White Paper

United States: Security Maturing into a Growth Enabler and a Competitive Advantage

Cybersecurity is one of the most significant challenges to the United States' economic and national security.[1] Cybercrime goes beyond data theft. Cyberespionage, hacktivism, and cyberterrorist attacks to critical national infrastructure raise deep concerns in the country.

The global economic landscape is complex, and the United States faces increasing competition from emerging economies. Strong security can support the country's long-term growth. It helps U.S. organizations to protect their most valuable data and be more confident about the integrity of their systems. From a government perspective, security is also about sovereignty and peace of mind for its citizens.

Major Findings

In this paper, Cisco experts analyze the IT security capabilities of organizations in the United States, using data from the Cisco 2014 Security Capabilities Benchmark Study.[2] We found that:

- U.S. organizations outsource security services more than those in the other countries we studied. This strategy may help them to reduce costs while improving efficiency. It may also reflect the shortage of security professionals available for hire in the country.
- U.S. organizations use more processes to analyze compromised systems and eliminate the causes of security incidents than do businesses in other nations. The use of more processes may indicate that U.S.

[1] "The Comprehensive National Cybersecurity Initiative," The White House: https://www.whitehouse.gov/issues/foreign-policy/cybersecurity/national-initiative.
[2] For more information on this study and the other white papers in this series, see the final pages of this document.

organizations have a better understanding of the full attack continuum than do organizations in other countries.

- U.S. businesses report dealing with fewer public data breaches than their non-U.S. counterparts. The lack of reporting requirements in the United States may contribute to this difference.

Fighting One of the Biggest Threats to Economic and National Security

The United States is the world's largest economy, with an estimated GDP of $18 trillion.[3] The country has a strong international presence, both culturally and diplomatically. However, companies that want to invest in the country or maintain their headquarters in the United States face several barriers. High labor costs, an increasingly complex regulatory environment, and burdensome corporate taxes may make the U.S. less attractive than emerging countries, especially for multinational firms.

Although it is increasingly difficult to compete on costs, the U.S. offers a supportive environment for research, development, and innovation. Therefore, U.S. organizations must be able to protect their data and assets in order to maintain their competitive edge. In this sense, security may enable economic growth.

The White House calls cybersecurity "one of the most serious economic and national security challenges we face as a nation, but one that we as a government or as a country are not adequately prepared to counter."[4] Cyberespionage, including the theft of patents and intellectual property, and cyberattacks funded by nation-states are real concerns for U.S. businesses and government entities. In 2015, the U.S. Office of Personnel Management reported a data breach that affected about 22 million people. It is possibly the largest U.S. government hack to date.[5] Attacks against critical infrastructure could also pose a threat to the nation's economy and citizens.

In a response to these threats, both public and private sectors are increasing their defenses and improving collaboration. The recently passed Cybersecurity Information Sharing Act (CISA) encourages companies to share threat information with one another and with the government.

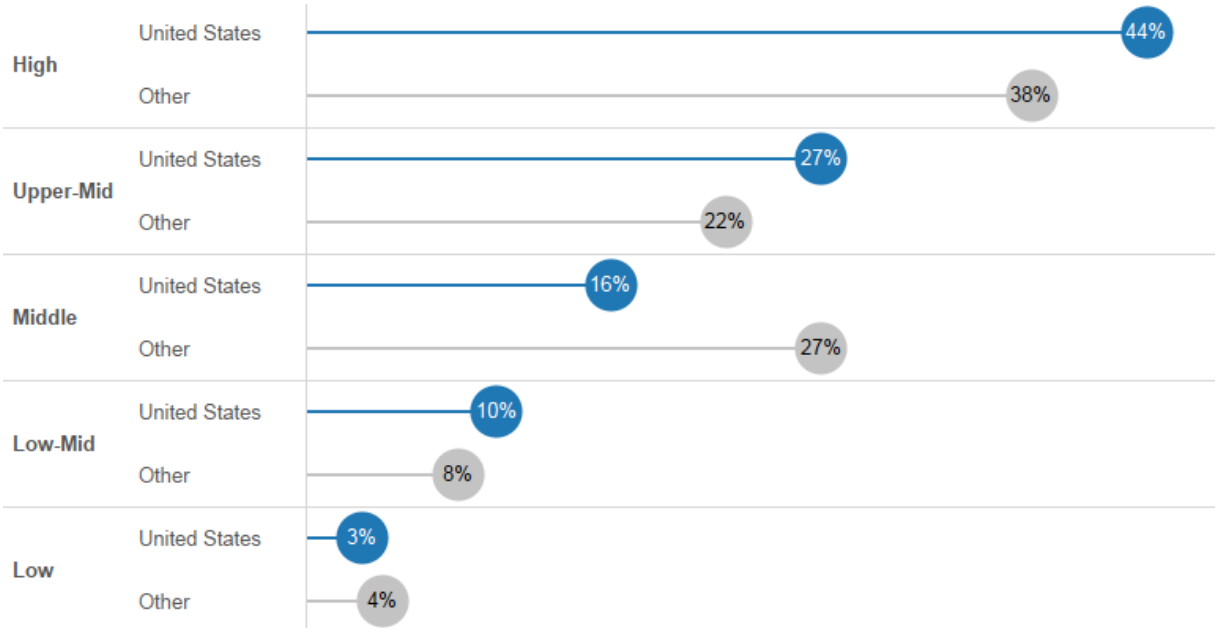
In general, the United States has stronger defenses than other countries, but the overall numbers from our study show there is still room for improvement. U.S. organizations have to change their perception of security and accept it as an ongoing necessity. It should be built into all business processes and aligned to business objectives. In this way, it can help protect the country's competitive edge.

U.S. Organizations Lead in the Use of Security Threat Defenses, But Not in the Use of Cloud-Based Solutions

Based on the responses of security professionals to our study, we categorized 71 percent of U.S. organizations as either "upper middle" or "high" in terms of their security sophistication. In other countries, this figure is 60 percent (Figure 1).

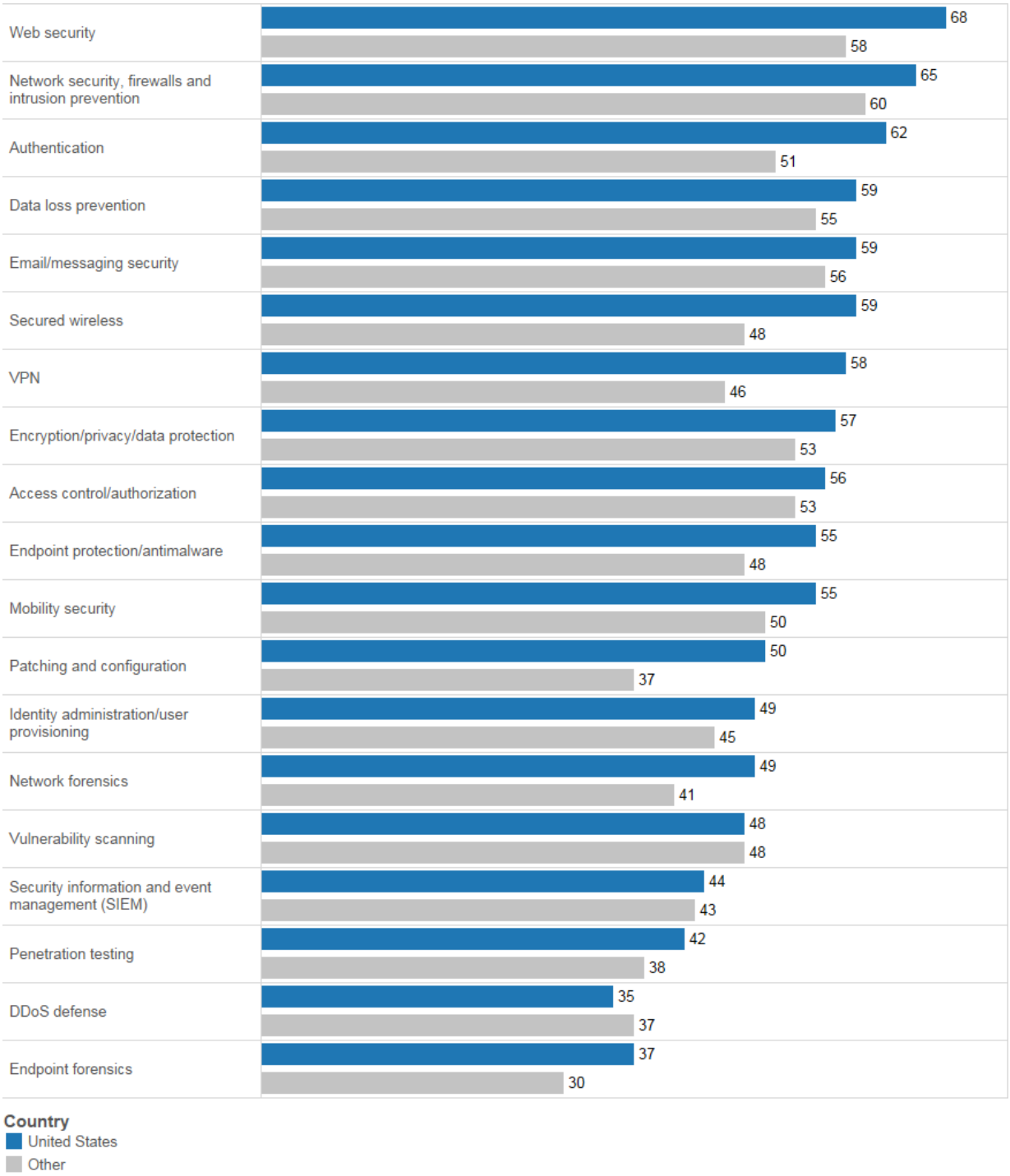
[3] "World Largest Economies," *CNN Money*: http://money.cnn.com/news/economy/world_economies_gdp/.
[4] "The Comprehensive National Cybersecurity Initiative," The White House: https://www.whitehouse.gov/issues/foreign-policy/cybersecurity/national-initiative.
[5] "About Those Fingerprints Stolen in the OPM Hack," The Atlantic, September 23, 2015: http://www.theatlantic.com/technology/archive/2015/09/opm-hack-fingerprints/406900/.

Figure 1. Security Sophistication Levels in the U.S. and Other Countries, by Percentage of Organizations



In general, U.S. organizations use more threat defenses than non-U.S. organizations (Figure 2). Web security is one area in which U.S. organizations show the greatest advantage over other countries. Sixty-eight percent of U.S. businesses report that they employ this type of solution; 58 percent of non-U.S. organizations do. Other areas in which U.S. organizations are ahead of other countries by more than 10 percent are authentication, secured wireless, and VPN.

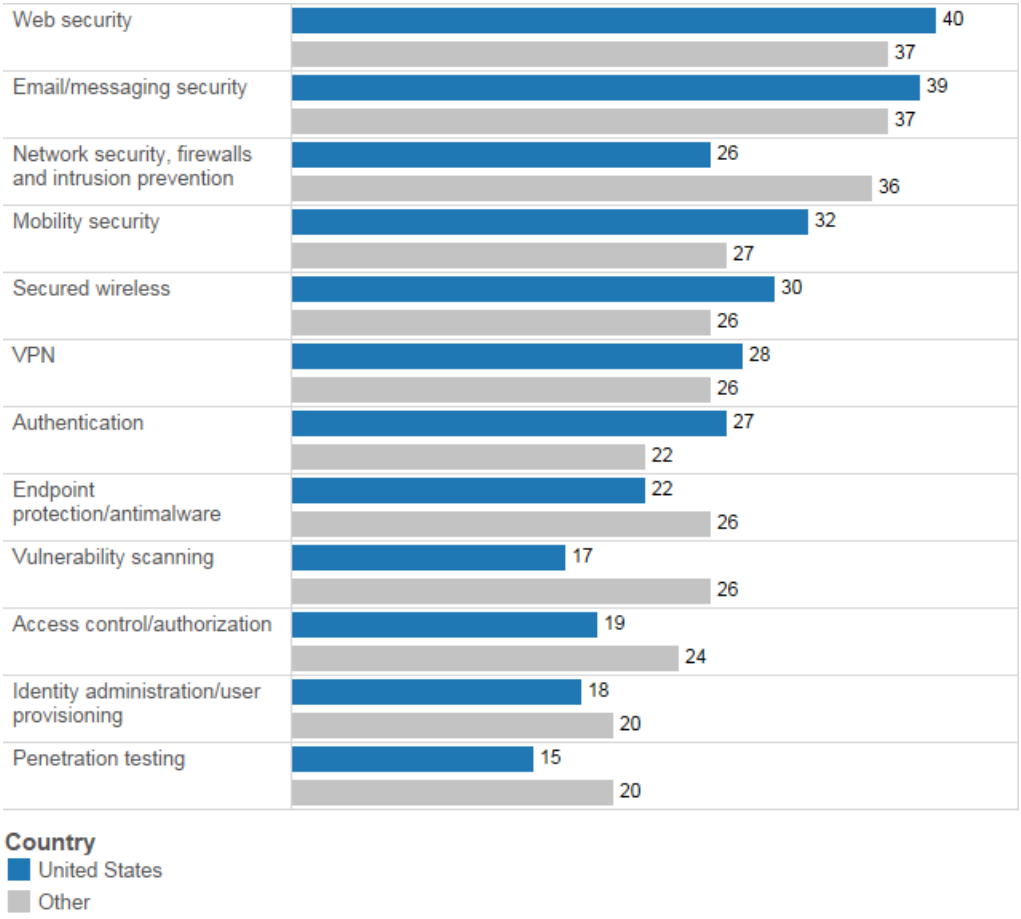
Figure 2. Percent of U.S. and Non-U.S. Organizations Using Various Threat Defenses



Although the United States leads other nations in the use of threat defenses, its overall use of cloud-based security solutions is at level similar to or less than that of other nations. Organizations in this country may have already invested in security solutions on-premises. In that case, adopting cloud solutions may involve a migration of data. The effort needed to migrate data could delay the process or inhibit some organizations from making the transition.

The most significant difference is in the use of cloud-based solutions for network security, firewalls, and intrusion prevention: 36 percent of non-U.S. organizations use this technology, but only 25 percent of U.S. businesses do. Vulnerability scanning had a similar margin of difference: 26 percent of non-U.S. businesses use a cloud-based solution for this process, but only 17 percent of U.S. organizations do (Figure 3).

Figure 3. Percentages of U.S. and Non-U.S. Organizations Using Various Cloud-Based Security Threat Defenses

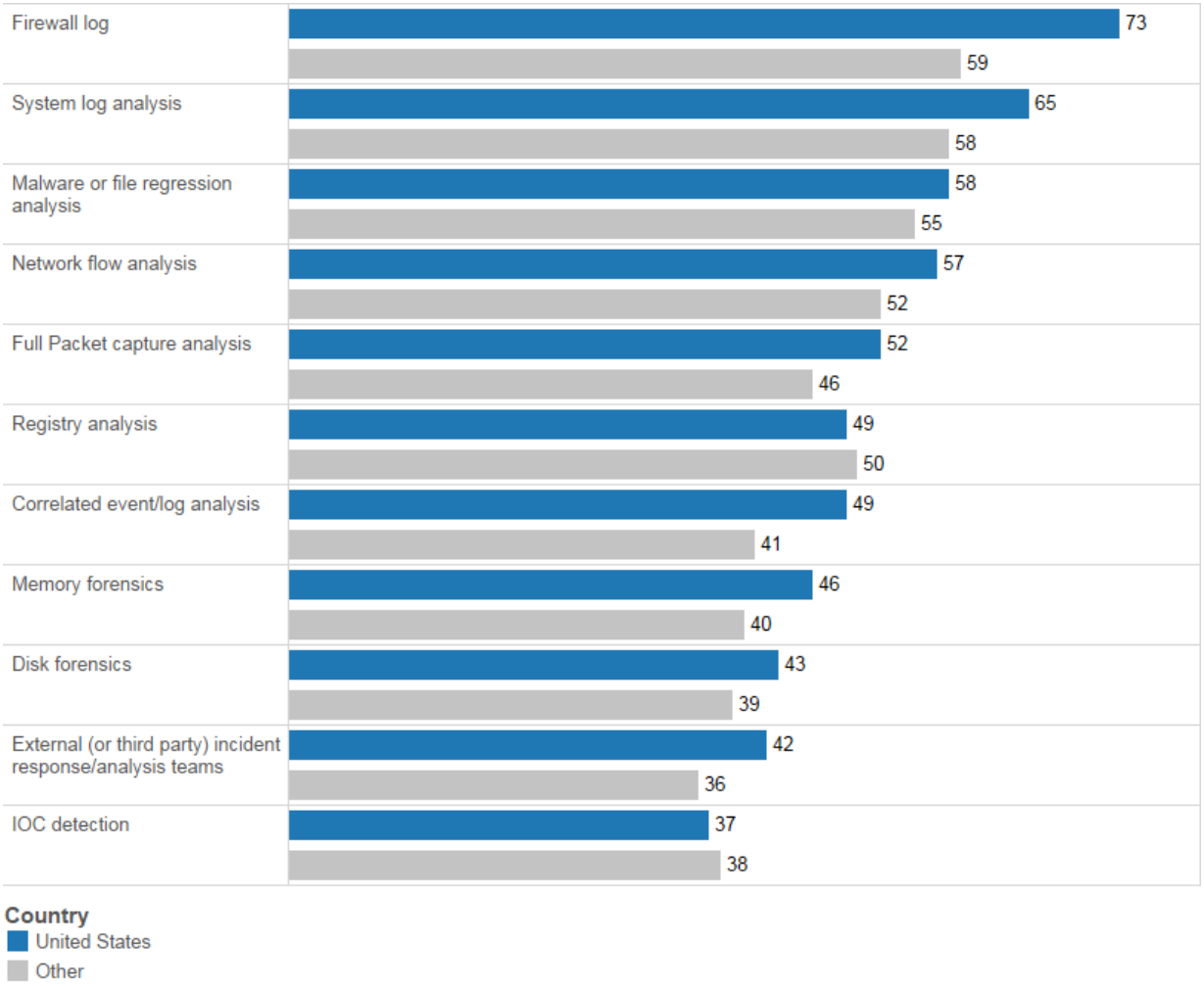


Despite positive comparative results, the overall adoption of threat defenses by U.S. organizations can still be improved. It currently ranges from 37 percent to 68 percent (Figure 2). For example, 35 percent of U.S. organizations do not have network security, firewalls, and intrusion prevention tools, which are considered basic defense tools.

U.S. Organizations Lead in the Adoption of Most Security Processes

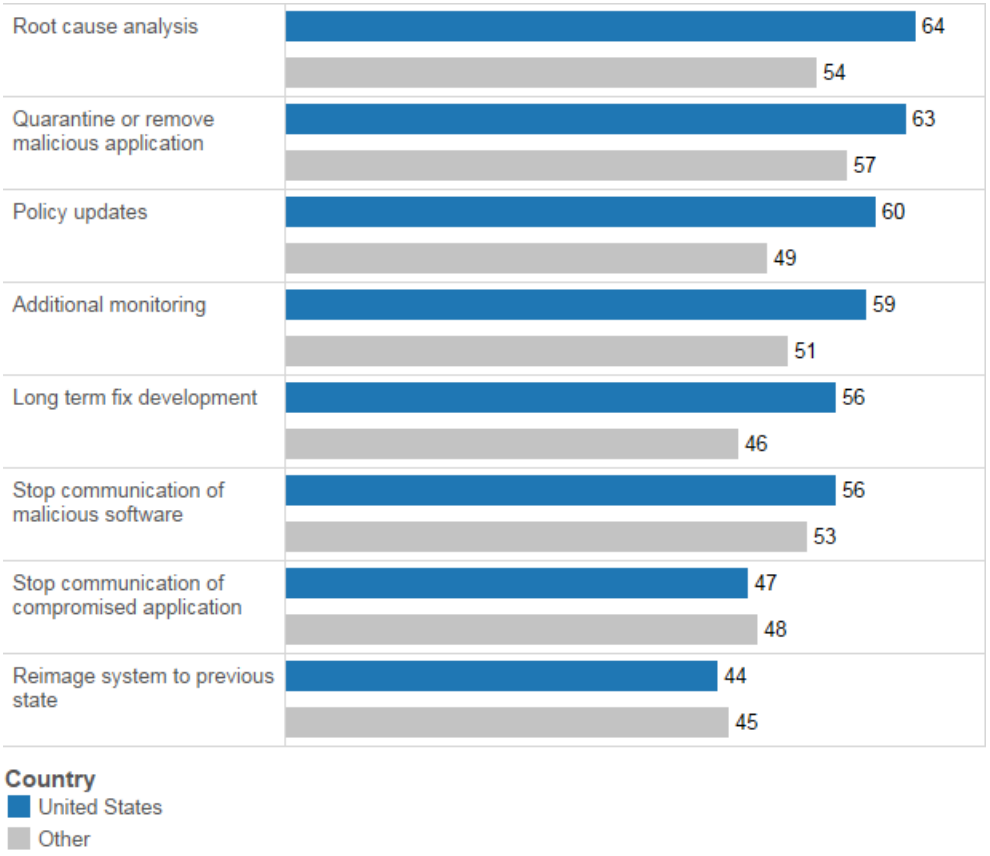
When it comes to security processes, U.S. organizations seem to be ahead of other countries on many fronts. For example, U.S. organizations appear to be using more processes to analyze compromised systems than do businesses in other nations. As Figure 4 shows, a significantly higher percentage of U.S. businesses (73 percent) use firewall logs than do businesses in other countries (59 percent). However, the United States lags slightly behind other nations in the use of processes such as registry analysis and indicator of compromise (IOC) detection.

Figure 4. Percentages of U.S. and Non-U.S. Organizations Using Selected Processes to Analyze Compromised Systems



Additionally, we found that U.S. organizations use more processes to eliminate the causes of security incidents than do their counterparts in other countries (Figure 5). In particular, they appear to be much more likely to use policy updates than non-U.S. businesses: 60 percent compared with 49 percent. Reimaging a system to its previous state and stopping the communication of compromised applications are the only two processes where the use by non-U.S. businesses appears to be similar to that of U.S. organizations.

Figure 5. Percentages of U.S. and Non-U.S. Organizations Using Selected Processes to Eliminate the Causes of Security Incidents



U.S. organizations are also significantly more likely (42 percent) than those in other countries (34 percent) to use gold image restoration to restore affected systems to pre-incident levels. They are generally on a par with businesses in other countries in their use of other processes for system restoration.

In addition to restoring systems, companies should also apply the intelligence they gather after an attack to improve their defenses. Having well-though-out processes also supports a more effective use of threat defense tools.

All these findings regarding security processes suggest that many U.S. companies are on the right path to protecting themselves against the full attack continuum. Many seem to understand that robust security practices go beyond attempting to stop every threat. Instead, they appear to assume they may be breached and are preparing plans to detect and mitigate damages.

However, despite the positive comparative results, the overall adoption of processes by U.S. organizations falls below 65 percent. (One exception, as seen in Figures 4 to 6, is firewall logs, which 73 percent of organizations use.) Some processes, such as IOC detection, rank as low as 37 percent. Clearly, many U.S. organizations still have to work on improving their security capabilities.

Publicly Breached U.S. Organizations Use DDoS Defenses More Than Non-Publicly-Breached Organizations

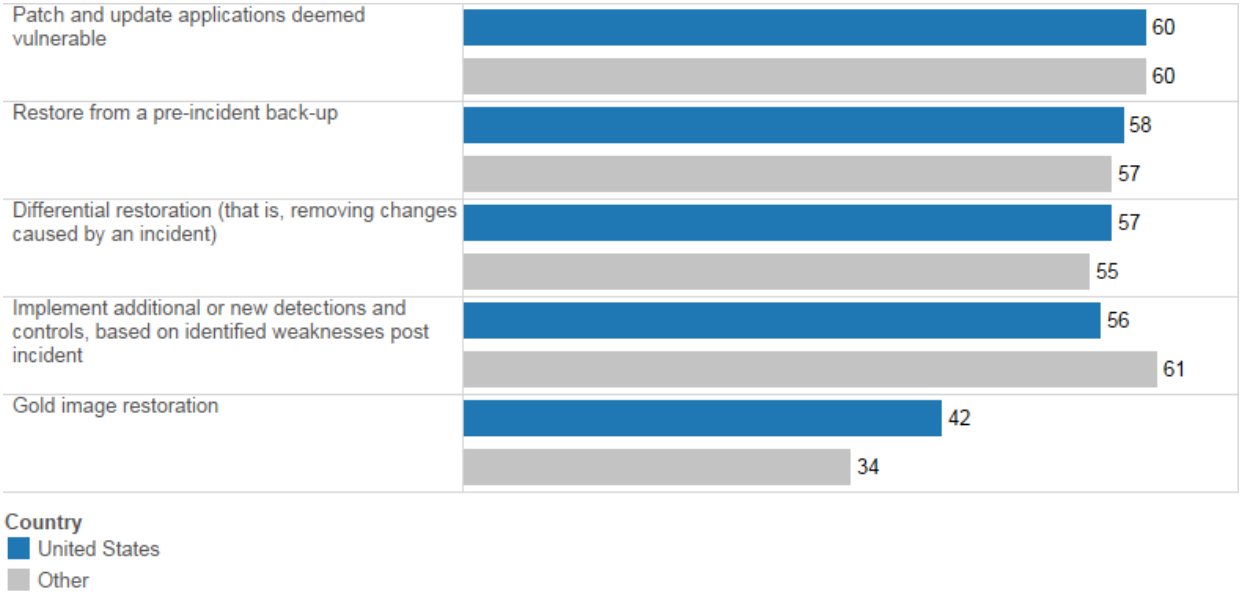
Fewer U.S. organizations (44 percent) report dealing with data breaches that have led to public scrutiny than do their counterparts in other countries (55 percent). However, this gap may not be an indication that U.S. organizations are, in fact, experiencing fewer security breaches.

Two important dynamics are at work: First, some U.S. businesses may not report security breaches. Many industries and states do not mandate disclosure, so companies may avoid reporting a breach because they fear the impact on their reputation. Moreover, the lack of a uniform way to report security breaches in the United States also makes it difficult for organizations that want to, or have to, share information. Legislative changes aim to address the latter. The Cybersecurity Information Sharing Act of 2015 (CISA), passed by the U.S. Congress in October 2015, provides incentives for companies to share information about "cyber threat indicators" with federal law enforcement.[6]

The second dynamic is the shortage of skilled security professionals. U.S. businesses may not have adequately staffed security teams. When that is the case, reporting a breach may not take priority.

Another effect of the lack of in-house security personnel is that U.S. organizations' rely more on third-party experts for security services. Only 17 percent of U.S. companies handle all security requirements internally. Outside the United States, 22 percent of companies do so. U.S companies use outside resources more than other countries for advice and consulting, auditing, and monitoring (Figure 6).

Figure 6. Percentages of U.S. and Non-U.S. Organizations That Outsource Various Security Services



U.S. organizations will continue to struggle to find skilled security and IT talent to manage increasingly sophisticated tools and processes. The enactment of CISA, and the regulatory demands around data privacy and security, will likely impel U.S. businesses to engage more third-party security experts in the future.

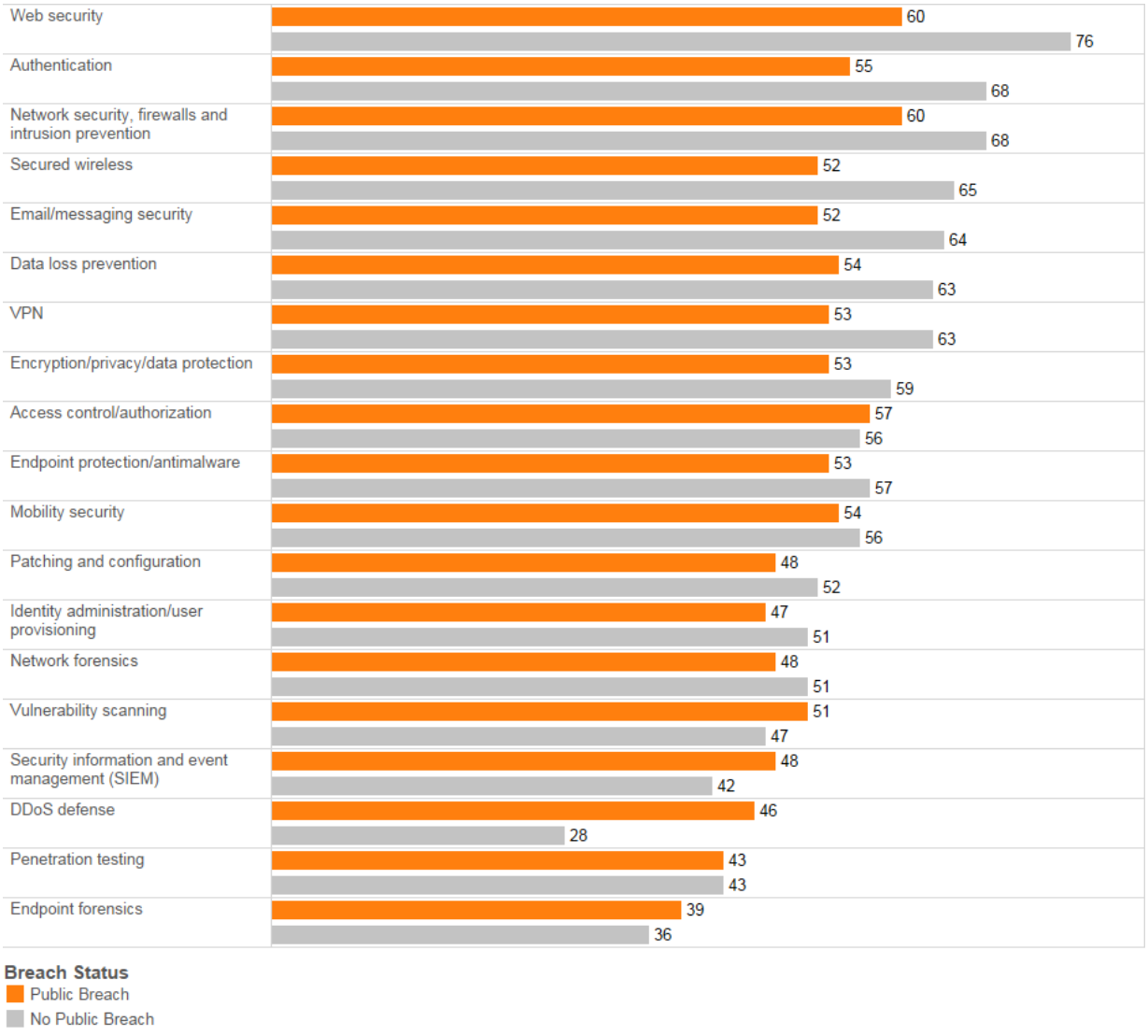
Interestingly, we found that a public breach does not seem to influence the use of threat defenses in U.S. organizations. Unlike the U.S., most other countries we studied presented a pattern. For some, a public breach resulted in a greater adoption of certain tools. For others, publicly breached companies seemed to use fewer tools.

[6] "S.754 – Cybersecurity Information Sharing Act," 114th U.S. Congress, October 2015: https://www.congress.gov/bill/114th-congress/senate-bill/754.

There are two statistically significant exceptions among U.S. organizations: distributed denial of service (DDoS) defense and web security (Figure 7). Publicly breached organizations in the U.S. report a much higher use of DDoS defense solutions (46 percent) than do non-publicly-breached businesses (28 percent). Businesses that have endured a public breach probably take care to strengthen their DDoS defenses first as a way to avoid future public exposures and to protect their customers. DDoS attacks tend to be high profile. They can also be extremely disruptive and often conceal the theft of data or funds.

Web security, however, shows the opposite trend. Seventy-six percent of non-publicly-breached organizations in the United States use web security tools, but only 60 percent of publicly breached organizations do.

Figure 7. Percent of U.S. Organizations Using Various Security Threat Defenses, by Public Breach Status

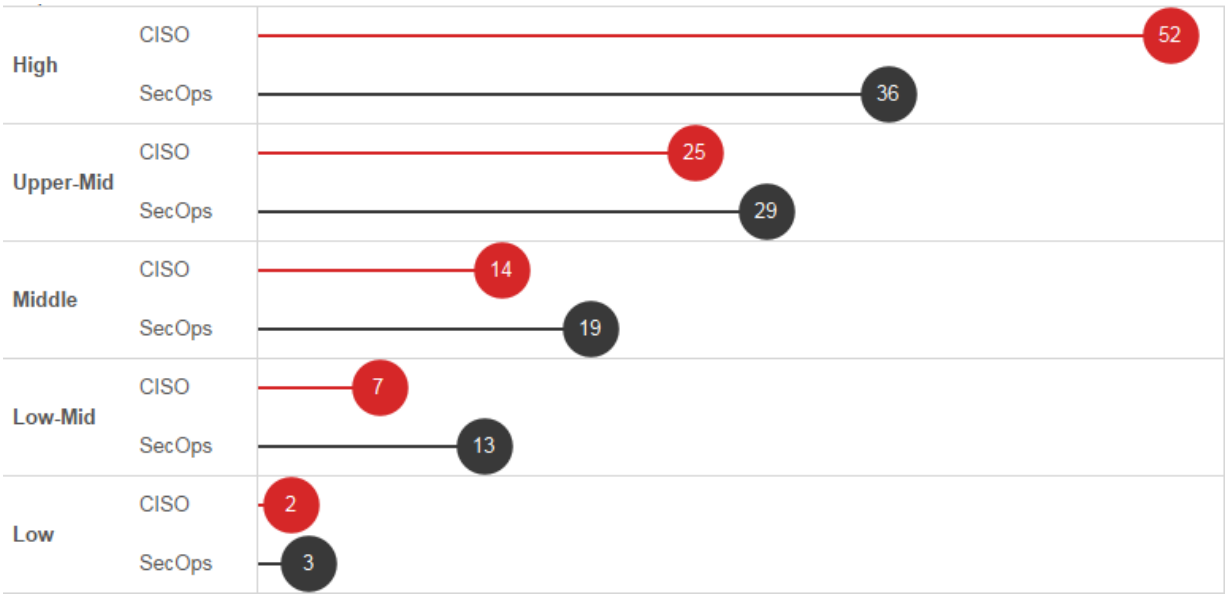


CISOs and SecOps: Significant Gaps in Perceptions About Security Sophistication

Chief information security officers (CISOs) and security operations (SecOps) managers working at U.S. organizations are not aligned in their perceptions about their organization's level of security sophistication. CISOs

are far more optimistic in their assessment. Seventy-seven percent of these security professionals were mapped as either “upper middle” or “high” in their perceptions of security sophistication, but only 64 percent of SecOps managers were (Figure 8).

Figure 8. Perception of Security Sophistication in U.S. Organizations, by Role



We attribute the lack of alignment largely to the nature of their roles. CISOs focus their attention on the overall security strategy for the organization and are likely to take a “big picture” view of cybersecurity risks. SecOps managers deal directly with the day-to-day “firefighting” of security threats.

A general lack of communication between these security professionals, which we found to be typical in organizations across countries and industries, may exacerbate the difference in perceptions. Better communications between CISOs and SecOps managers could help reduce the gap. This change could also lead to a more realistic outlook of the organization’s state of security.

Recommendations for Improving Security Sophistication

This paper shows that U.S. organizations seem to have stronger security capabilities than those in other countries. However, when analyzing the numbers by themselves, without drawing comparisons, we notice that the figures are all quite far from 100 percent. Many companies seem to be on the right path, but others lack strong defenses. Still, all companies must accept that security requires an ongoing commitment, regardless of the tools and processes they have in place now. In addition, they must consider all aspects of security—before, during, and after an attack. Assuming that a breach will happen at some point may prompt companies to adopt a more proactive approach.

U.S. businesses looking to achieve higher levels of security sophistication should, among other things, deepen their understanding of their security environment. They will benefit from understanding the specific risks in their industry and their businesses, including what data they need to protect most. Such a self-evaluation will help them develop more targeted security initiatives. Companies will be better prepared when they accept the dynamic nature of security threats and consider security as an enabler of business growth.

U.S. organizations that exhibit high levels of security maturity share certain characteristics. Businesses that wish to join their ranks should take note of these three in particular:

- Nearly all (91 percent) of the security personnel in highly sophisticated organizations report that the security tools they use for detecting network anomalies and dynamically defending against shifts in adaptive threats are either “extremely effective” or “very effective.” Less than half (42 percent) of the personnel in less sophisticated organizations report their tools to be that effective.
- Nearly all (94 percent) of the security personnel in highly sophisticated organizations report that the security tools they use to enforce security policies are either “extremely effective” or “very effective.” This figure drops to 51 percent when respondents are from less sophisticated organizations.
- Nearly three-quarters of security personnel (74 percent) from highly sophisticated organizations strongly agree that their business is doing a good job of building security into procedures for acquiring, developing, and maintaining systems and applications. This figure is only 45 percent in less sophisticated organizations.

U.S. businesses should also consider taking the following actions to improve their overall security posture:

- Focus on user education, and invest more in training for in-house security and IT personnel. Both of these can help improve cybersecurity over the long term.
- Increase integration between the security and IT teams, and between the security team and the business. Security should not be an afterthought but designed and embedded into everything the organization does.
- Understand the organization’s security environment in order to develop more targeted and effective security initiatives. Know what data the business has. Segment and classify it. The security team can then focus on protecting what is most important.
- Consider more outsourcing of complex security tasks. As the study findings show, U.S. organizations look to outside resources primarily for services such as advice and consulting and auditing. Less than half of these businesses outsource security monitoring, and even fewer look to third-party experts for incident response and remediation.
- Recognize that security is an enabler of business growth. U.S. organizations should work to establish a clear link between business goals and the security needed to achieve those objectives. CISOs can play an important role in helping to elevate the importance of cybersecurity in the organization.
- Prepare to act after a breach has occurred. For example, draft an incident response strategy and adopt more forensics tools. This precaution may help organizations reduce the effect of a security breach as well as gather intelligence to strengthen their defenses and avoid future breaches.

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 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