6th Term Core Human Resource Development Program

Introducing Our Efforts in Final Projects

A final project is that the trainees utilize their knowledge and experience absorbed through our year curricula and tackle agendas set for their dispatching company and industry as a team. The six-term trainees conducted twenty-two projects, and we will introduce four projects this time. Please visit the IPA website for other projects.
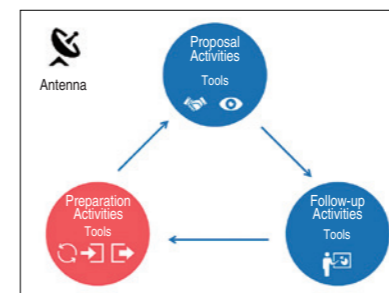
🎓 How to win Security Investments

◆ Backgrounds and Issues

The number of cyber crimes and their damages have been increasing, and each company expects that information security-related expenditures will also increase; however, the percentage of its expenditures in IT budgets has been decreasing. Thus, the priority of security measures might be low in the future. The project team identified the challenge of winning continuous security investments (budgets and cooperation) within the organization and launched this project to ensure proactive 'investments' rather than reluctant 'cost'.

◆ Issue-Solving and Outcomes

The team interviewed security staff and management from sixteen company to solve this issue. The members discussed and analyzed the issue based on the interviews. Through these activities, the team created a reference material called "How to win Security Investments," compiling methods, tools, and best practices enabling us to keep winning security investments. First, the team categorized the whole picture of how to win investments into the processes: Preparation activities, Proposal activities, and Follow up activities, like the diagram below; besides, they expressed the antennas to obtain information inside and outside of the companies. Their outputshows the concrete methodologies and examples for each item. For instance, preparation activities represent methodologies for establishing a foundation to win investments easily, how to make management involved, provide information, and connect outside of the companies. We can find websites focusing on proposal activiti es for security investments; however, the core features of this project outcomeare to consistently demonstrate not only those proposal activities but also everyday attitudes and activities after winning security investments.

Mr. UEDA Yuji, Azbil Corporation
(2nd from the front row left)and the project members

Interview with A Graduate

> ### What is your utmost benefit from this project?

We could identify, so to speak, stakeholder communication by security style. In the drastically changing cybersecurity environment, we also summarize how to engage in each department and management. Through the face-to-face interviews with companies, we learned real examples like actual efforts undertaken by each company and the stances and thoughts of security taken by the staff and management; thus, we deepened our insights.

> ### Methods for utilizing project outcomes

You can utilize our project outcome when considering the activities that make other departments and management regard security as their own issue. With the perspective of only getting a security budget, cybersecurity might not be a company-wide effort, even though we obtain the budget. The features of our outcome are that we incorporated the perspectives of both budgeting and eliciting cooperation.

> ### This is unique to the ICSCoE!

The trainees of the ICSCoE are a neutral, regardless of their company, and have access to people on the front lines without being cautioned. I had the opportunity to meet people, mainly the graduates of the Core Human Resource Development Program, through the interviews and felt the ideal Core Human Resource we are supposed to be and the connections as colleagues of the ICSCoE.

Antenna · Proposal Activities Tools · Preparation Activities Tools · Follow-up Activities Tools

The whole picture of how to win security investments

For download this outcome

🎓 Plus・Security Human Resource Development

◆ Backgrounds and Issues

Recently, the departments within enterprises, not only the security department, have been facing a shortage of plus・security human resources who can conduct their operations with security awareness. More specifically, these problems are that many people do not recognize security issues as their own business, and the concept of secure-by-design has not pervaded society. Due to these circumstances, the team launched this project intending to raise security awareness in planning, development, design, establishment, and operations departments, understand damages when occurring incidents, and recognize concrete work for system configuration.

◆ Issue-Solving and Outcomes

① Hands-on Training

The team developed hands-on training through which users can experience simulated incidents and examine those causes and countermeasures. By taking this training, users can understand the risks of cyber attacks and the points becoming the origin of attacks. Also, this training enables users to design, construct, and operate their systems with secure-by-design awareness during practical operations. Moreover, since personnel from various departments can participate in this training, the team also aims to provide them with an opportunity to consider measures based on the knowledge and thoughts of different departments.

Items	Contents willing to teach	Security Holes	Scenarios
①	Risks of phishing emails	—	A critical incident facing information leakage caused by phishing emails
②	Management of credentials	Store the large file stating the credentials (ID and password for log-in) on the desktop	Unauthorized access to more high-order devices by using the credentials stored in the infected device
③	Risks of reusing passwords	Use the same password for different accounts	Lateral movement and intrusion into deeper NW due to reusing the same password
④	Least privilege	Accounts granted excessive authority	Browse files not authorized to access and encrypt them by editing
⑤	Configuration of access controls	Unnecessary FW configuration	Poor access controls from NW for server administration to external NW

Training scenario examples

② Security Item Search Tool

For the users without knowing specific security measures that they should take, the team created search tools to comprehend security items necessary to consider during their business assignments.

This tool enables users to search items through 3 approaches: business contents, incident cases, and word retrieval, and the team shapes it to access necessary information efficiently. Moreover, the purpose of this tool is that users can understand each item and recognize the importance of constructing and operating secure systems.

The screen images of tool

Interview with A Graduate

Mr. NISHIGUCHI Tomoya
Optage, Inc.

> ### What is your utmost benefit from this project?

Through my experience leading the project team, I gained management abilities to pull a team together. To become a leader, personnel generally need to reach sufficient age and experience; therefore, it is hard for enterprises to entrust a leader to younger personnel. I did not have enough experience, but I took it as a precious opportunity to be a leader and led the final project. At first, I had a bitter experience not processing the project since I could not summarize things logically. However, I could manage to finish the project. I believe it was also a great benefit to realize the importance of decision-making capacity as a leader to determine the direction of our project.

> ### Methods for utilizing project outcomes

I want to organize in-house hands-on training by customizing it for my company and adding more scenarios. Also, I plan to deploy our security item search tool within the enterprise and introduce incident cases at the regular meetings.

> ### This is unique to the ICSCoE!

That would be an incredible environment where I could casually communicate with fellow trainees from various enterprises we belong to, occupations, and ages. That is unique to the ICSCoE. During the final project, I cultivated personal exchanges in different areas. It was the most meaningful to gain experience I had never had during practical operations within my company; for instance, I could deepen my knowledge and skills of OT systems I had never touched.

Construction Industry and Cyber Security (CICS)

◆ Backgrounds and Issues

In the construction industry, companies are using Digital Transformation to improve operational efficiency and enhance the comfort, convenience,and safety of buildings. On the other hand, there are issues in awareness and countermeasures for cyber security.

◆ Issue-Solving and Outcomes

To enhance security awareness in the construction industry, the project team focused on two security themes to address the issues and provided the solutions.

Theme 1

Construction Industry and Cybersecurity Education

The team believes it is essential to improve security awareness throughout the supply chain in the construction industry. In response, they created a cybersecurity educational video that aims to make cybersecurity education accessible to industry members and educate them about incidents. The video explains actual and potential incidents that have happened or may happen in the construction industry in a narrative form. Additionally, they have documented the method by which anyone can create and modify such educational videos quickly and easily at a low cost.

Theme 2

Cybersecurity in Building Facilities

The team examined and listed out the cybersecurity measures needed for each stakeholder throughout the long-term lifecycle (design stage through to demolition) of the building and provided two solutions and important points for constructing a secure building.

① Self-Checklist

A checklist was developed to instruct the person in charge to consider and implement at every stage of the building lifecycle, including design and specification review, and construction. Each item on the list has its target stakeholders identified, and the list can be used to ensure that all parties involved have a clear understanding of each other.

② Guide for Checklist Items

The team summarized the "background and purposes" of the question items in the Self-Checklist, the "possible risks" if not implemented, and the "explanation of contents and examples of measures" that are crucial for achieving the items on the list.

For download this outcome

Project Leader
Mr. Satoshi Kikugawa (front row center)
Kinden Corporation
Nine members of the project team includee general contractors, subcontractors, vendors, manufactures, and user companies that are connected to the construction industry.

Interview with A Graduate

⟨ **What is your utmost benefit from this project?** ⟩

Thanks to the lecturers' precise advice and their in-depth review, we gained a new perspective from this project. For instance, the idea of considering the checklist items in terms of stakeholders and building lifecycle came from the discussions we had with the lecturers.

⟨ **Methods for utilizing project outcomes** ⟩

The video will be the best tool for raising security awareness. To illustrate, it is possible to display it on digital signage at the construction site. We also have established a method for making videos that is both affordable and quick, so that you can immediately create a video to alert within the company when a new incident case arises. The checklist offers clues on when, who, with whom and how to consider and implement measures, given that the construction industry is entangled with many different positions.

⟨ **This is unique to the ICSCoE!** ⟩

The connections among the trainees will broaden the scope of our activities. For example, our connections as trainees allowed us to organize an office building study tour, interview industry associations and receive feedback on our project outcomes from ICSCoE graduates, which provided us with a broader perspective and deepened our knowledge.


International Security Controls

◆ Backgrounds and issues

As global corporate management and system integration progress, security enhancement becomes an issue for the whole enterprise group. In the meantime, Europe and the United States have disclosed the advanced regulations and guidelines; thus, Japanese enterprises have been required to respond to them. However, it is crucial to comprehend the actual conditions of undertaken security measures at overseas sites, and enterprises face the issue that it is also troublesome to obtain a whole picture of regulations and guidelines and apply them to concrete measures. In this project, the team created two outcomes, the Maturity Model and Best Practice Guide, to respond to advanced security requirements overseas and contribute to increasing security levels for the whole enterprise, including its overseas sites.

◆ Issue-solving and outcomes

① Maturity Levels

The team established the maturity model - which enterprises can compass how overseas sites handle - and provide benchmarks. When creating this model, the members read up on the representative international regulations and guidelines and extracted 75 requirements emphasizing during the actual operations. In this model, the team set required countermeasures and the results by examining international standards and documents as evaluation axes. Moreover, they list the criticality and coverage of each item for users to comprehend more smoothly.

Development process of Maturity Model and summary of the model
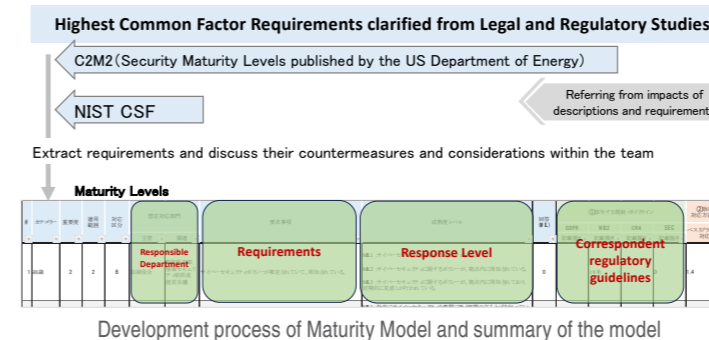
② Best Practice Guide

The team compiled the examination results as their case studies, primarily intended as references for security planning personnel when deriving concrete measures. Their outcome is a collection of concrete measures undertaken by domestic sites; thus, their guide enables domestic and overseas sites to build a relationship to increase the maturity level through reciprocal cooperation.
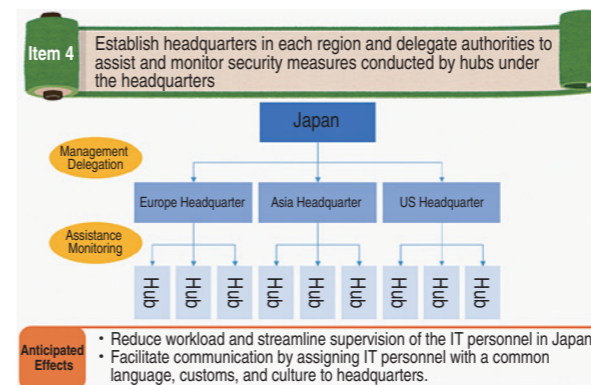
Samples of Best Practice Guide

Interview with A Graduate

(From left)
Ms. GOTO Naho, Ebara Corporation
Mr. TOMOFUJI Ryosuke, Daikin Industries, Ltd.

⟨ **What is your utmost benefit from this project** ⟩

Mr. TOMOFUJI : My great benefit was to expand my connections among instructors, fellow trainees, and graduates and to be in an incredible environment where I could casually ask my curious topics, such as the security condition of my company and perceptions. For instance, I had an opportunity to inquire about the circumstances of security measures at overseas sites; it would be impossible for me to gain such knowledge. It was hugely helpful. The connections I have built will be the biggest weapon for me and my company.

⟨ **Methods for utilizing project outcomes** ⟩

Ms. GOTO : I want to know the maturity level at each site and examine the gaps between the ideal and actual levels. I am speculating to contrive the stepping-stone security measures to prepare for local responses at overseas sites and global cooperation as confirming those examination results.

⟨ **This is unique to the ICSCoE!** ⟩

Mr. TOMOFUJI : Departing from my regular work, I could dig in a wide-ranging field for one year. I should engage in all areas since I feel many subjects get involved in security. Therefore, learning cybersecurity in advance, which I will have to experience in the future, was a great benefit.

Ms. GOTO : Actually, I have a background in liberal arts, but I could understand the points that I should study to play an active role as a core human resource from now on through the systematically organized curricula. Besides, we can receive practical exercises for incident responses only at the ICSCoE but nowhere else. I could experience a series of flows from information gathering and decision-making to responding firsthand that will be my valuable assets directly linked to my further practical operations.