White Paper

Government: Strengthening Defenses and Adopting a Framework for Collaboration

Government organizations are at high risk of cyber attacks. Cyberterrorists, hacktivists, and other criminals aim not only to disrupt public services but also to retrieve critical and confidential data that can be used for political or financial gain. In addition, many governments are increasing their online services to citizens in the interest of austerity, efficiency, and transparency. The impact of any attack on citizens and the economy could be significant and long-lasting.

Most government organizations understand these risks and are focused on strengthening their defenses. Despite this commitment, however, the sector's security sophistication is at a level similar to that of other industries.

- Government agencies and the military are known for their disconnected operations among departments and divisions. Their complex and often inflexible organizational structure makes it difficult for them to streamline processes and share information effectively.
- Greater collaboration—throughout various levels of government, between public and private entities, and across borders—could make the sector more secure overall. The adoption of a common cybersecurity framework, and the implementation of trusted systems, could enable this type of collaboration.

Major Findings

In this paper, Cisco experts analyze the IT security capabilities of the government sector of nine countries, using data from the Cisco Security Capabilities Benchmark Study.[1] We surveyed security professionals in Australia, Brazil, China, Germany, India, Italy, Japan, the United Kingdom, and the United States. In our analysis we have found that:

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

- Government organizations are at a similar level of security sophistication as organizations in other sectors. This is the case even though government bodies use more threat defenses and more processes to analyze compromises, eliminate the causes of incidents, and restore systems to pre-incident levels.
- Government organizations use more cloud-based solutions than their counterparts in other sectors, especially if they have suffered a public data breach.
- Public scrutiny following a data breach appears to be a strong motivator for government entities to increase their threat defenses.
- Government organizations that have a high level of security maturity share several characteristics. Among them is the perception by security personnel that they have highly effective tools for detecting network anomalies and for dynamically defending against shifts in threats.
- The government sector, compared to other sectors in the study, relies more heavily on outsourced security services.

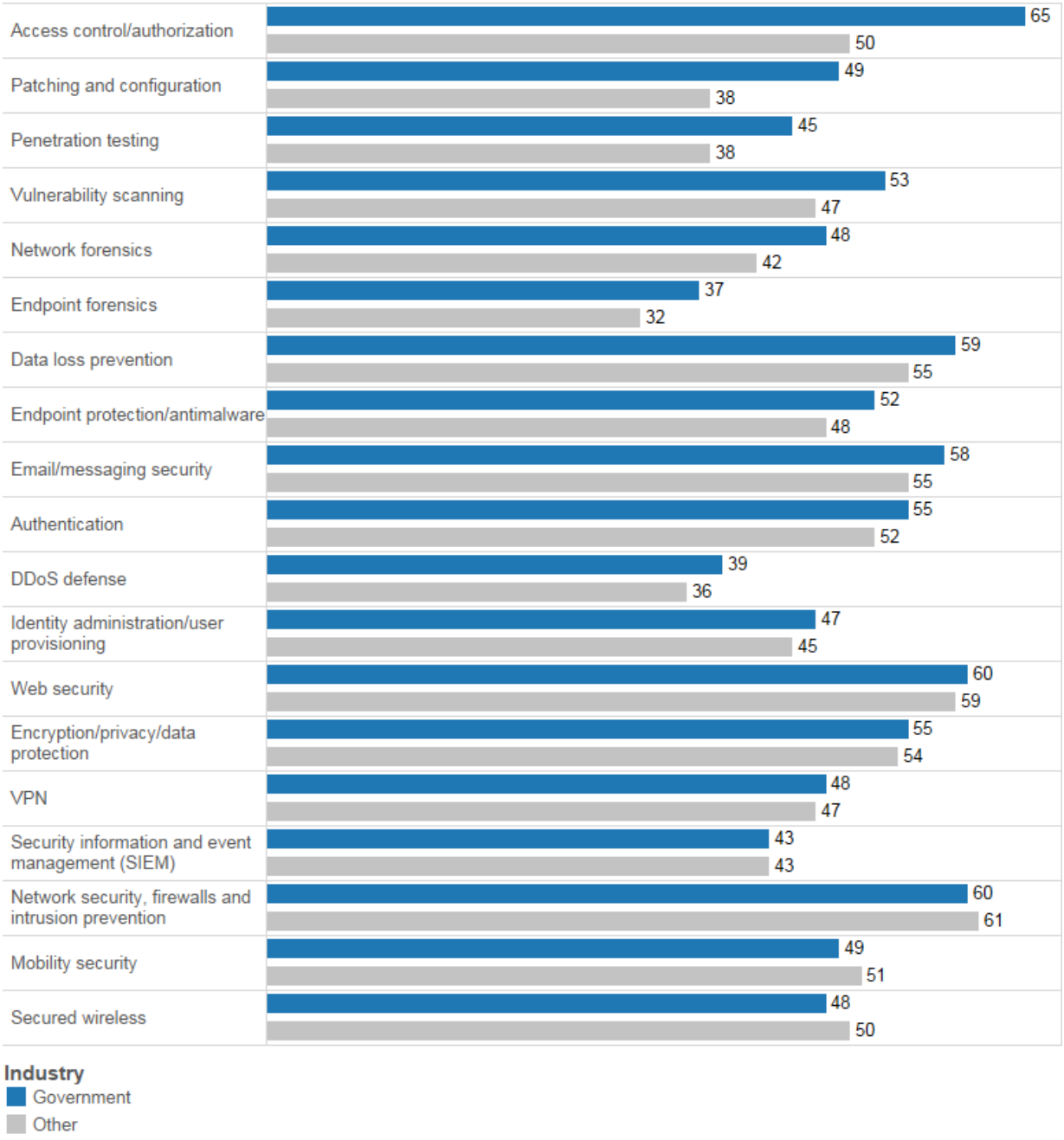
Government Organizations Are More Strongly Equipped with Threat Defenses

Government entities outpace nongovernment businesses in their use of almost every type of threat defense we analyzed (Figure 1). However, the average across all sectors is low. Therefore, despite this apparent advantage, there is still room for improvement.

For example, government organizations use access control and authorization solutions significantly more than organizations in other industries: 65 percent versus 50 percent. And nearly half (49 percent) of government organizations use patching and configuration tools, compared with only 38 percent of nongovernment organizations. But when looking at the government figures in isolation, there is still a large gap to be filled, with 35 percent not using any access control and authorization solutions, and 51 percent not using patching and configuration products.

It is important to note that the governments we analyzed take different approaches to cybersecurity. There are disparities in budgets, security laws, privacy laws, and the perceived risk of cyberterrorism and other attacks. There are also great differences between the resources of local and central governments. These factors are likely to influence each country's level of investment in security and also the types of solutions they adopt.

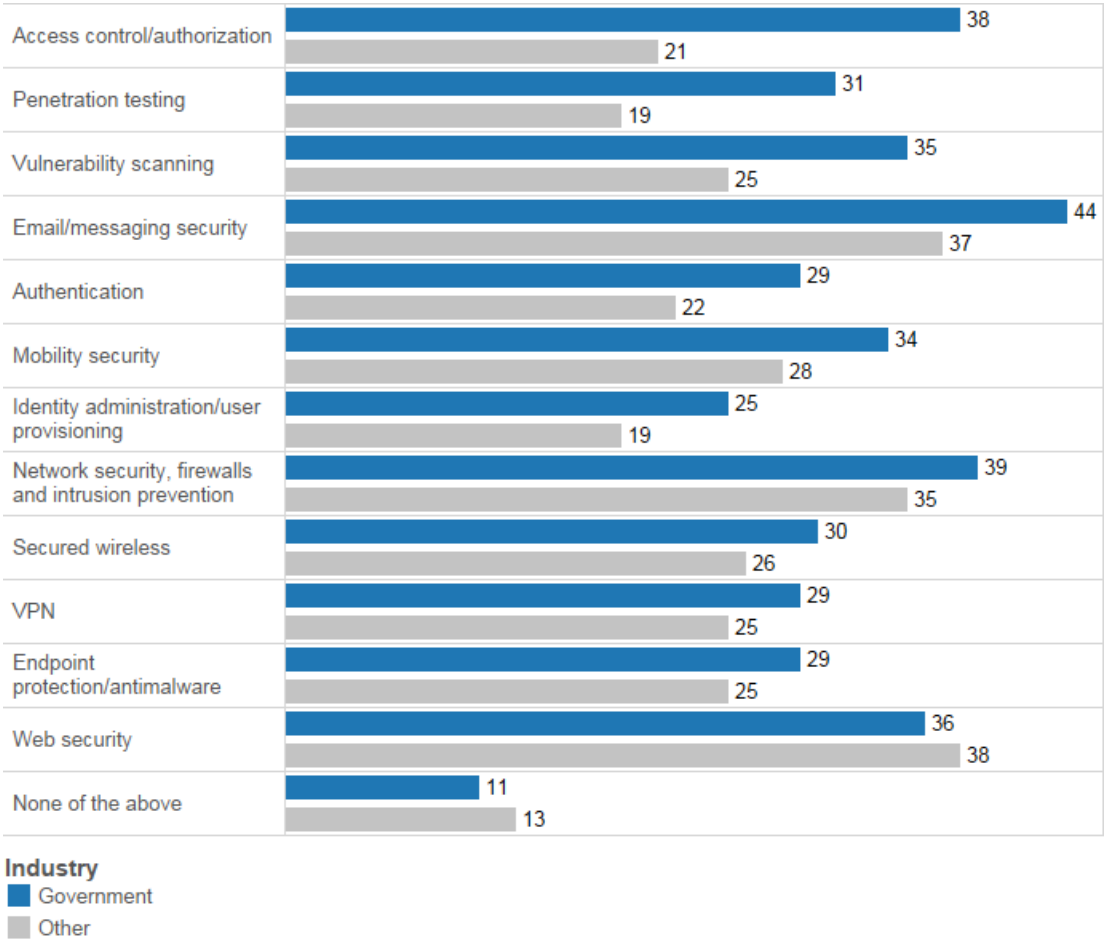
Figure 1. Percentages of Organizations Using Various Types of Security Defenses



The government sector is on a par with other sectors in its use of security information and event management (SIEM). It lags only slightly in three areas: network security, firewalls, and intrusion prevention; mobility security; and secured wireless.

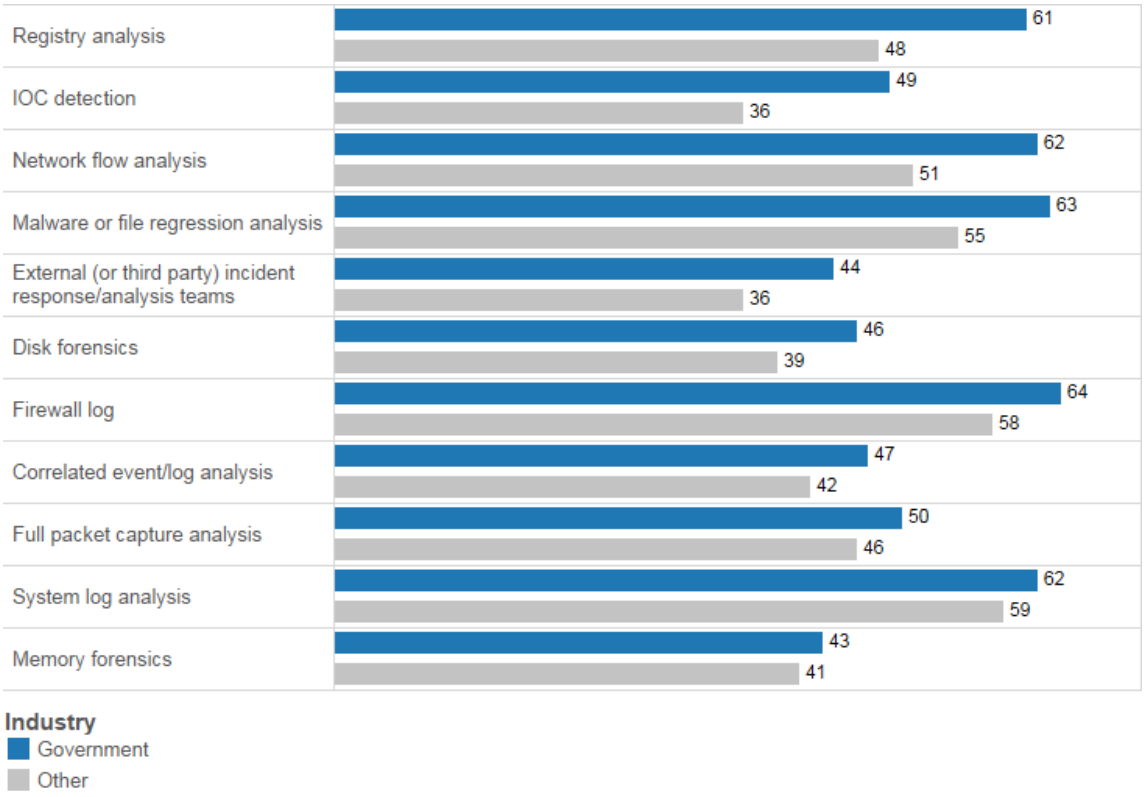
Government entities are also using cloud-based threat defenses more than the other sectors represented in our study. For example, 38 percent of government organizations say they use cloud-based solutions for access control and authorization, while only 21 percent of nongovernment businesses report using this specific defense measure (Figure 2).

Figure 2. Percentages of Organizations Using Cloud-Based Security Defenses



The study also found that governments tend to use more processes to analyze compromised systems and eliminate causes of security incidents than other sectors (Figure 3). For instance, government entities are far more likely to use processes such as registry analysis, indicator of compromise (IOC) detection, and network flow analysis than nongovernment businesses. They are also more likely to turn to third-party resources for assistance.

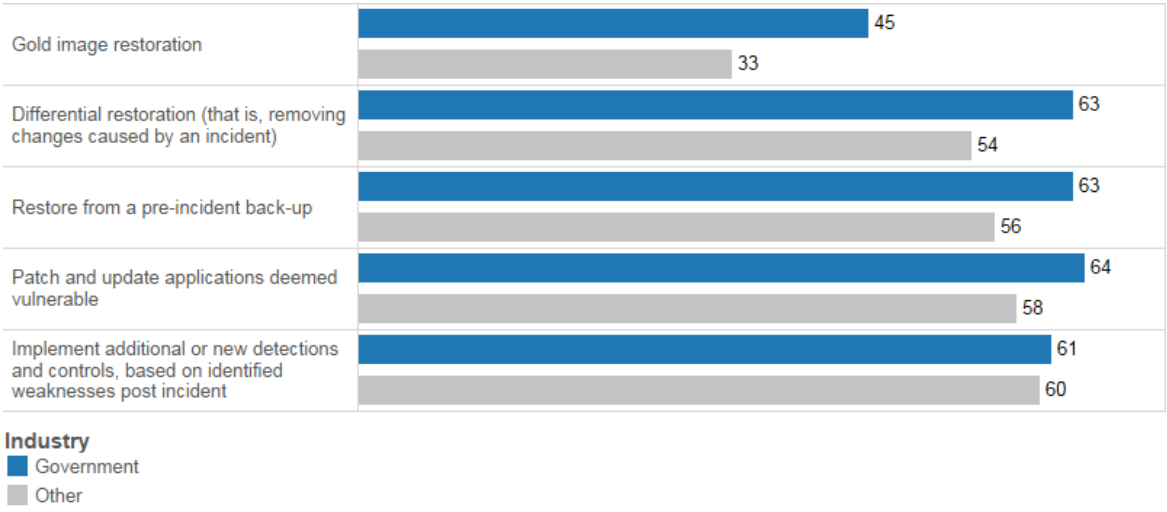
Figure 3. Percentages of Organizations Using Various Processes to Analyze Compromised Systems



Government organizations also use more processes to restore affected systems to pre-incident levels (Figure 4). For instance, nearly half (45 percent) of government entities use gold image restoration, while one-third (33 percent) of businesses in other sectors use this process. In addition, our study found that the government sector relies on differential restoration (removing changes caused by a security incident) significantly more than other sectors.

But again, as we saw with threat defense tools, the use of more processes by governments does not mean that they are in an ideal position. Their use of processes to analyze compromised systems (Figure 4), for example, ranges from 45 percent to 64 percent, which shows there is still an opportunity for improvement.

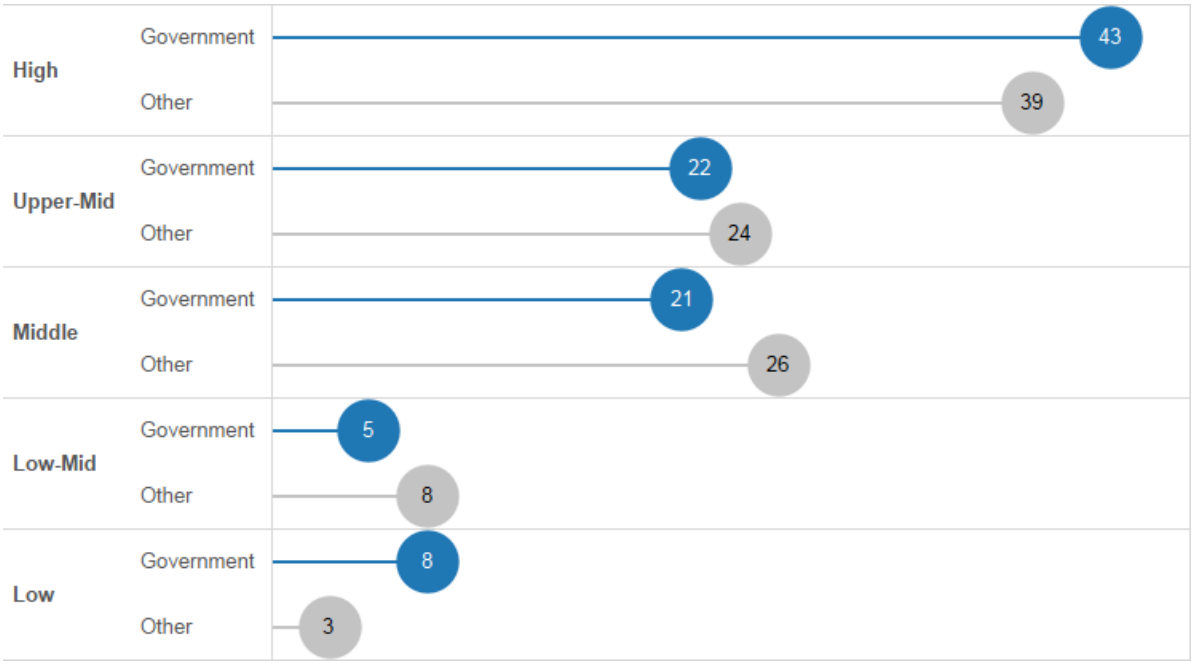
Figure 4. Percentages of Organizations Using Various Processes to Restore Affected Systems



Security Sophistication Similar to That of Other Industries, Despite More Tools and Processes

Although the government sector surpasses other sectors in its use of tools and processes for cybersecurity, its overall security sophistication is essentially at the same level. We categorized 65 percent of government organizations as either “upper middle” or “high” in terms of their security sophistication, and we mapped 63 percent of nongovernment businesses to those categories (Figure 5).

Figure 5. Levels of Security Sophistication in Government and Nongovernment Organizations, by Percentage

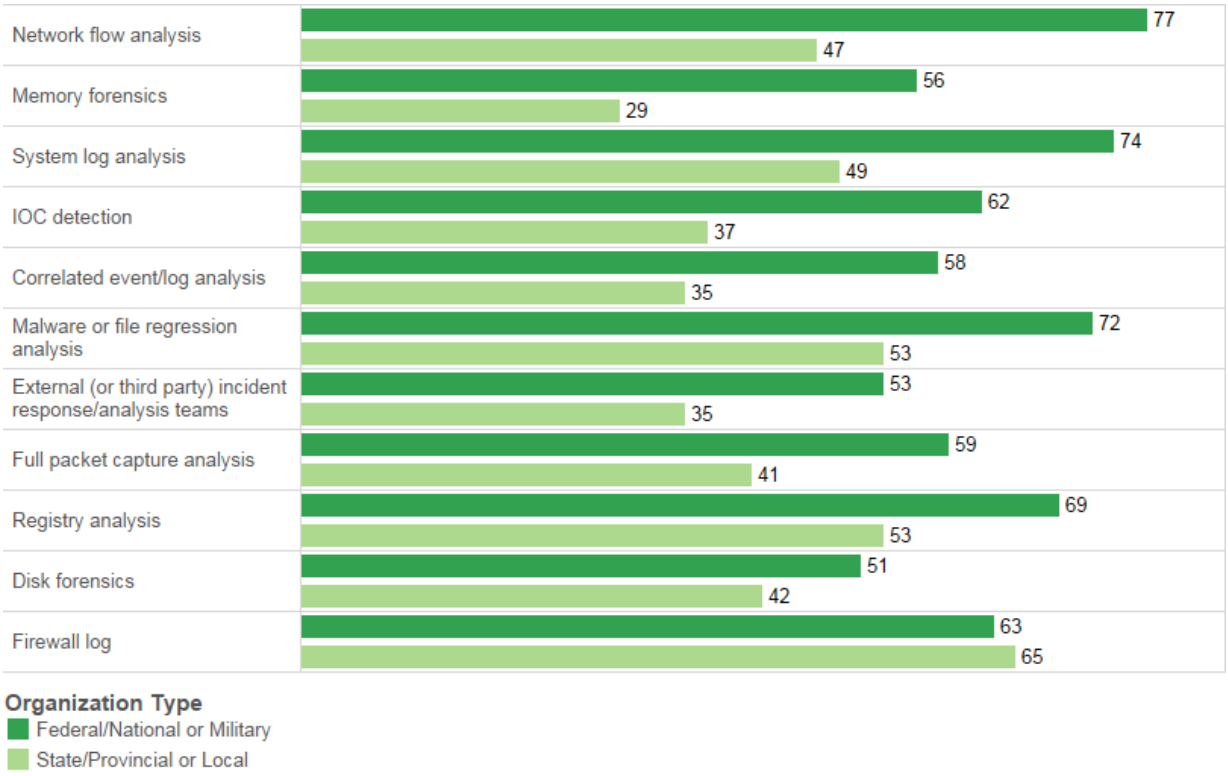


A number of factors are likely undermining government organizations’ efforts to reach higher levels of security sophistication. We have mentioned the overall complexity and disconnected nature of organizations in the sector. A

lack of resources—both in funding and personnel—may also be a major issue, especially for those entities operating at the state or local level.

In fact, further analysis of our findings indicated that federal government and military entities are more likely to use more processes such as network flow analysis, malware or file regression analysis, and system log analysis to analyze compromised systems than organizations at the local or state government level (Figure 6). Federal government and military organizations are likely to have larger budgets for cybersecurity. They are also more targeted by cyberattacks and therefore need to implement an array of advanced security measures.

Figure 6. Use of Processes to Analyze Compromised Systems, by Type of Government Organization

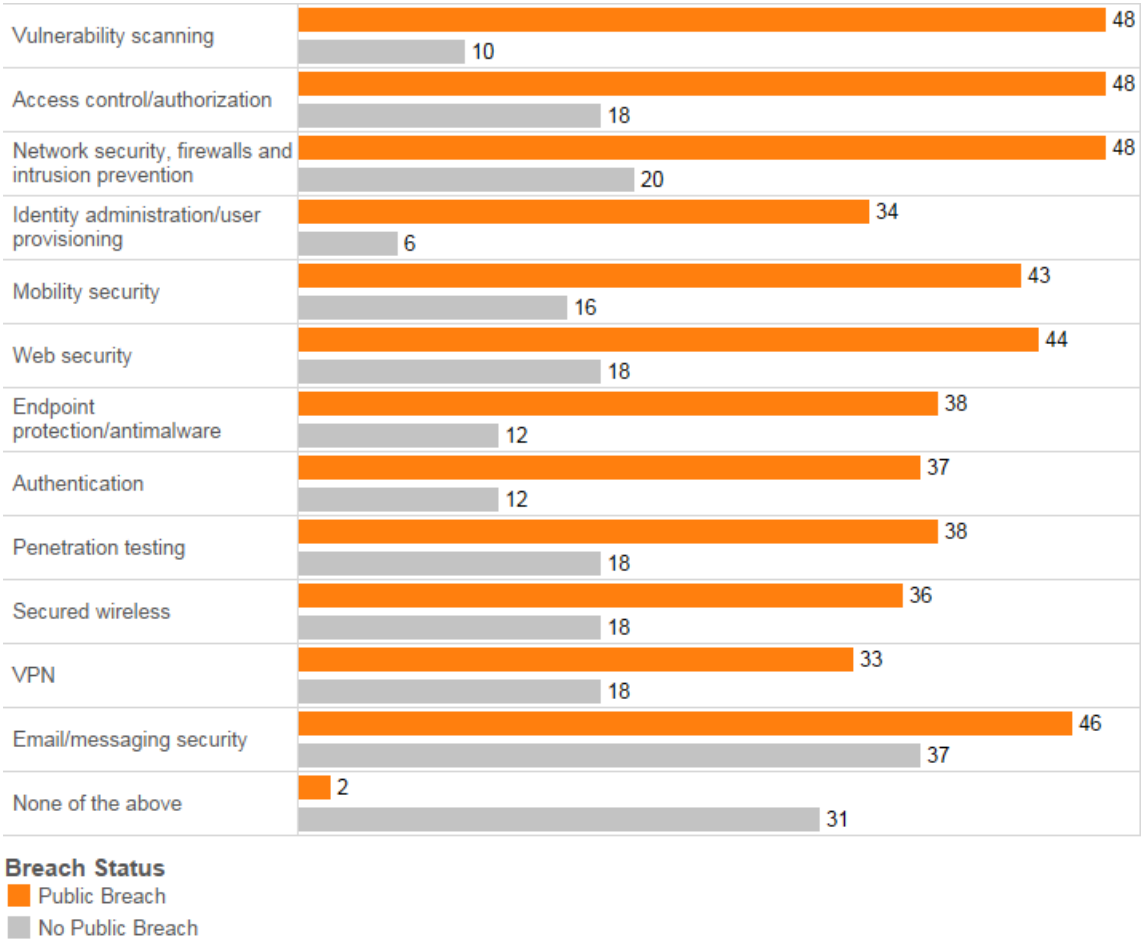


Public Breaches May Increase Focus on Security Defenses

Our study found that government organizations are more likely to have suffered a public breach than private-sector businesses: 66 percent and 55 percent, respectively.

Government organizations that have suffered public scrutiny following a security breach appear to be more motivated to enhance their security measures. They also want to solve the problem and get back to normal operations as quickly as possible, which is likely why the adoption of cloud-based defenses is higher within this group (Figure 7).

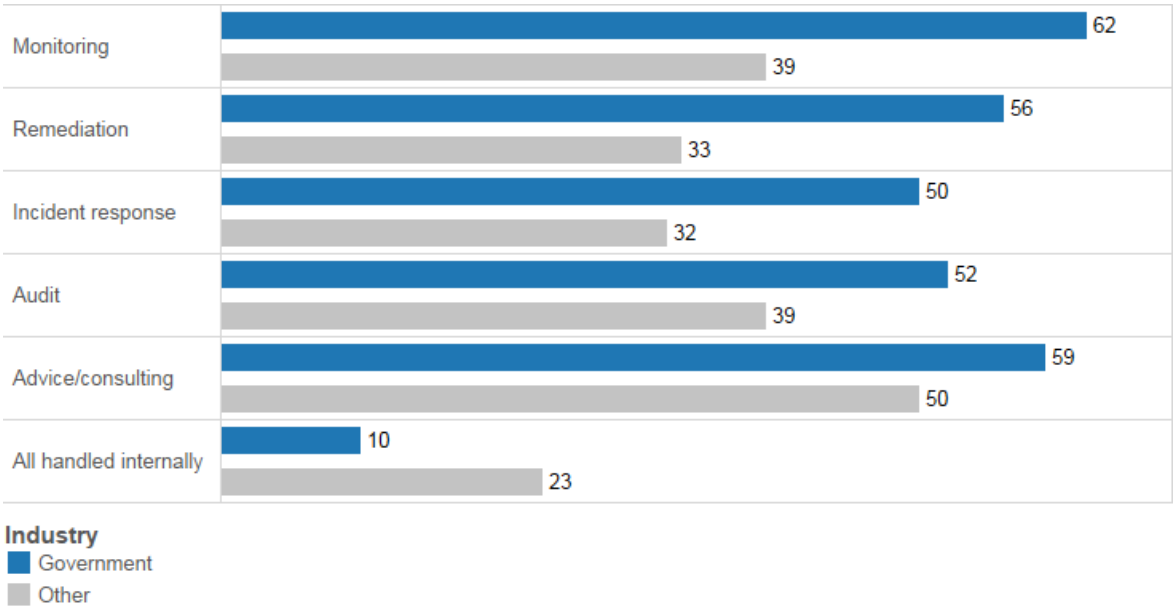
Figure 7. Percentages of Organizations Using Various Cloud-Based Threat Defenses, by Public Breach Status



More Outsourcing of Security Services in Government than in Other Sectors

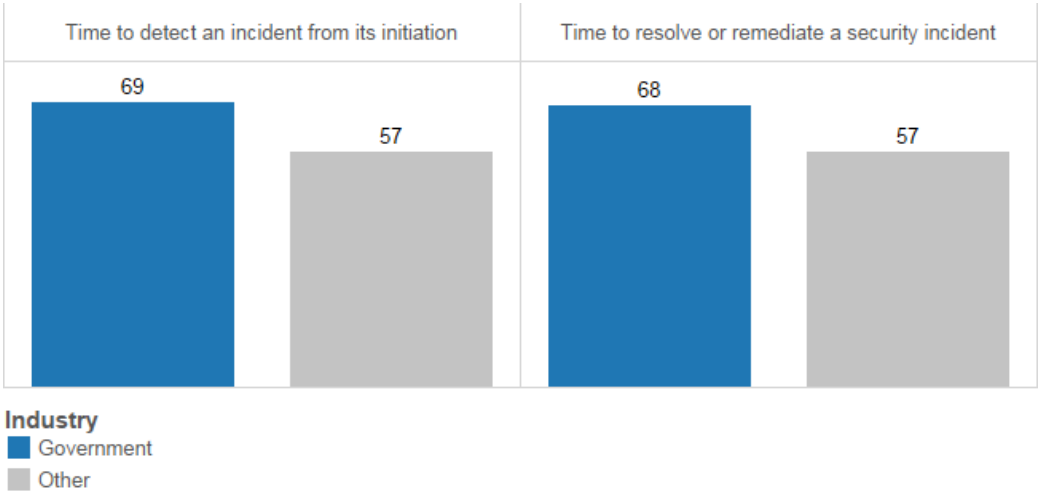
A lack of resources is likely a primary reason why government organizations are significantly more likely to outsource security services than nongovernment businesses (Figure 8). There is a global shortage of skilled IT resources, which is affecting IT hiring in all industries. However, government organizations are generally at an even greater disadvantage in recruiting and retaining cybersecurity staff, because businesses in the private sector can usually offer higher compensation.

Figure 8. Percentages of Organizations Relying on Outsourcing for Various Security Services



According to our study, however, when government entities choose to outsource security monitoring, either fully or in part, the third-party vendor handles a smaller percentage of the monitoring workload (37 percent) than the workload outsourced by nongovernment entities (43 percent). In addition, government organizations that outsource their security workload are more likely than private-sector entities to rely on time to detection and time to resolution as the top measures of third-party performance for these services (Figure 9).

Figure 9. How Organizations Measure Performance of Third-Parties That Provide Security Monitoring

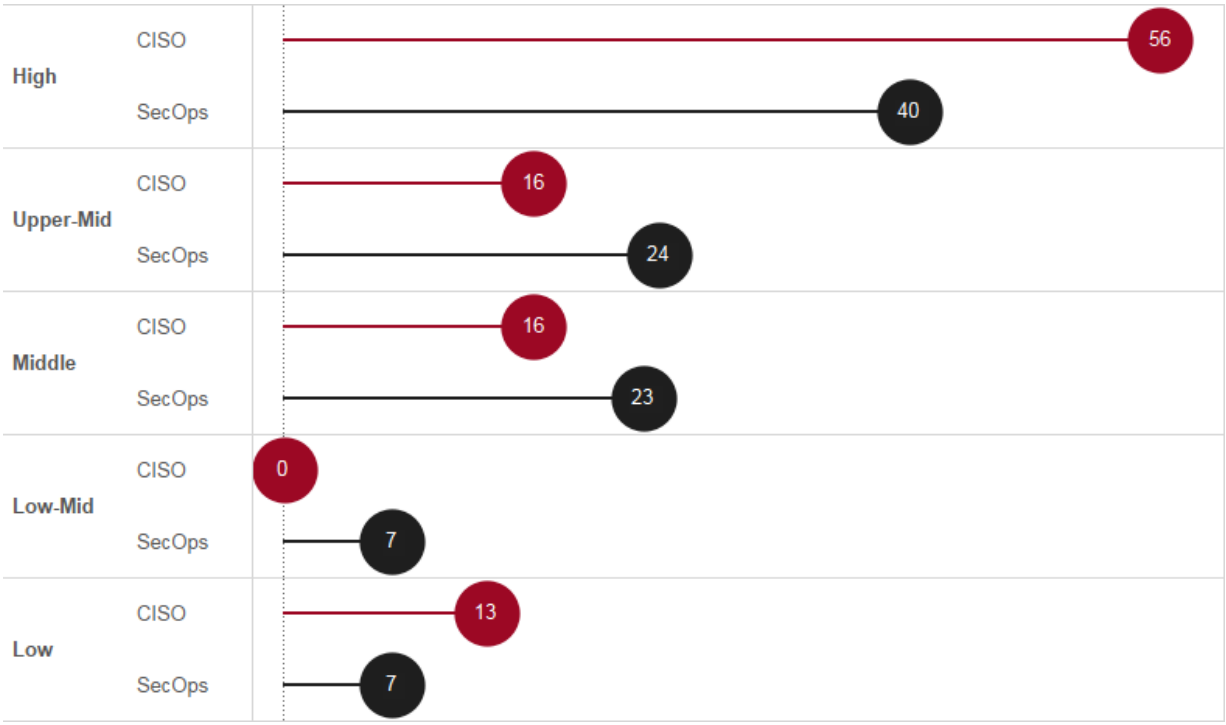


CISOs and SecOps Managers: Different Views on the Organization's State of Security

Chief information security officers (CISOs) and security operations (SecOps) managers working in the government sector are not aligned in their perceptions of the state of security in their organizations. CISOs are significantly more optimistic than SecOps managers (Figure 10). This finding is consistent with the overall study we conducted.

We mapped 72 percent of CISOs as either “upper middle” or “high” in their perceptions of security sophistication, compared with 63 percent of SecOps managers.

Figure 10. Perception of Security Sophistication in Government Organizations, by Role (in Percentages of Respondents)



One possible cause for this gap: CISOs are focused on the overall security strategy for an organization, while SecOps managers are dealing directly with the day-to-day “firefighting” of threats. A general lack of communication between these professionals, which we found to be typical across industries, may exacerbate the differences in perception.

The adoption of commonly accepted cybersecurity frameworks can enhance communication and also help CISOs gain a better picture of their organization’s security sophistication. In turn, CISOs will be armed with more insight and information that they can use to influence management to promote greater collaboration on security measures within the organization, with other government agencies, and with businesses in the private sector.

Recommendations for Improving Security Sophistication

Security personnel at government organizations with higher levels of security sophistication seem confident in the effectiveness of their security tools. Some of the top influencers of security sophistication in this sector include:

- Security that is built into procedures for acquiring, developing, and maintaining systems and applications
- Regular reviews of security practices and tools to ensure they are up to date and effective
- Well-managed and effective technical security controls in systems and networks

To raise their overall level of security sophistication, government organizations should strive to adopt these practices, as well as make a concerted effort to improve collaboration with:

- **Suppliers**: Carefully selecting suppliers and making sure they are transparent about their practices can help reduce vulnerabilities and build more trust in the supply chain.

- **The private sector:** Government organizations should invest more in public-private partnerships. Although private companies may be able to attract more resources to protect their own organizations, they also look to the government to help increase security for all businesses and citizens, and they want to aid in those efforts.
- **Organizations at all levels of government:** Federal governments should share information, practices, and resources to support local and state governments. Building stronger lines of communication among agencies and moving away from a "siloed" approach can strengthen the national security infrastructure.
- **Other nations:** Joint security efforts among governments is important because timely intelligence is essential to the success of a threat-centric defense model. If governments around the world invest in safe (even anonymous) ways to exchange security information, they can better meet their core objectives of protecting their citizens, their sovereignty, and their economy.

Adoption of a common cybersecurity framework can go a long way toward facilitating cooperation and collaboration at all levels of government, between the public sector and private industry, and across borders.

Learn More

To understand how attackers are evolving their techniques to evade defenses, using stealthy tactics based on agility, speed, adaptation, and even destruction, get the Cisco 2015 Midyear Security Report at www.cisco.com/go/msr2015.

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, get the Cisco 2015 Annual Security Report at www.cisco.com/go/asr2015.

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 12/15