lakyara vol.222

Special Edition

Protecting companies against cyber-attacks

-Interview with Christopher Crowley by Mitsuyoshi Sugaya-

10.September.2015

Nomura Research Institute, Ltd.

Executive Summary

Information theft and other losses due to cyber-attacks is a growing problem even in Japan. Fortification of information security has become an urgent priority for Japanese companies and organizations. NRI SecureTechnologies' Mitsuyoshi Sugaya spoke to information security expert Christopher Crowley, a SANS Institute certification instructor, about defenses against increasingly sophisticated cyber-attacks in the US.

Christopher Crowley

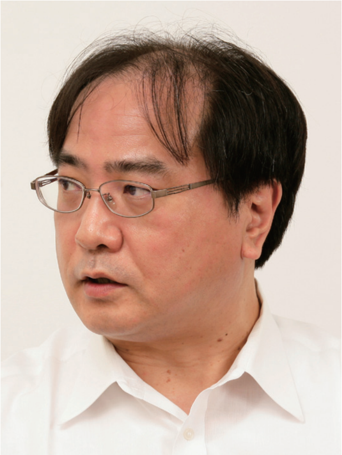
Certified Instructor, SANS Institute

Mr. Crowley has 15 years of experience in security management and network security. He currently works as a consultant in the Washington, DC, area. His specialties include penetration testing, network defense, incident response and forensic analysis. He holds numerous global certifications, including GSEC, GCIA, GCIH, GCFA, GPEN, GREM, GMOB and CISSP.

Mitsuyoshi Sugaya

Director/Fellow, NRI SecureTechnologies, Ltd.

Joined Nomura Research Institute in 1991. After working as an information security consultant, he helped to launch NRI SecureTechnologies. He has been a director of NRI SecureTechnologies since 2006. He is also Board Chairman of Financials ISAC Japan and Vice President of the Japan Information Security Audit Association. He holds a doctorate in engineering and GCIH.



Cybercrime in US today

Mitsuyoshi Sugaya: Although Japan is a low-crime country by global standards, cybercrime is on the rise, partly due to its borderless nature. Targeted cyber-attacks in particular have increased dramatically in recent years. Is the same true in the US also?

Christopher Crowley: Yes. One recent example is a breach involving the US Office of Personnel Management. The breach targeted US government staff who have security clearances granting them access to confidential information. Eighty percent of government personnel with security clearances had their personal information stolen. These are the people charged with defending information. The breach makes the [attackers'] toughest job easier because they now know whom to target.

Sugaya: In Japan, e-mails with malware-infected file attachments sent by cybercriminals posing as a colleague or business associate of the recipient are becoming increasingly common. In response, a growing number of companies are training their employees not to fall prey to such targeted attacks. Is such training conducted in the US and, if so, how effective is it?

Crowley: Such training still doesn’t work in the US. The problem is that one or two successful incursions are enough to give the attacker organization enough access to move forward. Training has raised awareness substantially but recipients of baited e-mails still continue to make mistakes.

The idea of defense [against such attacks] is shifting from the concept of we can prevent things to we know that some of our prevention will fail, so we need to pay more attention to detecting issues when they arise in order to thwart the attackers' ultimate objective.

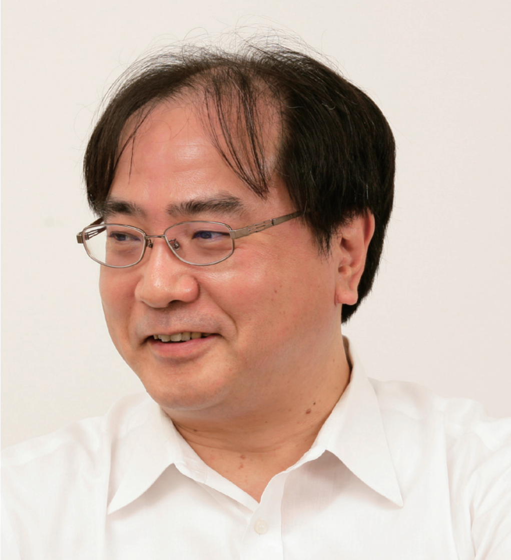
Sugaya: Another form of targeted attack that is on the rise in Japan is theft of money through unauthorized wire transfers via online banking platforms. The attackers target individuals or businesses that are online banking customers, not corporate websites, and install malware on the victims' computers. Such thefts are consequently difficult for banks to prevent. What types of security measures are effective against such attacks?

Crowley: I've seen an increase in reports of that type of theft in the US also. In the financial industry, banks have started working together to share information about the attackers and their methodologies to more quickly shut down the resources that the attackers are using and identify victims to limit losses. Because these attackers are ultimately using the same software and tactics, sharing information is an effective defense strategy.

Another strategy banks are using is technical countermeasures, the most common of which is out-of-band verification. When a customer initiates an online transaction, the bank requires additional verification in the form of a mobile transaction authentication or authorization number sent to the customer's cellphone by text message. Most banks offer this functionality.

Sugaya: So effective security requires multiple lines of defense such as prompt information sharing and technical countermeasures.

Another form of cyber-attack, one that is still rare in Japan, is ransomware, malware that encrypts files on the victim's computer and demands that the victim pay a ransom to regain access to the files. The threat of ransomware becoming more common in Japan is a concern. How should one respond to a ransomware attack? Would you advise paying the ransom or abandoning the hijacked data?



Crowley: I'll tell you a story. A friend contacted me one day asking for advice. Her company's primary server with nearly two terabytes of data had been hijacked by ransomware. The first thing I asked was, Do you have a secondary copy of this data securely stored offsite? They didn't. So I suggested that they immediately engage a company that specializes in responding to such incidents but not pay the ransom. I told her to be sure to get professional guidance because the people she was up against are professionals at extorting money.

Sugaya: So the moral of your story is that it is crucial to take the precaution of backing up important data, correct?

Crowley: That's right. The outcome was they were able to actually recover their data, but that's just one case. I've heard of other cases where ransoms were paid but the data were not recovered. Probably the most fundamental defense is to have multiple backups of your important data.

Promoting sharing of security information

Sugaya: You mentioned the importance of promptly sharing information. Financials ISAC (Information Sharing and Analysis Center) Japan was established last year for sharing information-security information among financial institutions. What is the secret to successfully information sharing among a diverse group of companies with different reasons for participating in the group?

Crowley: I think that a very important mechanism for sharing information is the ability to abstract the information away from your organization and turn it into actionable information. One such information sharing framework is Mandiant's indicators of compromise (IOC). It allows one organization to share details about an adversary or attack vector without divulging the attack's impact on itself or proprietary information about its information systems.

Another strategy for sharing information within a consortium is to have a mechanism that allows each member of the consortium to designate whom they are willing to share data with. ThreatConnect, an online information-sharing platform, does something along these lines. ThreatConnect has special interest groups and validates these groups' membership. Members are then able to share relatively sensitive information because they know who will get the information.

Sugaya: Financials ISAC Japan uses a similar mechanism called the Traffic Light Protocol (TLP) that enables information sources to restrict the scope of their information sharing by color-coding information (e.g., red information, yellow information) based on the extent to which they wish to share it.

Crowley: That's great.

How should management approach information security issues?

Sugaya: In recent years, information security has become a major management issue even in Japan. More and more companies are appointing chief information security officers (CISO). How should C-suite executives approach information security issues?

Crowley: I think that if you were going to establish a separate information security office headed by a CISO, you would need to ensure that the CISO's decisions are actually implemented across the organization. What I've seen in most large organizations is the CISO is often unable to effect organization-wide change. Or worse, the CISO has a lot of power and changes a lot of things but is out of touch with how the business is actually run or makes changes that are not consistent with the business's capabilities.

So to answer your question, the right mix is a CISO who understands the details of security and knows how to decide how much security is enough to allow the business to continue growing while preventing catastrophic failures.

Sugaya: With information security, you're damned if you don't and damned if you overdo.

Crowley: Exactly, because security is loss prevention. A business makes money however it makes money while security minimizes losses.

Sugaya: Japanese companies and organizations are increasingly establishing computer security incident response teams (CSIRTs) to deal with any incidents related to computer or network security. While information collection and analysis are supposedly important missions of CSIRTs when they are not responding to incidents, I feel that CSIRTs are actually often positioned as virtual response teams that spring into action when an incident occurs but otherwise perform IT-related functions other than security. How are CSIRTs set up in the US?

Crowley: I can tell you about two CSIRTs I've participated in. At the US Department of

Energy (DOE), there were multiple groups that functioned as CSIRTs even within one organization. Depending on the organizational units participating, different information would be shared in the different groups. Participation in each group depended upon the sensitivity of the data that was shared within that group. In all of the groups, a majority of participants were DOE staff whose sole role was incident response. Such an approach is typically the most effective.

A second example is a group called InfraGard run by the US Federal Bureau of Investigation (FBI). InfraGard allows people from different companies and specific sectors to come together to share information. Through my participation in InfraGard, I found that most of the other participants were not exclusively involved in information security. Their participation in InfraGard was a part-time duty. InfraGard functions more as an organizing principle to allow and facilitate information sharing.

Is it better to build an SOC in-house or outsource?

Sugaya: In addition to CSIRTs, the main purpose of which is incident response, another type of corporate organization involved in information security is security operations centers (SOCs), whose mission is information security monitoring. While SOCs play a central role in protecting information assets, having an in-house SOC is not feasible for all companies, even some large ones. Outsourcing of the SOC function is one option. How do US companies decide whether to build an in-house SOC or outsource?

Crowley: This is a very frequently asked question and I don’t have a single guiding principle applicable to all companies. I can’t say that companies up to a certain size are better off outsourcing. When people ask me what to do, I always suggest that they first identify what capabilities–human resources, technologies, hardware–their organization already possesses. Make those existing capabilities the foundation. If their capabilities don’t currently include a central correlation functionality to derive information from their data–in other words, the ability to identify within available data meaningful deviations from what’s acceptable–they need to work to enhance that.

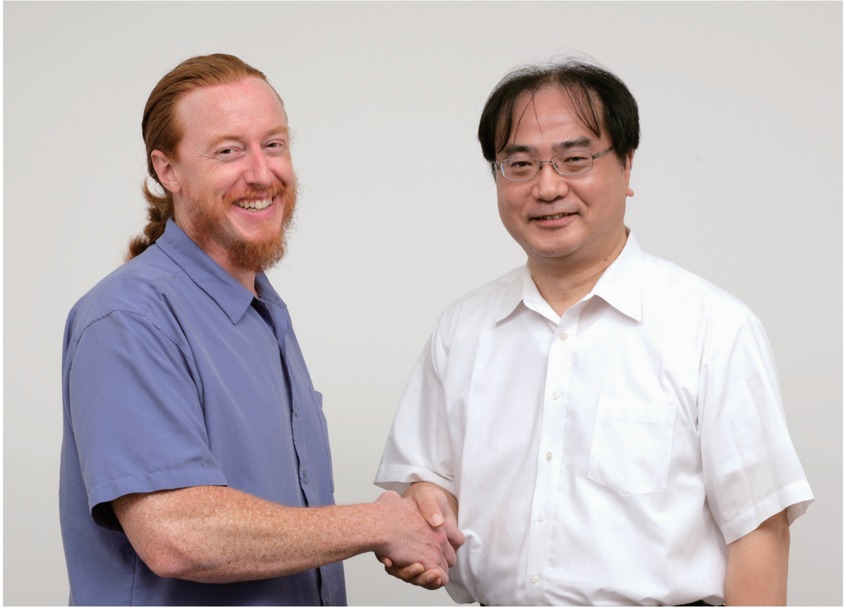
This doesn’t necessarily mean looking at all the network intrusion detection system data or looking at all of the alerts from any given tool. What I mean is the ability to really focus on what is most important to that organization. If a company doesn’t understand that themselves, it would be very hard to get an external service provider to effectively perform the SOC function. Outsourcing can be a very cost-effective strategy but to derive value from it, you have to inform the service provider what's important to you in order to get the right sort of escalation of information. Otherwise, you may end up with a third-party sending you alerts that are of little value to you and actually distract your incident-response staff from doing their jobs.

Sugaya: In short, whether a company has an in-house or outsourced SOC, it must have a clear understanding of what the SOC needs to do to fulfill its intended functions.

Crowley: Correct. And one way to acquire such know-how is through training courses offered by SANS, where I work as an instructor. SANS was founded in 1989 in the US to provide IT security training to government and corporate personnel. It now offers training courses not only in the US but throughout the world.

SANS courses are very good at training people who will participate in SOCs' operation and management. People who've been trained by SANS can help to refine the assessment of information within an SOC.

MITRE recently published an authoritative reference document for SOC specifications. It's available for free. However, its content is limited to considerations that should be taken into account when building an SOC. You still have to put all of those things into practice. And building an SOC is only the first step. An SOC's real value is the long-term use, management, and action that comes from it.



Sugaya: I expect that information security organizations such as CSIRTs and SOCs will require increasingly skilled personnel going forward. Adroitly utilizing specialized training courses is an effective means of cultivating such human resources.

Thank you for sharing your valuable knowledge with us today.

about NRI

Nomura Research Institute, Ltd. ("NRI", TYO: 4307) is an independent, global IT solutions and consulting services provider with annual sales of 406.0 billion yen as of FY ended March 2015. With front-to-back support for the buy- and sell-side, NRI's tradition of innovation has positioned them as a trusted international market leader. Leveraging NRI's global consulting business, NRI is able to provide innovative financial IT solutions for investment banks, asset managers, banks and insurance providers. For more information, visit www.nri.com.

The report is provided solely for informational purposes for our UK and USA readers and is not to be construed as providing advice, recommendations, endorsements, representations or warranties of any kind whatsoever.

Whilst every effort has been taken to ensure the accuracy of the information, NRI shall have no liability for any loss or damage arising directly or indirectly from the use of the information contained in this report.

Inquiries to : Financial IT Marketing Department
Nomura Research Institute, Ltd.
Marunouchi Kitaguchi Bldg.
1-6-5 Marunouchi, Chiyoda-ku, Tokyo 100-0005, Japan
E-mail : kyara@nri.co.jp

http://www.nri.com/global/opinion/lakyara/index