these differences.

Hitachi therefore provides a practical training course designed to develop human resources who can instruct security. The course shows trainees how to select suitable accident case studies, analyze accident causes, and create scenarios. It develops instructors who can plan their own security incident response training, create teaching materials for it, and teach classes. The course is being used by a number of departments for incident response education.

Human resources that have attained a certain security skill level find it difficult to achieve further growth from training courses alone. Aware that it takes a professional to train a professional, Hitachi has therefore created a community site serving as a hub of security-related information and expertise. The site is open to in-house experts such as the Hitachi-certified Information Security Specialists previously mentioned. The platform for expert discussion and communication that the site provides should enable users to help each other grow.

4. Security Human Resources Development in Collaboration with Clients

In addition to promoting development of in-house security human resources, Hitachi also takes part in collaborative programs with a number of industries. Drawing on the knowledge gained from these programs, it is helping improve the security of outside systems by providing services assisting in developing human resources at client sites.

4. 1

Training for Critical Infrastructure Providers: Development of OT Human Resources

To prepare for today's higher security risks, the critical infrastructure and industrial platforms behind control system (OT) applications require more robust cybersecurity measures, just as IT applications do. And, while technology-based measures designed to monitor, detect, prevent, and respond to attacks are important requirements for combating risks, building up organizations, and developing security human resources who can handle attacks are equally important.

Human resources who handle security measures for OT applications need more than just security knowledge. They also need to be highly familiar with both the control (OT) systems and business (IT) systems being protected, and to understand and respond to the risks that are unique to these systems.

Hitachi created a facility for OT Integrated Cyber Security Training called Nx Security Training Arena (NxSeTA) in August 2017. It draws on the technology and expertise Hitachi has gained from developing and manufacturing infrastructure systems for many years. NxSeTA has created OT and IT system environments simulating actual client environments, and provides Integrated Cyber Security Training Services that enable practical training designed to strengthen human resources and organizations (see **Figure 5**). The training curriculum is composed of the following:

(1) Lectures

Lectures cover the systems used in the training, basic security knowledge for IT and OT systems, and the latest examples of security incidents.

(2) Workshops

Trainees examine system configuration diagrams to extract anticipated risks, study detection and defense methods for these risks, and learn risk analysis methods.

(3) Hands-on training

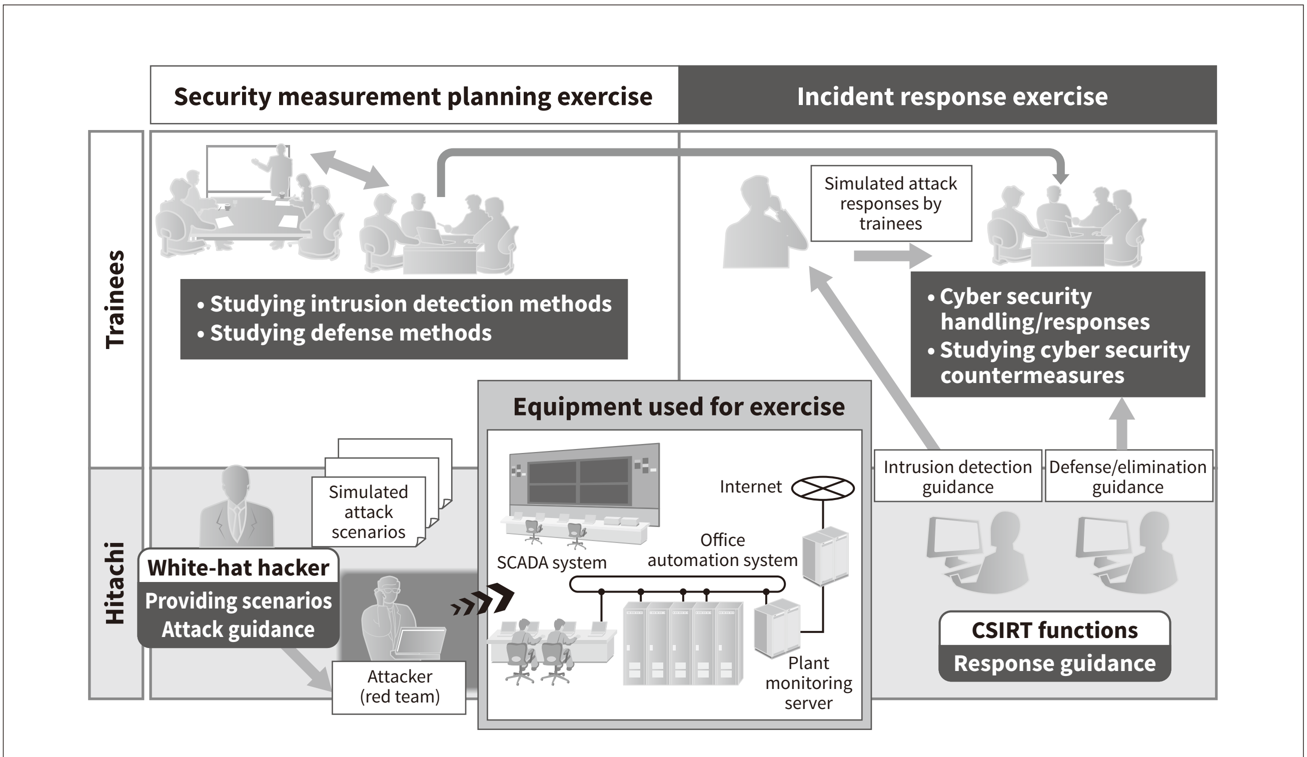
A practice network is used for practical lessons covering actual attack vectors and ways of defending against them.

(4) Roleplay exercises

Trainees play the roles of IT or OT system human resources and respond to attacks. Alternatively, they play the roles of corporate management or managers

Figure 5 — Use Scenario for NxSeTA

NxSeTA is a simulated cyber-attack exercise in which every trainee is assigned a role they play to experience how organization-wide countermeasures are implemented.


Security measurement planning exercise
Incident response exercise
Trainees
Hitachi
• Studying intrusion detection methods
• Studying defense methods
Simulated attack responses by trainees
• Cyber security handling/responses
• Studying cyber security countermeasures
Equipment used for exercise
Internet
Office automation system
SCADA system
Plant monitoring server
Simulated attack scenarios
White-hat hacker
Providing scenarios
Attack guidance
Attacker (red team)
Intrusion detection guidance
Defense/elimination guidance
CSIRT functions
Response guidance

CSIRT: Computer Security Incident Response Team SCADA: supervisory control and data acquisition to make business continuity decisions in response to reports from system administrators.

The curriculum aims to provide practical experience and training in how to implement countermeasures and make decisions when cyber-attacks occur, improving the response capabilities of the organization. The curriculum is customized to the client's needs.

Hitachi will continue working with clients to maintain and improve technology- and human-resources-based security measures for OT applications.

4. 2 Training for IT Users: Developing IT Human Resources

This section looks at the in-house security human resources development programs Hitachi has created that it is considering providing to outside clients.

Hitachi has trained a wide range of human resources using curricula designed to give them an overall understanding of cyber-attacks and to teach them how to respond to incidents. Trainees are required to learn some technical knowledge, but the emphasis is on mindset. Common security training tends to emphasize governance aspects (lists of items prohibited by rules), while Hitachi's training aims to teach trainees how to properly respond to incidents once they have understood the effect of each behavior.

(1) Learning the basics of responding to cyber-attacks

This e-learning unit is composed of a basic knowledge module and a hands-on learning module. The knowledge module teaches the basics of topics such as elementary cyber-attack methods and countermeasures, and reconfirms how experts will be contacted when incidents occur. The experience module uses video simulations to enable trainees to concretely visualize cyber-attacks. Case studies are presented that cover targeted cyber-attacks, ransomware infections, and two other incident types. They give trainees a visceral understanding of the type of behaviors that led to an incident in each case. Trainees also study the actions to take when incidents occur, working to become proficient in implementing the proper countermeasures.

(2) Cyber-attack countermeasure communication training

A group roleplay exercise done by playing a card game based on Trend Micro Inc.'s. Trainees are assigned roles in a simulated environment and play those roles. They must rely on fragmentary incident information to envision the incident that has occurred, determine its effects, study countermeasures, and coordinate with experts. The aims of the exercise are to increase the sensitivity of participants to cyber-attacks, enable them to share risks, and show them how to implement the proper countermeasures promptly when problems occur. These countermeasures involve reporting, communicating, and consulting with experts and related departments.

While using a generic simulated environment for communication drills and training is effective, it is more effective to simulate the environment that trainees know. When providing training for a wide range of trainees at a client site, the client human resources most familiar with the particulars of the organization should ideally serve as instructors and be assigned leadership roles. Hitachi is considering ways of providing outside clients with practical courses for instructor training to meet this need.

To improve the public's understanding of security and raise security standards, Hitachi will continue to work proactively with outside partners on common security education, using these efforts to help pursue collaborative creation activities with clients.

5. Conclusions

This article has looked at security human resources development programs provided collaboratively by industry, academia, and the government, along with Hitachi's in-house efforts in this area.

Hitachi will continue its ongoing efforts to keep systems secure and worry-free in today's ever-evolving digital era. In addition to ensuring the security of the products and services it provides, it will also keep improving and raising the standard of the security used to protect the systems that underpin every aspect of society.

References

1) Ministry of Economy, Trade and Industry, "Study Report of Recent Trends and Future Estimates Concerning IT Human Resources," (Jun. 2016), http://www.meti.go.jp/policy/it_policy/jinzai/27FY_report.html in Japanese.

2) Information-technology Promotion Agency, Japan (IPA), "10 Major Security Threats 2018,"https://www.ipa.go.jp/security/vuln/10threats2018.html in Japanese.

3) Cyber Risk Intelligence Center - Cross Sectors Forum, http://cyber-risk.or.jp/ in Japanese.

4) IPA, "What are the Skill Standards for IT Professionals?," https://www.ipa.go.jp/jinzai/itss/itss1.html in Japanese.

5) Information Processing Society of Japan, "Certified IT Professional Program," https://www.ipsj.or.jp/citp.html in Japanese.

Authors

Yoshitaka Tsushima
Security Human Resource Management Department, Cyber Security Technology Operations, Security Businesses Division, Service Platform Business Division Group, Services & Platforms Business Unit, Hitachi, Ltd. *Current work and research*: Development of cybersecurity human resources. *Certifications:* Certified Information Systems Auditor (CISA), Certified Information Security Manager (CISM), and Certified Information Systems Security Professional (CISSP).

Tatsuya Fujiyama
Security Human Resource Management Department, Cyber Security Technology Operations, Security Businesses Division, Service Platform Business Division Group, Services & Platforms Business Unit, Hitachi, Ltd. *Current work and research*: Development of cybersecurity human resources. *Society memberships*: The Information Processing Society of Japan (IPSJ). *Certifications:* CISA and CISSP.

Manabu Natsume
Security Business Planning Department, Business Management Division, Security Businesses Division, Service Platform Business Division Group, Services & Platforms Business Unit, Hitachi, Ltd. *Current work and research*: Business development, cyber and physical security. *Certifications:* CISA and CISM.

Motoshi Sakakura
Security Human Resource Management Department, Cyber Security Technology Operations, Security Businesses Division, Service Platform Business Division Group, Services & Platforms Business Unit, Hitachi, Ltd. *Current work and research*: Development of cyber security human resources.

Ryo Nakano
Security Human Resource Management Department, Cyber Security Technology Operations, Security Businesses Division, Service Platform Business Division Group, Services & Platforms Business Unit, Hitachi, Ltd. *Current work and research*: Development of cyber security human resources.