KASPERSKY lab

Practical guidance on tackling cyber threats

国立大学法人
名古屋工業大学

www.nitech.ac.jp

Japan's leading engineering college places Kaspersky Interactive Protection Simulation (KIPS) at the heart of its vocational training.

Nagoya Institute of Technology (NITech) is one of Japan's leading engineering colleges. Founded in 1949, it is home to around 5,600 students.

NITech's Koshijima Research Lab studies business continuity plans (BCP) in the context of cyberattacks. BCP-based approach has become an increasingly important topic in recent years. Koshijima Research Lab conducts regular security workshops alongside Japan's Information-technology Promotion Agency (IPA).

Challenge

Professor Ichiro Koshijima, who leads the lab, says the hardest thing about training cyber security personnel is that it is almost impossible to simulate a cyberattack on which to practice.

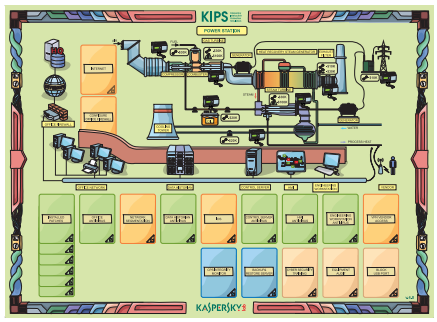
"A rapid and accurate initial response is vital when an incident occurs, and it is hard to figure out what the cause is. It could be human error, or it could be equipment trouble."

The NITech approach is for students to consider the possibility of a cyberattack immediately. He says hands-on exercises rather than academic study are preferable if students are to be encouraged to think logically and make flexible judgments.Having attended large-scale cyber security exercises in the U.S., alongside the Department of Homeland Security, Professor Koshijima says he was inspired to think differently about security training based on plant safety: "It seemed like a festival where members of the Computer Security Incident Response Team (CSIRT) had gathered to show off their brilliant skills. Problems with operating and managing critical infrastructure cannot be solved just in cyberspace. You have to rely on field operations."

Koshijima Research Lab's Control System Cyber Security Workshop is held twice a year alongside two IT companies. Professor Koshijima says he wanted an approach that reflected practical methodology and while inspiring participants business continuity plan for critical infrastructure under cyberattack requires not just an IT response, but on-site knowledge and communication for incident management."

"The BCP for critical infrastructure requires management ability, combining not just IT technology, but operational knowledge and communication skills."

Ichiro Koshijima
Professor at Nagoya Institute of Technology



Kaspersky Interactive Protection Simulation : KIPS

■ **The purpose of the game**

- Protect your company's assets as part of a plant cyber security team
- Find and analyze all pitfalls in cyber security system and make an appropriate incident response to maximize revenue during five turns. Total revenues determine the winner at the end of the game

Kaspersky Lab Solution

After searching for realistic exercise programs, Professor Koshijima found Kaspersky Interactive Protection Simulation (KIPS) offers the ideal, game-type structure.

The purpose of the game is for students to protect their company's assets as part of a plant cyber security team. Players oversee two production lines and have to maximize revenue during five rounds. Total revenues determine the winner at the end of the game.

"KIPS was the first time we saw a simulation game puts together for security management and business continuity management," says Professor Koshijima. By adding the knowledge obtained by the students' analysis to the workflow, and recording how participants thought and acted during the first four control system cyber security workshops, the Koshijima Research Lab has created a new format for the exercise, the KIPS NIT version.

In this version that was played on top of standard KIPS game, players are split into two teams: the HQ team, which acts as management, and the plant team, which deals with the actual incident. Teams are only allowed to communicate via chat, using their email address to make clear who is responsible for each decision made by card selection.

"Thanks to these innovations, the workshop was more interesting than ever," says Professor Koshijima. "At the wrap-up meeting, nobody cared what the final player rankings were. Many participants commented on the 'realness' of the simulation."

"The BCP for critical infrastructure requires management ability, combining not just IT technology, but operational knowledge and communication skills."

Ichiro Koshijima
Professor at Nagoya Institute of Technology

The data to drive ongoing improvements

All chat logs during the highly-praised new workshop were recorded and analyzed by the students at the Koshijima Research Lab.

Akihiro Tsuchiya, one of the students who contributed to the new exercise framework, explained that the differences between the good teams and the bad teams were obvious: "One thing I noticed when reading back over the chat logs was that teams with good results had a lot more positive conversations. On a team with poor performance, more members say "I am sorry" and show a posture that I can not be confident."

Professor Koshijima says this insight is hugely significant for future training. "Positive teams quickly and autonomously decided the information to be shared, in advance. They were clear in what action was to be taken. On the other hand, teams that were constantly apologizing to each other ended up chasing their tails." More research on these differences in behavior will result in more practical security personnel training, and he says: "What we are doing is a lot like creating a new MBA course.

"It is easy to tell people to prepare against cyberattacks, but you have to consider the human factors. To get people to work effectively, you have to lay the fieldwork. It is not enough to get a certification. With KIPS, our training will continue to let participants improve their ability to think and understand logically, to be able to respond flexibly to ever-evolving cyberattacks. We have great hopes for our future partnership with Kaspersky Lab."

Kaspersky Security Awareness:
http://www.kaspersky.co.jp/enterprise-security/cybersecurity-awareness

#truecybersecurity

www.kaspersky.co.jp

Kaspersky Lab HQ
39A/3 Leningradskoe Shosse
Moscow, 125212
info@kaspersky.com
www.kaspersky.com