White Paper

Security for Japan: Adopting Modern Tools

Japan has traditionally been confident about its ability to thwart cyber attacks, but that confidence may be wavering. A significant breach of private data at a government agency, along with preparations for the 2020 Summer Olympics in Tokyo, is causing security professionals to reconsider the threat defenses and processes they are using. Today, Japanese organizations generally lag behind those in other countries in terms of security sophistication and the use of modern threat defenses. We found that:

- The lack of well-defined security roles and strong security processes at the top level of organizations may cloud Japanese security professionals' views of their readiness to deal with cyber attacks
- Slow economic growth and cautious business practices may be stalling the purchase of more sophisticated threat defenses
- From a security perspective, Japan is ill prepared for the exponential growth of the Internet of Everything (IoE) and the challenges it introduces

Major Findings

In this paper, Cisco experts analyze the IT security capabilities in Japan, using data from the Cisco Security Capabilities Benchmark Study.[1] In our analysis, we found that:

- Without clear executive guidance on security policy, organizations in Japan do not perceive themselves to be as sophisticated as their counterparts in other countries: based on responses from security professionals, we classified 38 percent as either upper-middle or high in terms of their security sophistication, compared with 65 percent of organizations located outside Japan.
- Japanese organizations may be less likely to adopt tools that help protect their network infrastructure. For example, only 39 percent use web security tools, compared with 61 percent of organizations elsewhere.
- Japanese organizations may be less likely to see the value of common security tools and processes. For example, 70 percent of organizations outside Japan say they believe that tools for determining the scope of a compromise are effective, but only 48 percent of Japanese organizations do.
- Contrasting with Japan's strong focus on physical security and emergency response to natural disasters, it seems to place a lower priority on being able to respond to cyber attacks. Japanese organizations are less

[1] For more information on this study and the other white papers in this series, see the final sections of this document.

likely to adopt processes that can help mitigate cyber attacks. Fifty-five percent of non-Japanese organizations block the communication of malicious malware in order to prevent security incidents, compared with 37 percent of Japanese organizations.

Lower Security Sophistication

In Japan, there is a growing awareness that cybersecurity needs to be stronger and that organizations need to devote more time and money to building more sophisticated security frameworks. This awareness is being driven by several events. In 2020, Tokyo will host the Summer Olympics, and government officials are focused on mitigating attempts at cyberterrorism. In addition, the Japan Pension Service suffered a highly publicized data breach in mid-2015 after an employee opened a phishing email containing malware that attacked the department's network.[2] The country also recently introduced the My Number system for social security and tax identification, raising concerns that, if stolen, these numbers could make it easier for online criminals to access sensitive personal data.[3]

In 2015, the U.S. government suffered a large data breach at the Office of Personnel Management, and 21.5 million social security numbers are believed to be stolen, among other data.[4] The attack may serve as an example to other countries and prompt changes to prevent similar incidents.

The heightened awareness of the need for stronger cybersecurity comes at a time when Japanese organizations demonstrate lower security sophistication than organizations in other countries and lag behind other organizations in their use of threat defenses, according to the study. Significantly fewer Japanese organizations—38 percent—are classified as either upper-middle or high in terms of their security sophistication, based on survey responses from chief information security officers (CISOs), compared with 65 percent of organizations located outside Japan (Figure 1).

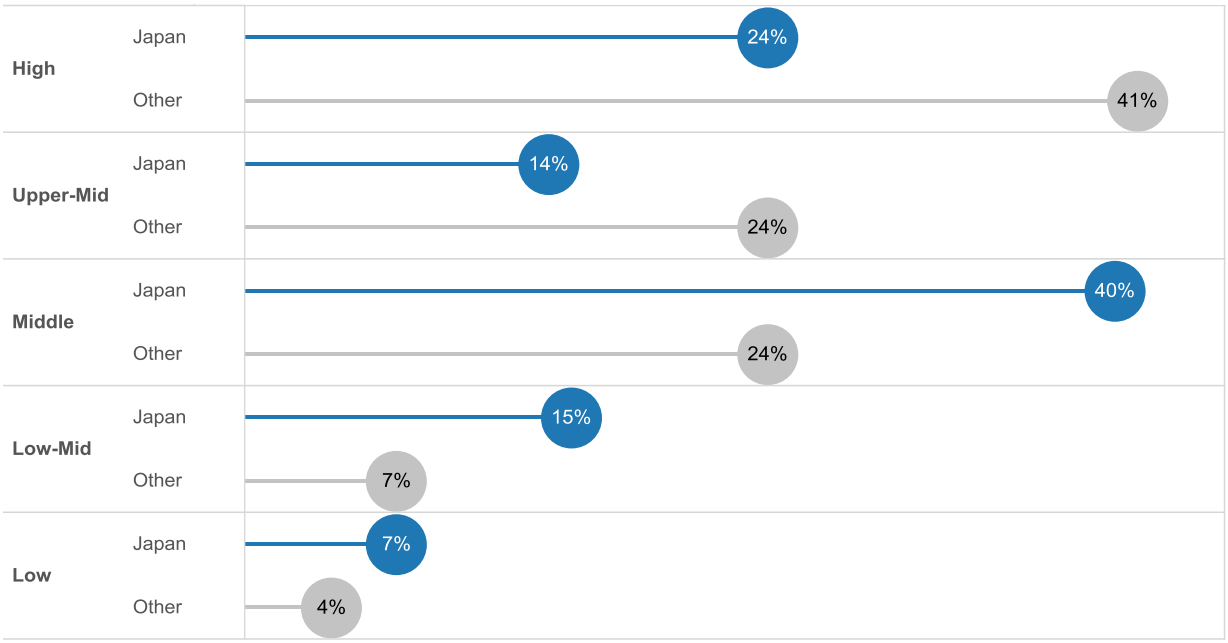
The gap between Japan and other countries in terms of sophistication may be due to the lack of well-defined roles for security at the executive level. In addition, the lack of sophistication and lower adoption of threat defense tools may be due to outdated ideas about the country's vulnerability to cyber attacks. Some Japanese enterprises tend to believe they are less likely to be targets of cyber attacks due to the language barrier.

[2] "Japan Pension Service Hack Used Classic Attack Method," *The Japan Times*, June 2, 2015: http://www.japantimes.co.jp/news/2015/06/02/national/social-issues/japan-pension-service-hack-used-classic-attack-method/#.VhgEBivO50f

[3] "Woman in Her 70s First Confirmed Victim of My Number-Related Fraud," *The Japan Times*, October 7, 2015: http://www.japantimes.co.jp/news/2015/10/07/national/crime-legal/kanto-woman-70s-first-confirmed-victim-fraud-laid-number-system/#.VhgHKCvO50d

[4] "Hackers Stole Social Security Numbers from 21.5 Million People in Recent Data Breach, U.S. Says," *The Huffington Post*, July 9, 2015: http://www.huffingtonpost.com/2015/07/09/social-security-data-breach_n_7764812.html

Figure 1. Perceived Level of Security Sophistication (in Percentages of Respondents)

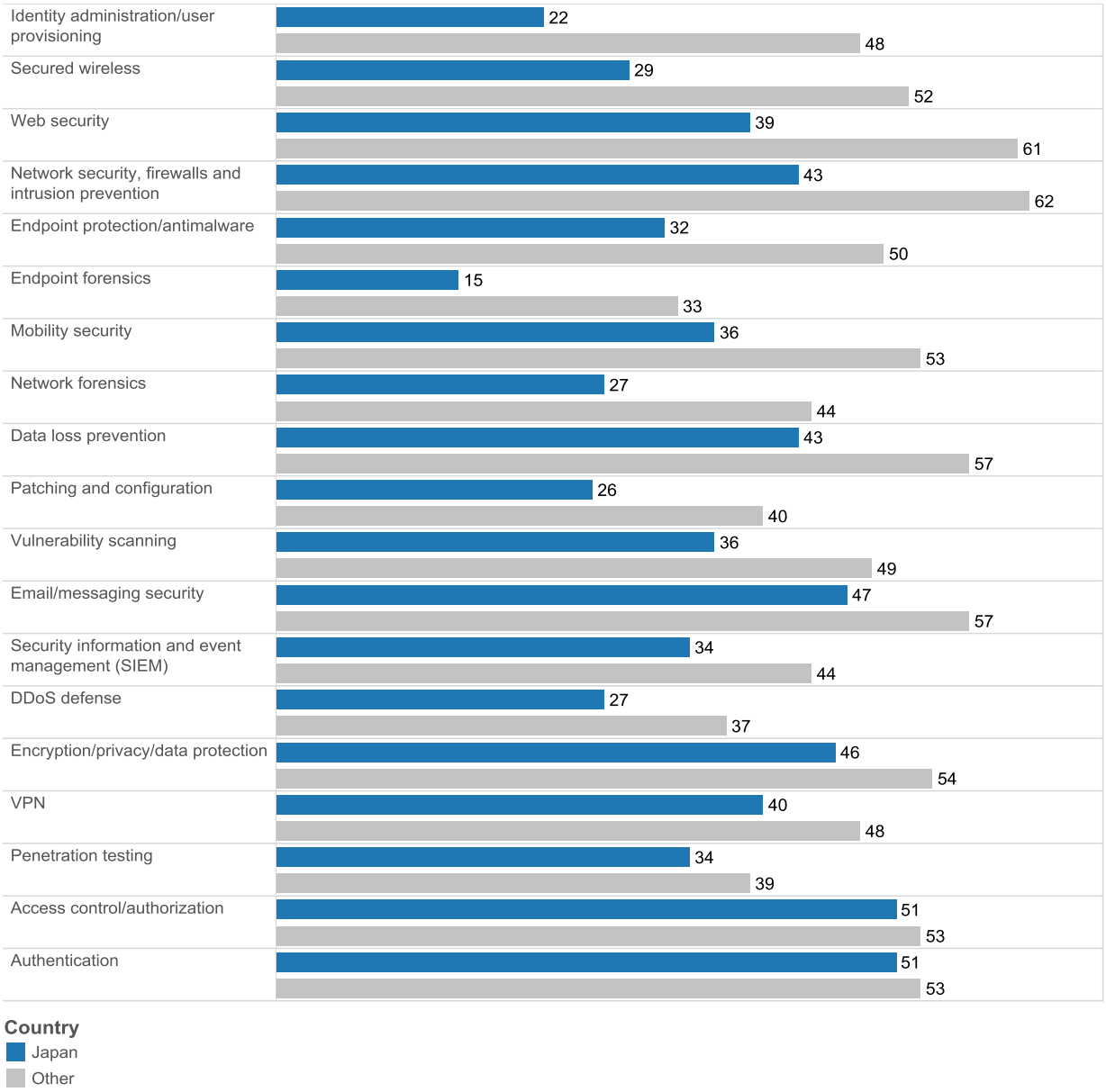


Less Use of Threat Defenses

Because Japan is vulnerable to earthquakes and tsunamis, government agencies and private enterprises have long been focused on the safety and security of the physical infrastructure. Unfortunately, this strong focus does not seem to extend to threats against virtual assets. Japan presents a lower use of threat defenses and other security tools and processes than other countries.

For example, 39 percent of Japanese organizations use web security tools, compared with 61 percent of all other organizations surveyed. Twenty-nine percent of Japanese organizations use secured wireless solutions, compared with 52 percent of all other organizations (Figure 2).

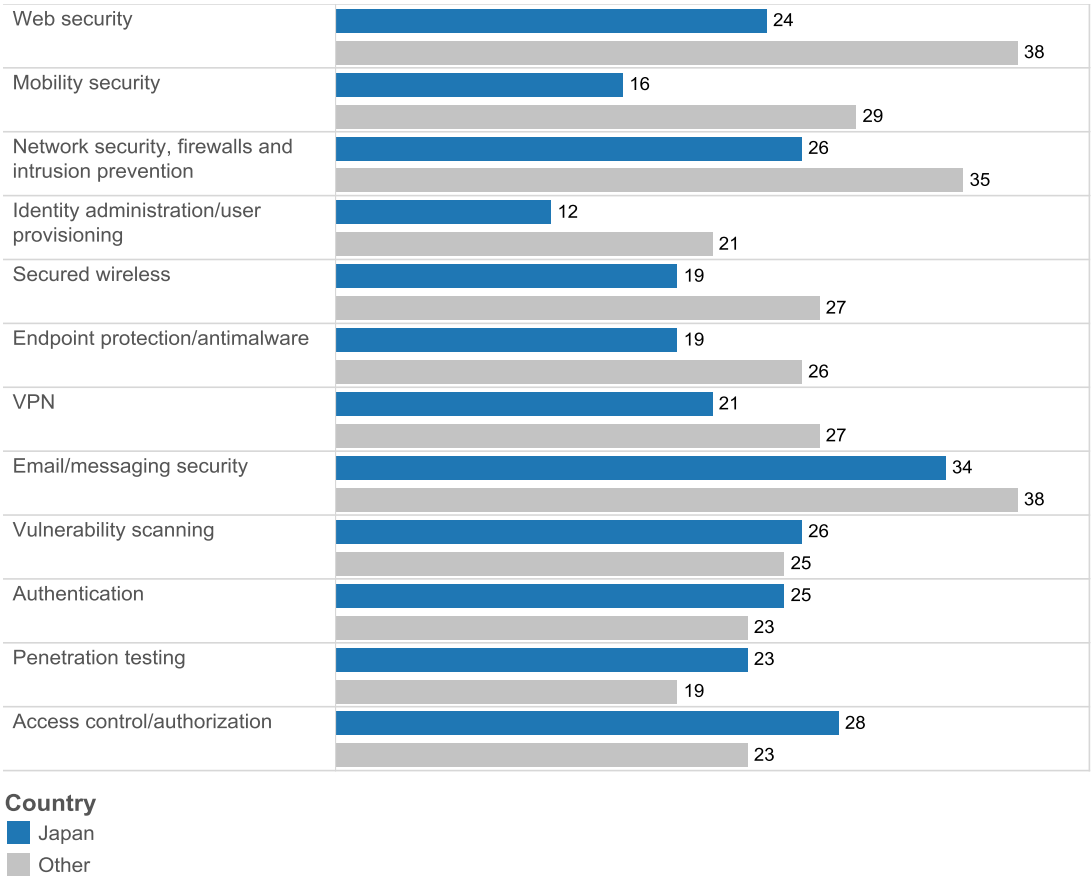
Figure 2. Adoption of Common Threat Defenses (in Percentages)



Despite Japan's overall readiness for cloud computing,[5] its use of cloud-based security solutions is lower than in other countries. For example, 38 percent of non-Japanese organizations use cloud-based web security, while only 24 percent of Japanese organizations do so. Twenty-nine percent of non-Japanese organizations use cloud-based mobility security, compared with just 16 percent of Japanese organizations (Figure 3). The low adoption of cloud-based security is likely a reflection of the overall lower adoption of threat defenses in Japan and not necessarily related to the platform.

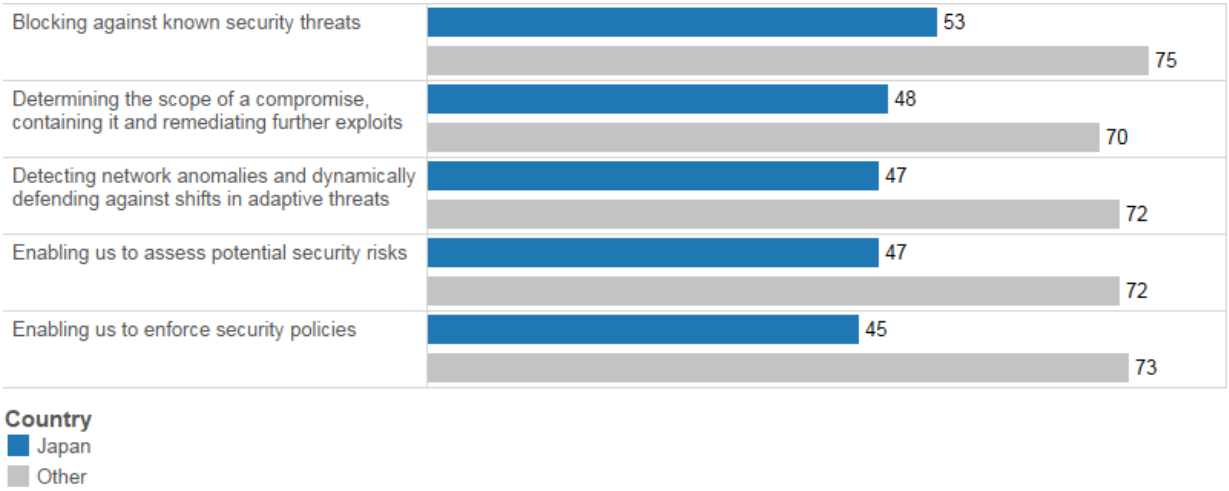
[5] 2013 BSA Global Cloud Computing Scorecard, http://cloudscorecard.bsa.org/2013/countries.html

Figure 3. Adoption of Cloud-Based Threat Defenses (in Percentages)



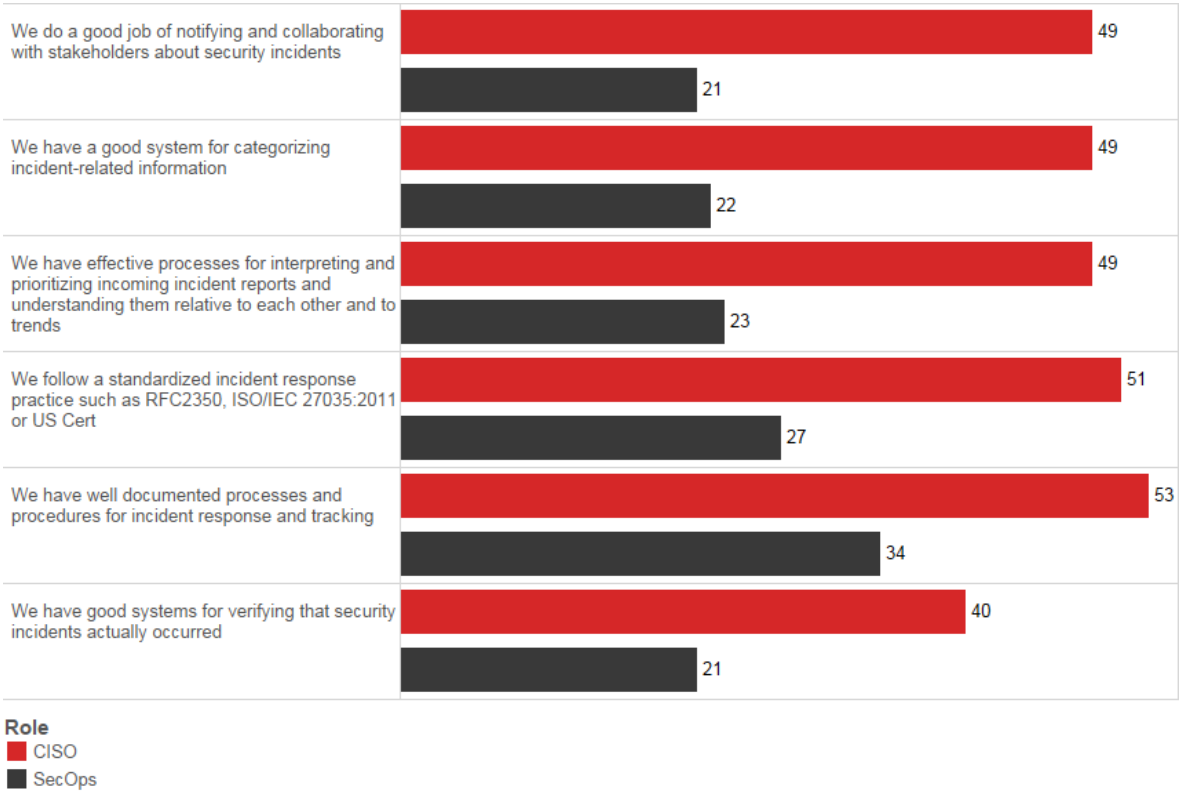
Security roles and strategies are not as well defined in Japanese organizations as they are elsewhere, nor is security viewed as a top priority at the executive level. The lack of clearly defined security roles and strategies may affect Japanese security professionals' perceptions of the value of certain security tools and processes. For example, 70 percent of organizations outside Japan say they believe that tools for determining the scope of a compromise are effective, compared with 48 percent of Japanese organizations (Figure 4).

Figure 4. Respondents Indicating Confidence in the Effectiveness of Their Security Tools (in Percentages)



The lack of well-defined security roles may also affect the views of CISOs and security operations (SecOps) managers on their security readiness. For example, 49 percent of CISOs believe they do a good job of notifying and collaborating with stakeholders about security incidents, but only 21 percent of SecOps managers feel the same way (Figure 5). In addition, 53 percent of CISOs believe they have well-documented procedures for incident reporting and tracking, compared with 34 percent of SecOps managers. One contributing factor to the gap in perception is that SecOps managers are closer to day-to-day security management than CISOs are. For this reason, SecOps managers may be more aware of their vulnerabilities and less confident in their capabilities.

Figure 5. Comparison of Japanese CISOs and SecOps Managers' Perceptions of Security Readiness



Lag in Using Processes to Analyze Compromises

With the exception of government entities, Japanese organizations are not required by law to adopt certain practices and processes regarding data protection and privacy. They are also not required to report breaches. The introduction of such requirements could stimulate Japanese security professionals to prioritize the adoption of in-depth security protections.

For example, Japan lags behind other countries in terms of analyzing network compromises to eliminate their causes. Fifty-seven percent of non-Japanese organizations use malware or file-regression analysis, compared with 35 percent of organizations in Japan (Figure 6). Fifty-five percent of non-Japanese organizations stop the communication of malware in order to eliminate the causes of security incidents, compared with 37 percent of Japanese organizations (Figure 7).

Figure 6. The Use of Various Methods to Analyze Compromises (in Percentages)

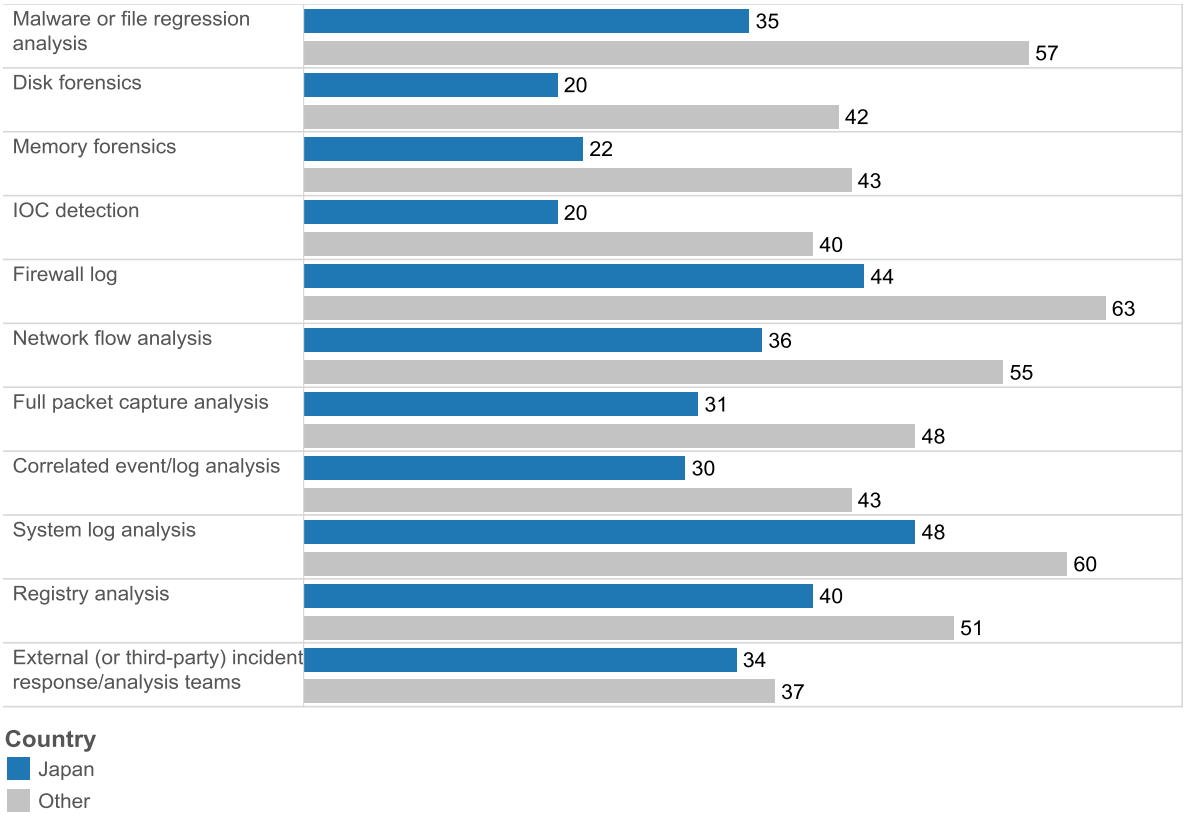
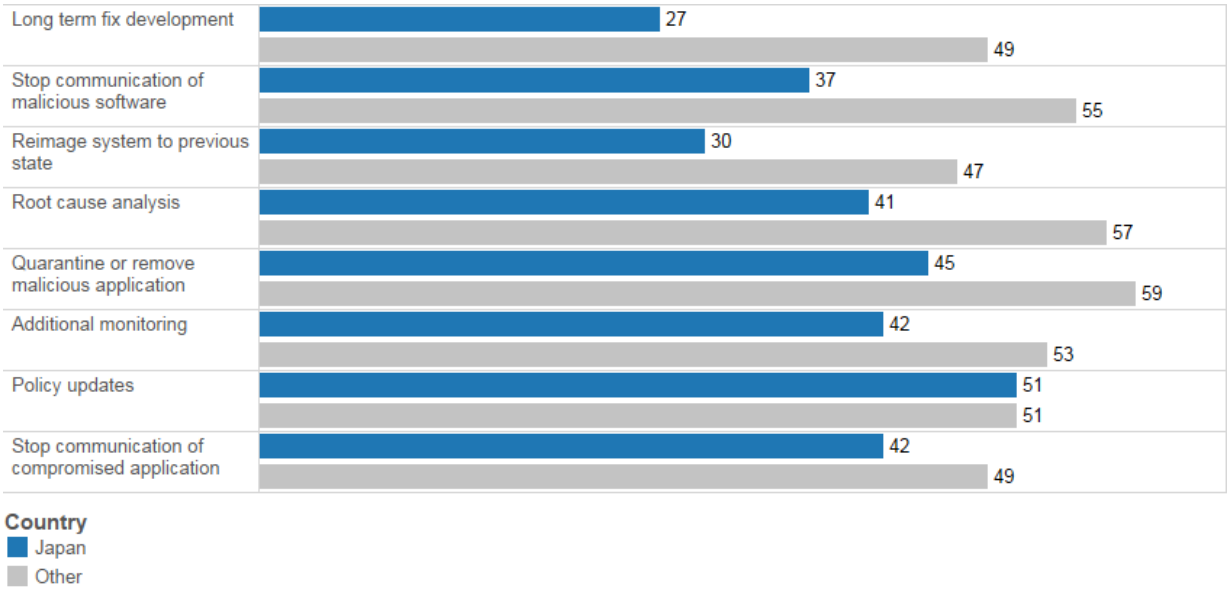
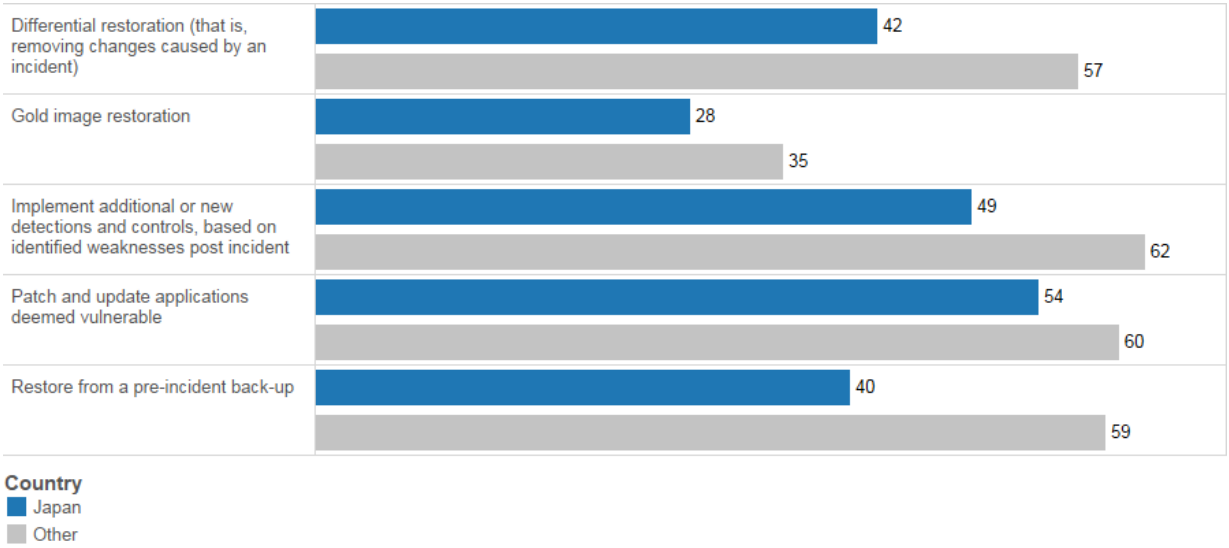


Figure 7. The Use of Various Methods to Eliminate the Causes of Security Incidents (in Percentages)



Likewise, Japan lags in the use of tools and processes that help restore affected systems to pre-incident levels. Fifty-nine percent of non-Japanese organizations will restore systems from a pre-incident backup. Only 40 percent of Japanese organizations will do so (Figure 8).

Figure 8. The Use of Processes to Restore Systems (in Percentages)



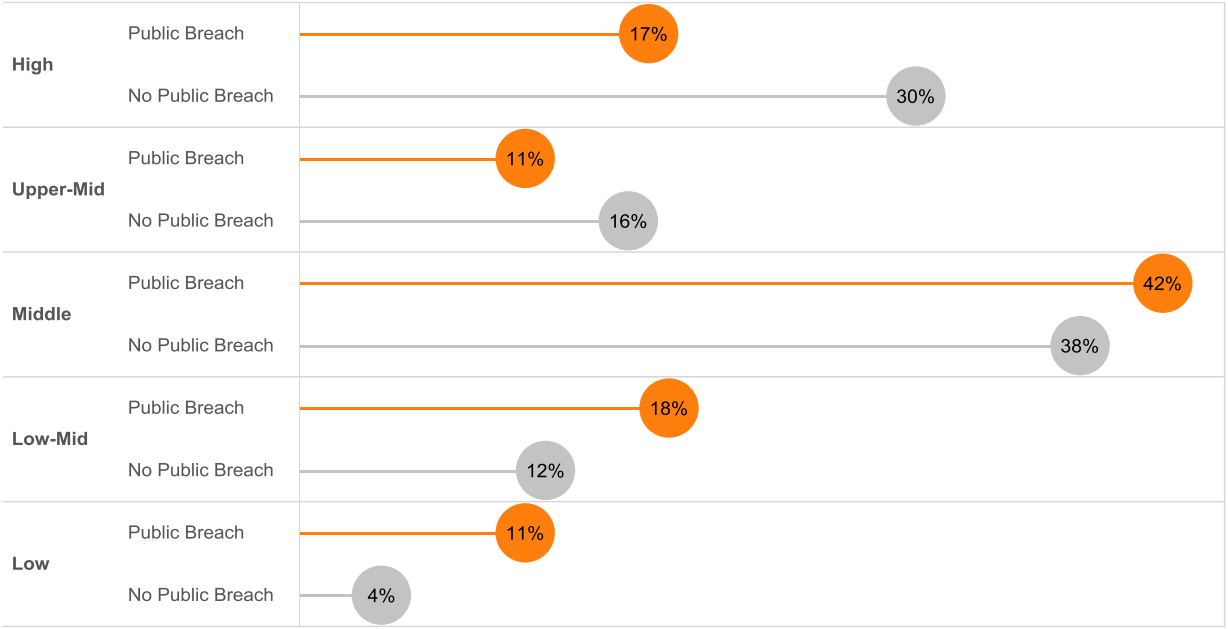
Without firm government standards for cybersecurity practices, organizations in Japan may be less likely to adopt practices that are more common in other countries. For instance, they are slightly less likely to have formal written security strategies that are reviewed regularly: 56 percent of Japanese organizations have them, compared with 60 percent in other countries. This may also be a result of the lack of clear definition of security roles and requirements at the executive level.

In addition, 45 percent of Japanese organizations follow a standardized information security policy practice such as ISO 27001, compared with 53 percent of organizations in all other countries. In Japan, organizations may not value the importance of such certifications because they don't play a role in stopping attacks or protecting organizations from cybercrime.

Publicly Breached Organizations Rank Lower in Sophistication

Japanese organizations that have suffered a public breach present a lower level of security sophistication. Twenty-eight percent of Japanese organizations that have dealt with a public data breach were classified as either upper-middle or high in terms of their security sophistication, while 46 percent of non-publicly-breached organizations were classed as upper-middle to high (Figure 9).

Figure 9. Level of Perceived Security Sophistication in Publicly Breached and Non-Publicly-Breached Japanese Firms



The level of sophistication can be related not only to how much an organization invests but, more importantly, to how it perceives the importance of security. This dynamic is more acute in publicly breached organizations. In general, many Japanese organizations do not yet see the importance of security, and this posture is reflected in their processes and policies. But publicly breached organizations in Japan tend to invest more in tools and to focus on bringing their systems up to date. For example, 73 percent of organizations that have dealt with a public breach believe their security infrastructure is up to date, while only 51 percent of non-publicly-breached companies believe their infrastructure is up to date. Public scrutiny apparently prompts some changes. However, changes to management structure, training, processes, and policies, which could lead to higher sophistication, take longer to implement.

Conclusion: Openness to Adopting Threat Defenses

In a country with a conservative approach to change, and with sensitivities around spending after years of slow growth, it is not easy to improve the security infrastructure. However, with threats on the rise, and with the world's attention turning to Japan in a few years as preparations for the 2020 Summer Olympics begin, now is the time for Japan's security community to bring about change.

According to a recent Gartner survey, 87 percent of the CIOs in Asia Pacific and Japan said that the digital world is creating new levels of risk, and 69 percent said that the discipline of risk management is not keeping up.[6] As products and systems relying on the Internet of Everything (IoE) become more popular, Japanese security professionals will have even more reasons to elevate their security sophistication and preparedness.

[6] "Gartner Survey Finds Digital Business Will Drive 75 Percent of CIOs in Asia/Pacific and Japan to Adapt Leadership by 2018," Gartner, March 18, 2015: http://www.gartner.com/newsroom/id/3008817

Organizations in Japan should:

- Understand that security is a business challenge, not only an IT challenge. Security breaches could affect revenue directly and also bring intangible damage to their brands and reputation. These breaches could also expose customers to risk, betraying the trust they place on their vendors.
- Place greater responsibility for security at the highest levels of the organization, which will demonstrate its value to all employees.
- Develop a more realistic view of security threats and the damage they can do to an organization's reputation.
- Allocate more money to expanding their portfolios of tools and processes that can protect networks from threats.

Learn More

To learn how to become more resilient to new attacks and compete more safely in the digital age, get the Cisco 2016 Annual Security Report at www.cisco.com/go/asr2016.

To learn about Cisco's comprehensive advanced threat protection portfolio of products and solutions, visit www.cisco.com/go/security.

About the Cisco 2014 Security Capabilities Benchmark Study

The Cisco 2014 Security Capabilities Benchmark Study examines defenders across three dimensions: resources, capabilities, and sophistication. The study includes organizations across several industries, in nine countries.

In total, we surveyed more than 1700 security professionals, including chief information security officers (CISOs) and security operations (SecOps) managers. We surveyed professionals in the following countries: Australia, Brazil, China, Germany, India, Italy, Japan, the United Kingdom, and the United States. The countries were selected for their economic significance and geographic diversity.

To read findings from the broader Cisco Security Capabilities Benchmark Study referenced in this paper, get the Cisco 2015 Annual Security Report at www.cisco.com/go/asr2015.

The latest version of the study is now available in the Cisco 2016 Annual Security Report: www.cisco.com/go/asr2016.

About This White Paper Series

A team of industry and country experts at Cisco analyzed the Cisco 2014 Security Capabilities Benchmark Study. They offer insight on the security landscape in nine countries and six industries (financial services, government, healthcare, telecommunications, transportation, and utilities). The white papers in this series look at the level of maturity and sophistication of the survey respondents and identify the common elements that indicate higher levels of security sophistication. This process helped contextualize the findings of the study and brought focus to the relevant topics for each industry and market.

About Cisco

Cisco delivers intelligent cybersecurity for the real world, providing one of the industry's most comprehensive advanced threat protection portfolios of solutions across the broadest set of attack vectors. Cisco's threat-centric

and operationalized approach to security reduces complexity and fragmentation while providing superior visibility, consistent control, and advanced threat protection before, during, and after an attack.

Threat researchers from the Collective Security Intelligence (CSI) ecosystem bring together, under a single umbrella, the industry's leading threat intelligence, using telemetry obtained from the vast footprint of devices and sensors, public and private feeds, and the open-source community at Cisco.

This intelligence amounts to a daily ingestion of billions of web requests and millions of emails, malware samples, and network intrusions. Our sophisticated infrastructure and systems consume this telemetry, enabling machine-learning systems and researchers to track threats across networks, data centers, endpoints, mobile devices, virtual systems, web, email, and from the cloud to identify root causes and scope outbreaks. The resulting intelligence is translated into real-time protections for our products and services offerings that are immediately delivered globally to Cisco customers.

The CSI ecosystem is composed of multiple groups with distinct charters: Talos, Security and Trust Organization, Active Threat Analytics, and Security Research and Operations.

To learn more about Cisco's threat-centric approach to security, visit www.cisco.com/go/security.

Americas Headquarters
Cisco Systems, Inc.
San Jose, CA

Asia Pacific Headquarters
Cisco Systems (USA) Pte. Ltd.
Singapore

Europe Headquarters
Cisco Systems International BV Amsterdam,
The Netherlands

Cisco has more than 200 offices worldwide. Addresses, phone numbers, and fax numbers are listed on the Cisco Website at **www.cisco.com/go/offices.**

Printed in USA 11/15