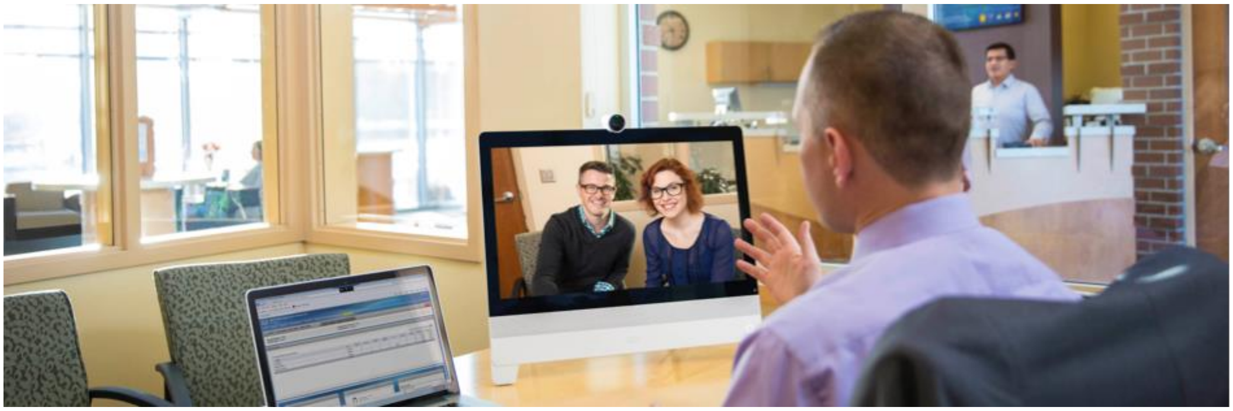
# Telecommunications: Process Improvement Offers a Path to Higher Security Sophistication



The telecommunications (telecom) industry is the backbone of essential services that depend on connectivity. These include emergency response, utility, transportation, and financial services. Telecommunications companies (telcos) are targeted not only by average cybercriminals but also by adversaries looking to create widespread business and service disruption or to access data that could compromise the telcos' operations, their customers, or even national security. Telcos are also under pressure to comply with many laws and regulations. At the same time, a competitive environment demands that they deliver new services and business outcomes with less cost, less complexity, and greater agility.

It is surprising then, that given these circumstances, the sector's overall security sophistication is not higher than that of other industries. Our experts also found that:

- Telcos that have not suffered a public security breach appear to be overly confident about the effectiveness of the security technology they have in place.
- There is a lack of alignment between chief information security officers (CISOs) and security operations (SecOps) managers, reflected in their perceptions about their tools, processes, and security readiness. This divergence could be a challenge to telco performance.
- Although most security professionals in this industry view their security infrastructure as being very up to date and constantly upgraded with the best technologies available, the low use of many essential threat defenses suggests otherwise.

## Major Findings

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

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

- Telcos are more likely than organizations in other industries to use threat defenses such as VPN, authentication, and mobility security, including cloud-based versions of these solutions. This high use is probably due to telecommunications having a more mobile workforce than other industries.
- Telcos are more likely than organizations in other industries to follow a standardized information security policy practice, and a significant majority of these companies have ISO 27001 certification. Regulatory pressures are likely to have influenced both trends.
- Telcos that have suffered a security breach that led to public scrutiny report a higher use of network and endpoint forensics tools and distributed denial of service (DDoS) defense solutions than telcos that have not endured a public breach.
- Less than half of telcos report using security information and event management (SIEM) as a threat defense. The low use of SIEM could be a primary reason why many telcos have less confidence in their security processes; they may not be able to fully understand the output from SIEM solutions.

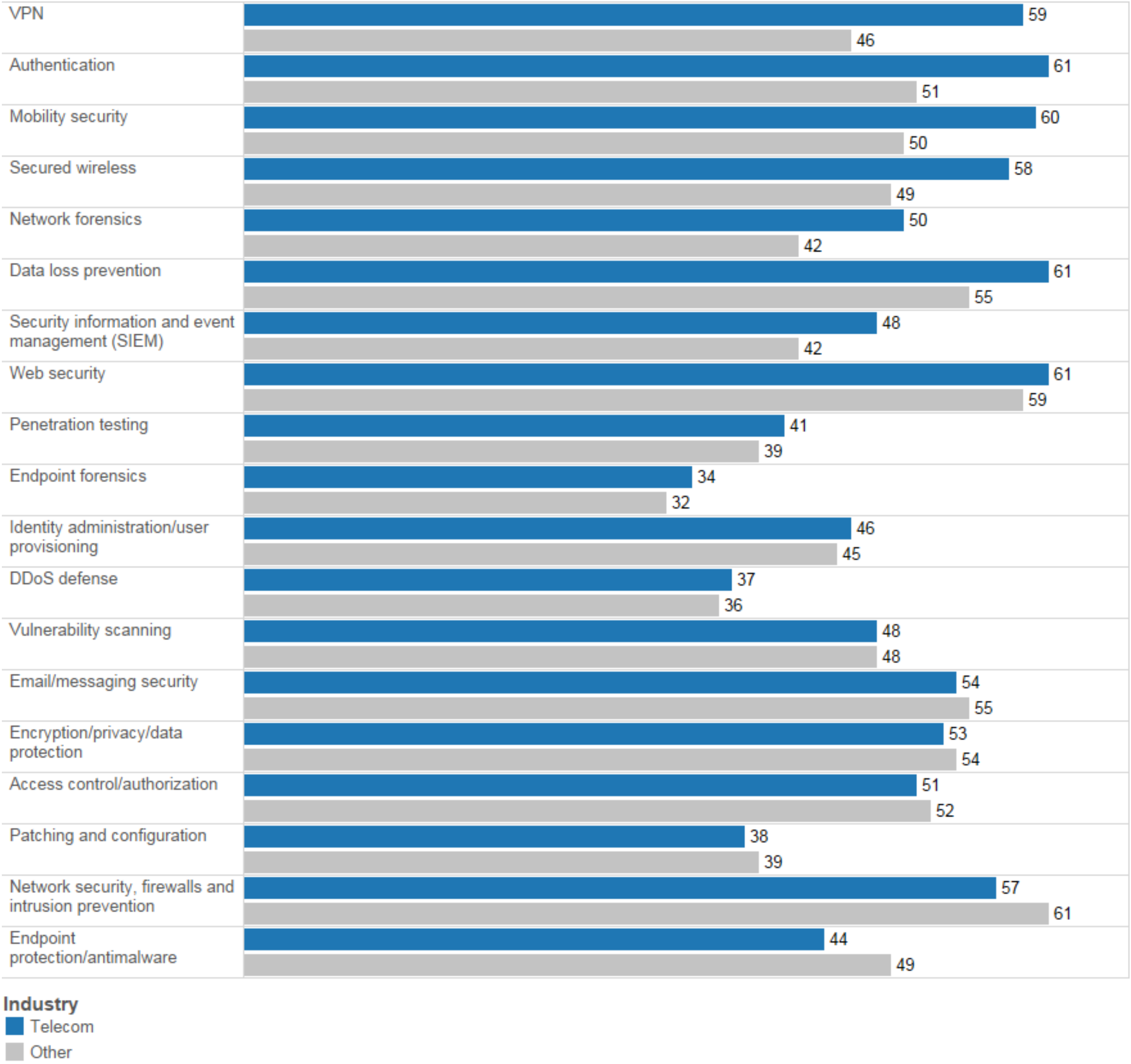
## Telcos Invest More in Tools to Support Mobile Workers and Rely More on Outsourcing

To maintain a competitive advantage, telcos must continually modernize their operations so that they can deliver new types of services and improve the customer experience while maintaining cost efficiency. At the same time, they need to bolster their threat defenses to meet regulatory requirements as well as expectations from customers and partners. Given their limited budgets, many telcos are not prioritizing investments in security.

Telcos’ use of tools such as web security, penetration testing, patching, and configuration is similar to that of other industries we analyzed (Figure 1). However, telcos lag slightly behind other organizations in several areas, such as network security, firewalls, and intrusion prevention.

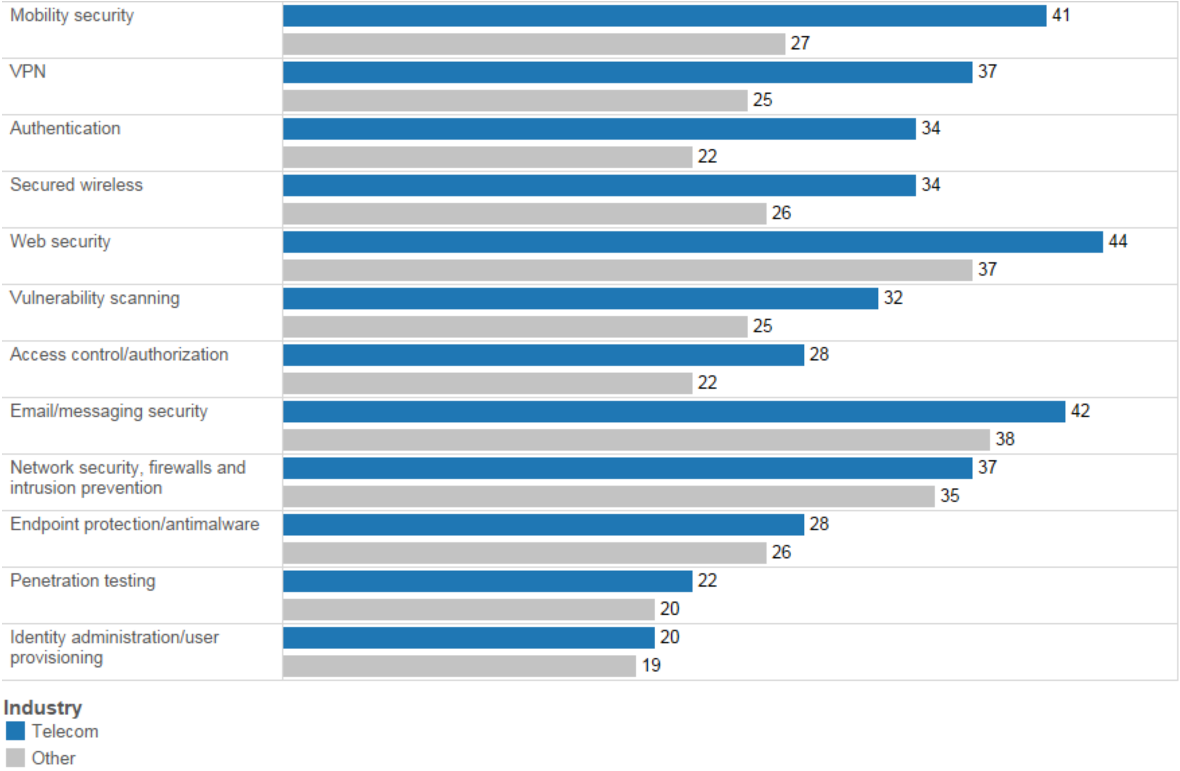
Telcos use VPN, authentication, and mobility security more than organizations in other industries. They are likely investing more in these tools to support highly mobile and remote workforces. Because telcos resell these services, there may also be a lower barrier to their own adoption.

**Figure 1.** Percentages of Organizations Using Various Threat Defenses



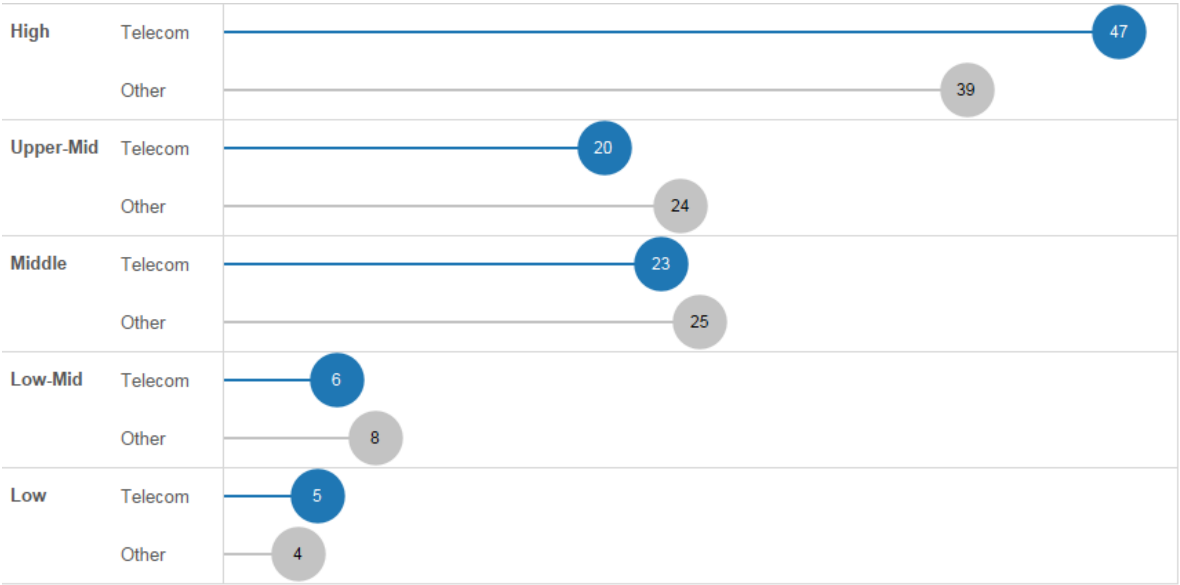
Telcos use cloud-based defenses more than firms in other industries, which also may be related to their need to support mobile and remote employees. As an example, 41 percent of telcos report that they use cloud-based solutions for mobility security, compared with 27 percent of organizations in other industries (Figure 2).

**Figure 2.** Percentages of Organizations Using Various Cloud-Based Threat Defenses



As for security processes, the telecom industry has an optimistic view of its sophistication. This perspective is in line with those of other industries. Based on the perceptions of security professionals, we categorized 67 percent of telcos as either upper-middle or high in terms of their security sophistication, compared with 63 percent of organizations in other industries at these same levels (Figure 3).

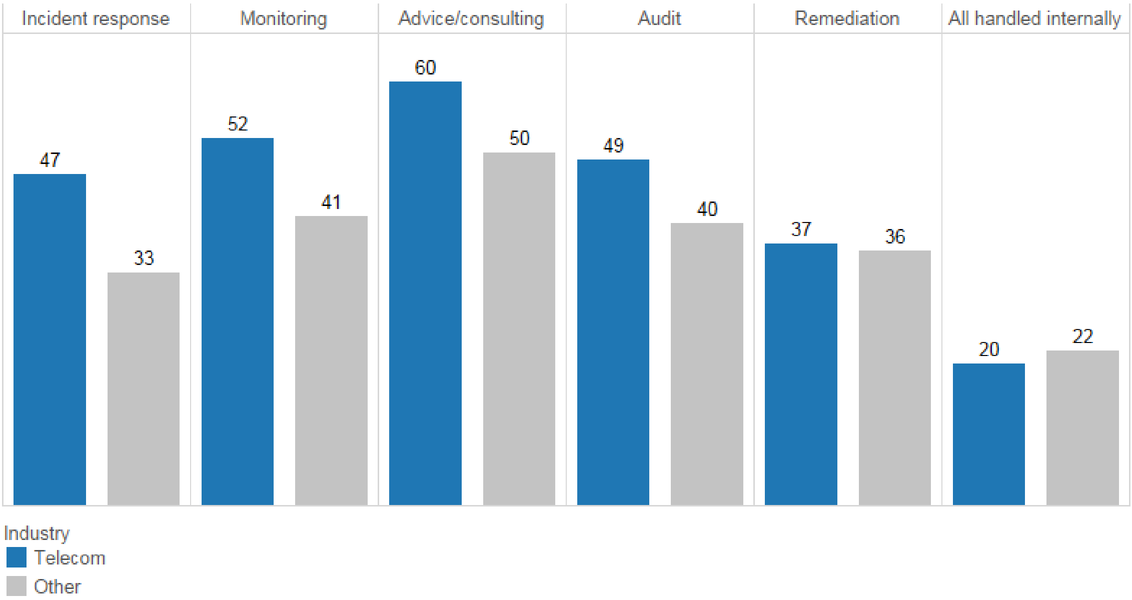
**Figure 3.** Perception of Security Sophistication (in Percentages)



Moreover, the telecom industry is more likely to outsource security services than other industries (Figure 4). This finding is not surprising, given that telcos frequently outsource other services to help keep costs down for their subscribers and to access expertise they may lack in-house.

Telcos are significantly more likely to rely on third-party resources for advice and consulting services related to security, for security monitoring, and for incidence response (Figure 4).

**Figure 4.** Outsourcing of Various Security Functions (in Percentages)

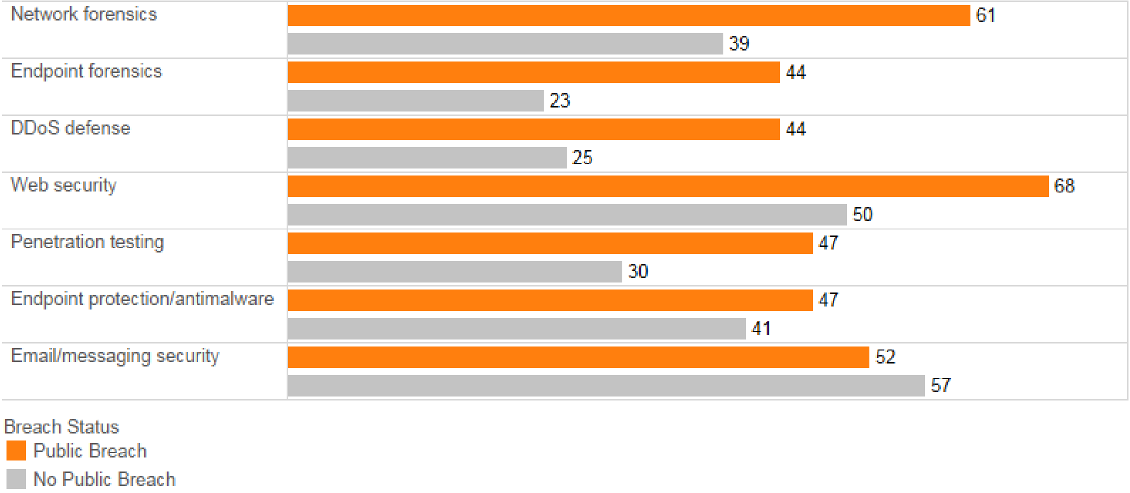


## Public Breaches Push Telcos to Embrace Forensics Tools and Improve Processes

Telcos that have suffered a security breach that led to public scrutiny report a higher use of network and endpoint forensics tools, according to our study. They also use DDoS defense solutions more than telcos that have not endured a public breach—44 percent and 25 percent, respectively (Figure 5).

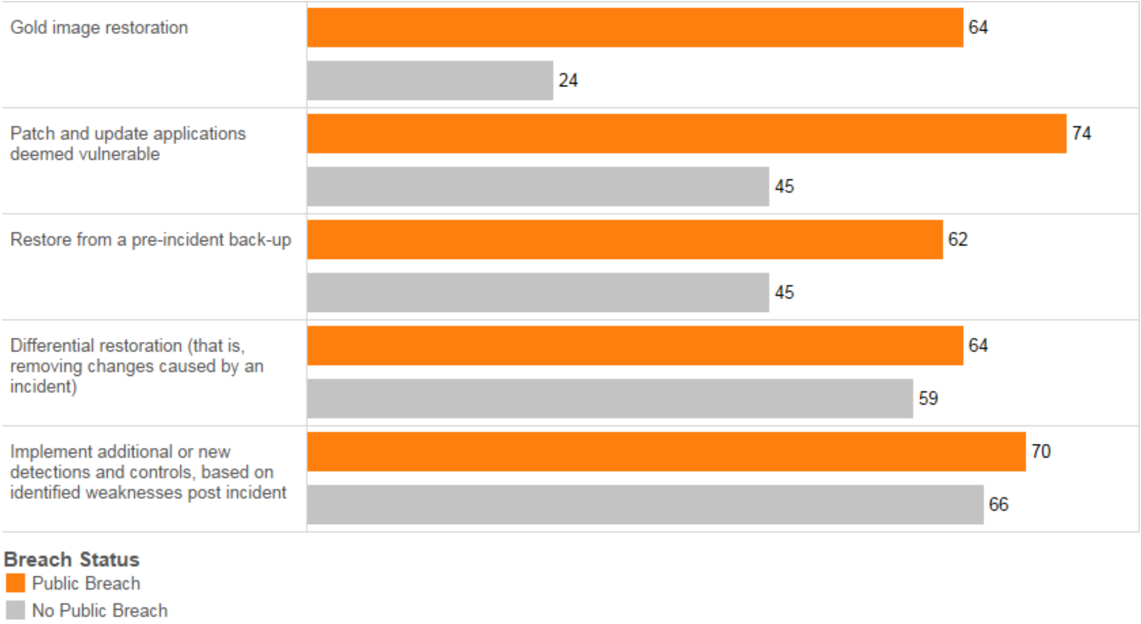
These measures are likely an effort to prevent future breaches that could affect service provision and lead to further public scrutiny and even regulatory fines.

**Figure 5.** The Use of Various Threat Defenses by Publicly Breached and Non-Publicly-Breached Organizations (in Percentages)



We also found that telcos that have suffered public scrutiny due to a breach—and that also consider their infrastructure to be very up to date—use more processes to restore affected systems to pre-incident levels. The starkest contrast is in the use of gold image restoration: 64 percent of publicly breached telcos use this process, compared to 24 percent of non-publicly-breached telcos that also report their infrastructure to be very up to date (Figure 6). In addition, while 74 percent of telcos in the former group patch and update applications deemed vulnerable, only 45 percent in the latter group report using that process.

**Figure 6.** Processes Used by Organizations with Very Up-to-Date Infrastructure to Restore Affected Systems to Pre-Incident Levels (in Percentages)



The fact that less than one-quarter of non-publicly-breached telcos that consider their infrastructure to be very up to date are using gold image restoration, and that less than half are patching and updating vulnerable applications, suggests that these companies may be overly confident about the effectiveness of the security technology they have in place. They also may also be unsure of what processes they should implement to support security technology and to help protect their network before, during, and after an attack.

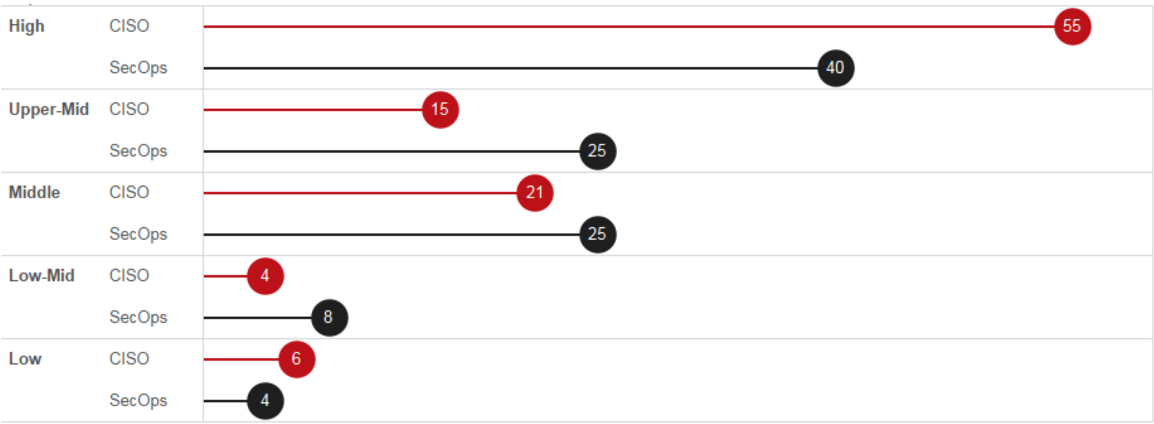
## Telcos More Likely to Follow a Standardized Information Security Policy Practice

The telecom industry is heavily regulated, and telcos must be able to demonstrate to regulatory authorities that they have implemented leading security processes. Standardizing their practices is a way to show that they are focused on keeping their customers' data safe, and it may even be a requirement in certain countries. This could explain the higher adoption of standardized information security (InfoSec) policies—62 percent of telcos, compared to 51 percent in other industries. Of those telcos that follow a standardized policy, 71 percent have an ISO 27001 certification,[2] compared with 56 percent in other industries.

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

Regarding their processes, 55 percent of CISOs categorize their organization as having a high level of security sophistication, compared with 40 percent of SecOps managers (Figure 7). However, when combining the results from the upper-middle and high categories of security sophistication, the gap in perceptions is not as pronounced: 70 percent of CISOs and 65 percent of SecOps managers fall into these categories. This suggests that despite CISOs' more optimistic views, these groups are relatively aligned. It is likely that security is already a boardroom topic for telcos; however, CISOs should become more aware of the day-to-day issues that SecOps managers face.

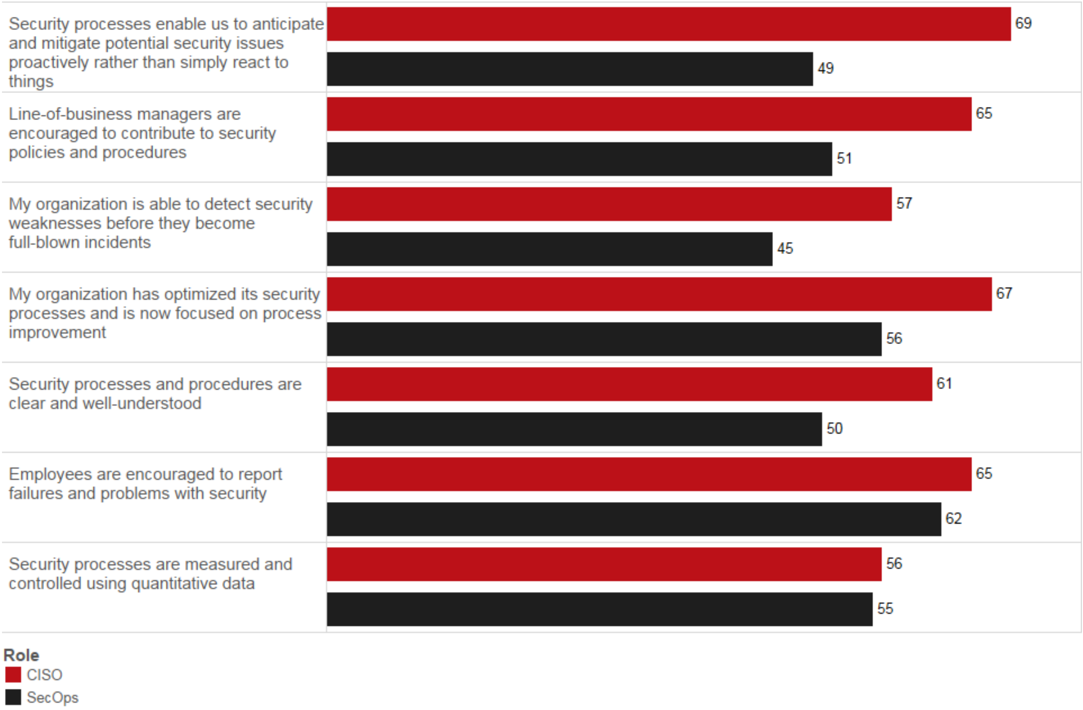
**Figure 7.** Perceptions of Security Sophistication, by Role (in Percentages)



CISOs and SecOps managers are closely aligned in their perceptions of security sophistication around employee engagement and control measures. However, they are significantly less in sync with regard to their organization's implementation of processes and the ability to mitigate risks. Sixty-nine percent of CISOs are confident that security processes enable their organization to be more proactive about identifying and responding to security issues compared with 49 percent of SecOps managers (Figure 8).

[2] ISO 27001, International Organization of Standardization: http://www.iso.org/iso/home/standards/management-standards/iso27001.htm

**Figure 8.** Perceptions of the Effectiveness of Security Measures, by Role (in Percentages)



## Mismatch Between Perception and Reality

In the telecom industry, CISOs and SecOps managers both appear to have significantly more confidence in the security technology that their organizations have implemented than in the security processes they use. Seventy-six percent of CISOs and 73 percent of SecOps managers surveyed report that their organization’s security infrastructure is very up to date and is constantly upgraded with the best technologies available.

However, looking back to the list of threat defenses in Figure 1, it does not appear that perception and reality are aligned. For example, only 37 percent of telcos report using DDoS defense tools. These solutions are critical for ISPs and other service providers, which are often targets of DDoS attacks. In fact, telcos that were categorized as having high security sophistication—and the most up-to-date infrastructure—were far more likely to be using DDoS defenses (44 percent versus 14 percent), according to our research.

In addition, less than half (48 percent) of telcos report using SIEM. The low use of this tool by telcos could be a key reason why these companies tend to have less confidence in their processes. By using SIEM, organizations demonstrate that they have processes in place to understand the output from their security solutions. Upon closer examination of the survey findings, we found that 60 percent of telcos that are highly confident in their security processes use SIEM.

## Recommendations for Improving Security Sophistication

Although many telcos are using “best in class” technology for security, overconfidence in the effectiveness of these solutions could be leaving many companies vulnerable to attacks. To get the greatest benefit from their security technology, telcos should focus on improving processes that support these solutions. In addition, they should:

- Increase their understanding of how to protect their network before, during, and after an attack, and plan accordingly for risks. A security breach should not be the impetus for strengthening defenses.

- Deepen executive engagement in security as a way to help improve processes. Ninety-three percent of CISOs and SecOps at telcos that were categorized as having high levels of security sophistication agreed that security roles and responsibilities had been clarified within their executive team.
- Focus on building security into systems and applications, and keeping them up to date.

To improve security, the telecom industry should focus on achieving operational excellence. Technology is a vital component to better security, but it is not enough. Telcos also need to have the right people and processess in place to ensure that security solutions run effectively, and they need to use metrics to verify the performance of their security technology.

## 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 global 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