Telecommunications: Preparing for the Security Business Opportunity

Telecommunications companies (telcos) are under intense pressure to protect their infrastructure, maintain compliance, and innovate continuously–all while providing reliable service. Recent high-profile data breaches in the sector have added to that pressure and raised more concern about the state of security in this industry.

Not surprisingly, many telcos lack confidence about their security posture. To regain it, telcos should proactively assess their security and make improvements. For larger telcos that can generate revenue from reselling security services to their customers, an investment of resources could prove particularly valuable to the business in the long term. To improve their security posture, telcos, large and small, need to:

- Gain visibility into the network and compress the time between detecting and remediating threats.
- Consider using services, such as outsourcing, as a way to develop a more cohesive security approach.
- Take a more balanced approach to preserving the confidentiality, integrity, and availability (the "CIA triad")[1] of information and services. These three aspects are equally important.

[1] The CIA triad is a well-known model in the development of information security policy. For more details, see "The CIA Triad," TechRepublic, June 2008: http://www.techrepublic.com/blog/it-security/the-cia-triad/.

Major Findings

In this paper, Cisco experts analyze the IT security capabilities of telcos using data from the Cisco 2015 Security Capabilities Benchmark Study.[2] For example, we learned that:

- There was a significant year-over-year decline in the percentage of telcos that could be categorized as highly mature in terms of their security sophistication. In our 2014 study, nearly half (47 percent) of these organizations were highly mature; in 2015, only one-third (33 percent) met that description.
- A similar decline was seen in the telcos' perception of their security infrastructure: In 2014, 74 percent of our respondents reported that their infrastructure was very up to date and constantly upgraded with the best technologies available. In 2015, only 55 percent of telcos made the same assessment.
- Telcos' declining confidence about the state of their security may be due partly to their being favorite targets of threat actors. More than half (57 percent) of telcos reported in 2015 that they had suffered a breach that led to public scrutiny. Less than half of the businesses in other industries (48 percent) reported that they had experienced a similar security breach.
- Smaller telcos are much more likely (59 percent) than larger telcos (43 percent) to rely on third-party resources for advice and consulting. This greater reliance may be the result of budget constraints. Outsourcing these services may help smaller telcos to improve their security posture while reducing costs and overhead.

Year-Over-Year Decline in Telcos' Confidence in Their Security Infrastructure and Overall Security Sophistication

A strong majority of telcos (74 percent) that took part in our 2014 study were confident that their security infrastructure was very up to date and constantly upgraded with the best technologies available. However, we noted then that the industry's low utilization of many basic threat defenses did not justify such high confidence.

The findings from the 2015 study suggest that security personnel at telcos have since realized that their overall level of security sophistication does need to improve. This realization is likely due to the telecommunications (telecom) industry experiencing a number of high-profile data breaches in recent years and the resulting scrutiny–from the boardroom, investors, regulators, and customers–of telcos' security practices.

Telcos now show levels of confidence that seem more aligned to the true state of their security: 55 percent of the respondents agreed that their security infrastructure is very up to date and constantly upgraded. (See Figure 1).

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

Figure 1. Percentages of Respondents in Telecom and Other Industries Agreeing with a Positive Description of Their Security Infrastructure: 2014 and 2015

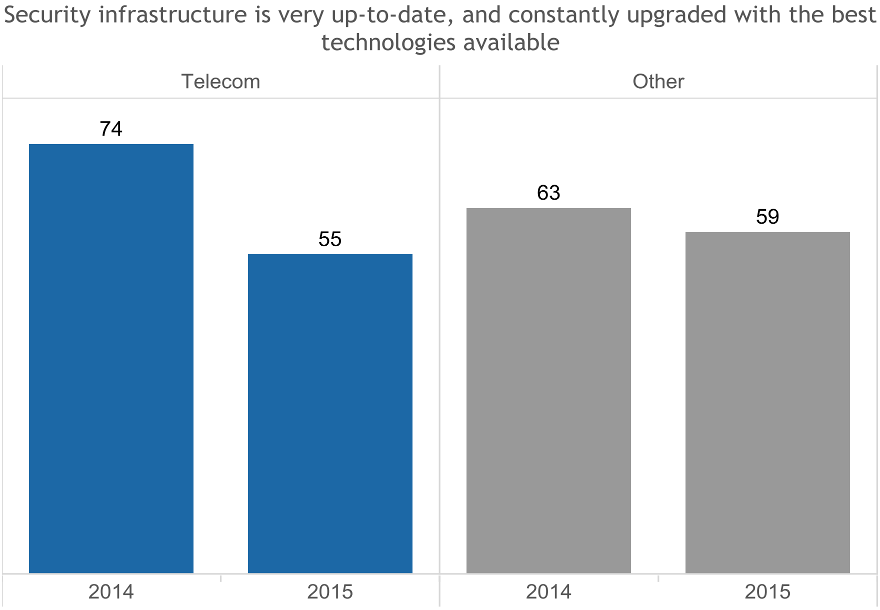
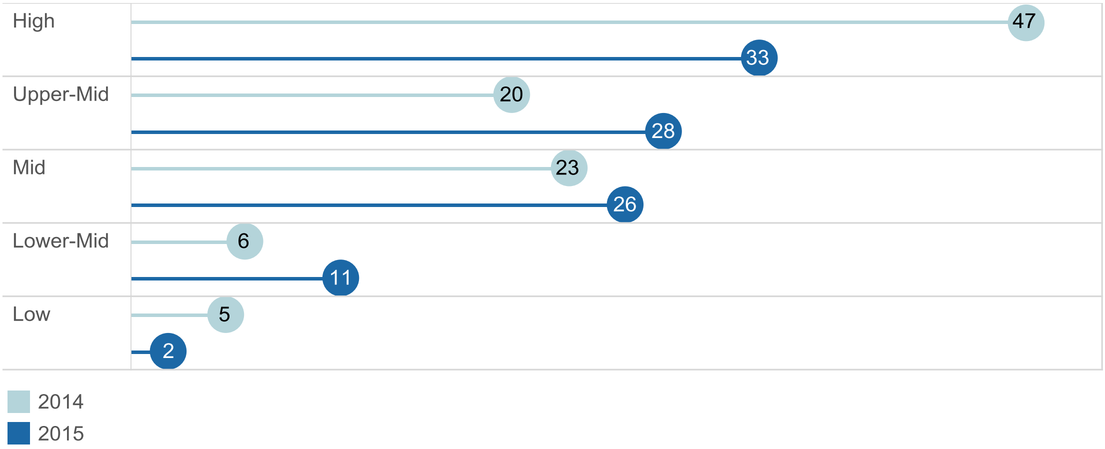


Figure 1 also shows that in 2015, telcos were slightly less likely than businesses in other industries to agree that their infrastructure is very up to date. In 2014, the opposite was true; the telecom industry had an 11 percentage point advantage over other industries.

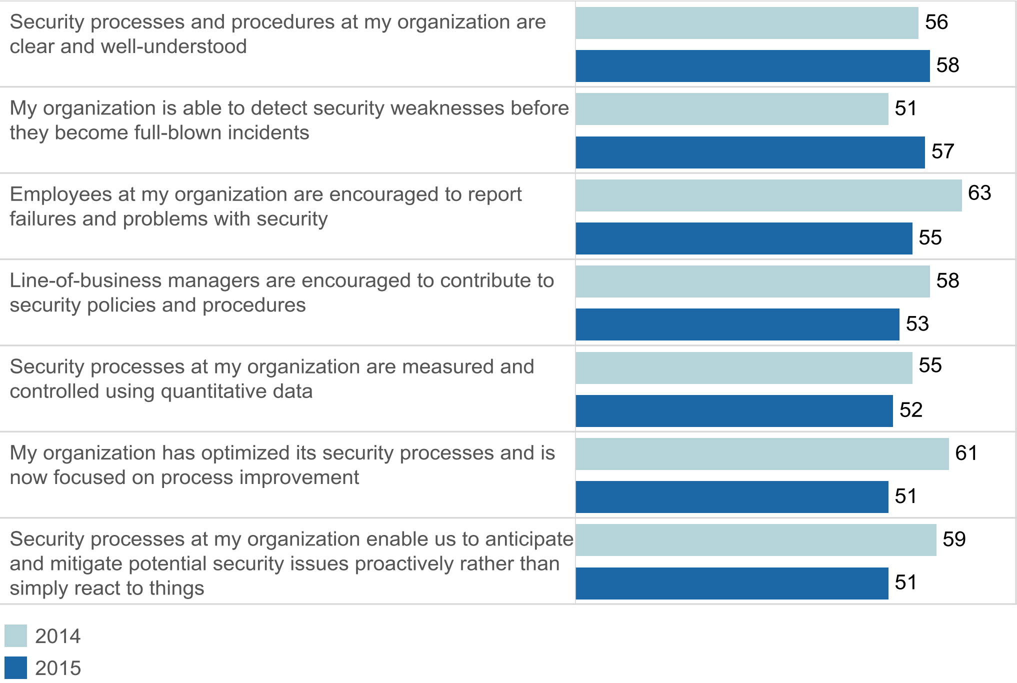
There was a sizable year-over-year decline in the percentage of telcos categorized as highly mature in terms of their security sophistication. Nearly half (47 percent) of the telcos in the 2014 study were highly mature. In 2015, only one-third (33 percent) met that description. (See Figure 2.)

Figure 2. Comparison of Telco Security Maturity in 2014 and 2015, in Percentages



In addition, as Figure 3 illustrates, respondents to the 2015 survey were less likely to strongly agree with most positive statements about their security culture. For example, 61 percent of telcos in 2014 agreed strongly that they had optimized security processes and were now focused on process improvement. Just 51 percent of the respondents had the same assessment about that aspect of their security culture in 2015–a 10-point decline.

Figure 3. Percentages of Telcos Agreeing with Various Statements About Security Culture: 2014 and 2015



This crisis of confidence among telcos could actually be a positive sign because it suggests that many of these businesses are not complacent about their security. As telcos become more vigilant about what is happening on their networks, they are realizing how challenging it is to detect and remediate threats quickly.

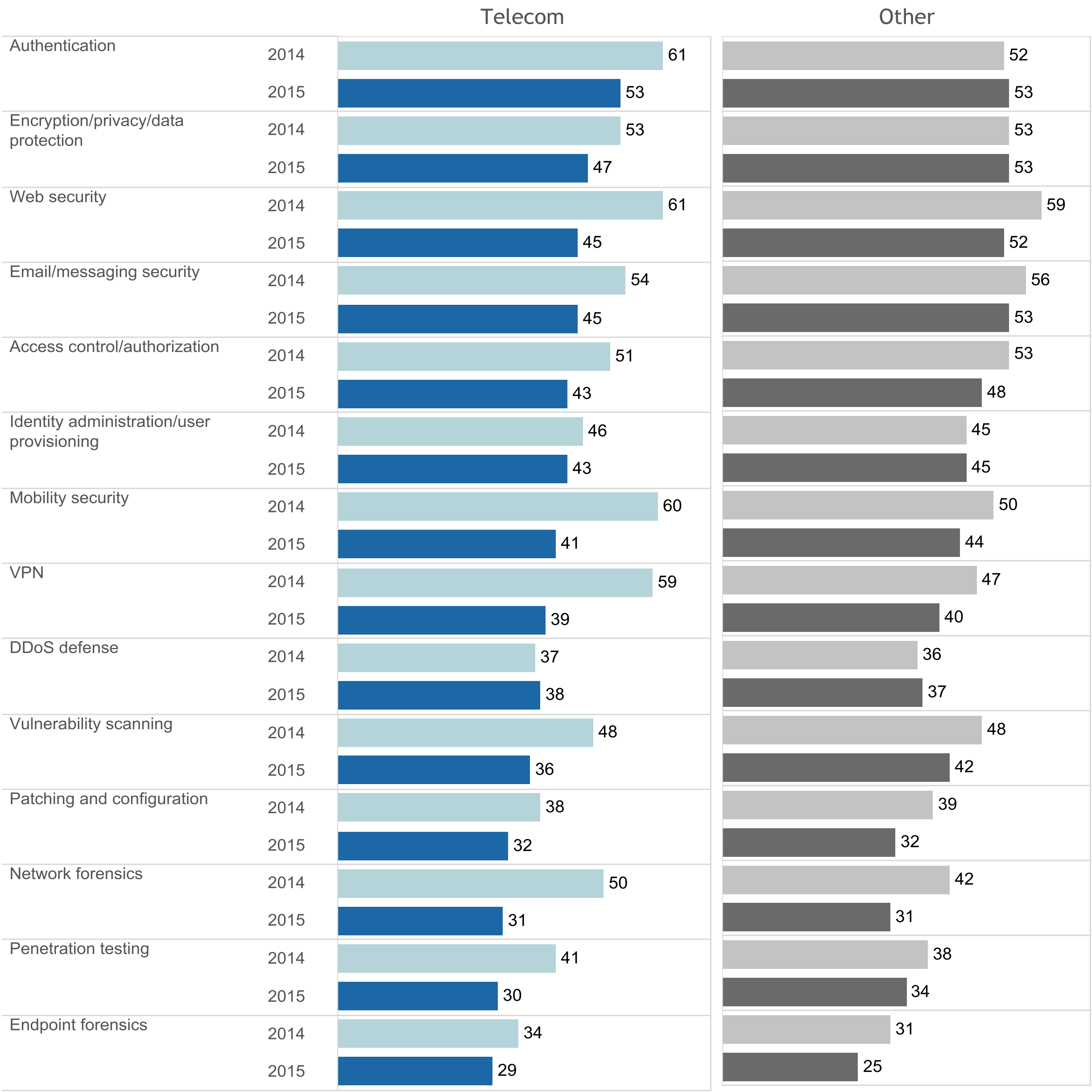
In the past, many telcos likely believed that their security posture was strong because they were working so hard to meet regulatory requirements related to security. However, the modern threat landscape is even more complex than the regulatory environment. Telcos are expanding their criteria for assuring security.

Telcos Using Fewer Threat Defenses and Processes than Companies in Other Industries

Findings from the 2014 study suggested that many telcos were not investing as much as they should in a number of main security threat defenses. It appears telcos did not increase their use of various security tools in 2015. In fact, they showed actual declines in a number of categories.

For example, as Figure 4 illustrates, there were notable drops in the use of threat defenses such as VPN, authentication, and mobility security. In 2014, telcos had an advantage over other industries in their use of these three tools. The 2015 drop brought telcos closer to the use in other industries.

Figure 4. Percentage of Companies Using Various Threat Defenses: Telecom and Other Industries, By Year



The 2015 findings indicate that the telecom sector's use of security threat defenses is now more on a par with the use reported by other industries. The declines in various categories could be the result of telcos–especially those feeling less confident about the status of their security infrastructure–assessing their use of threat defenses and determining what solutions they need to detect and respond to threats faster.

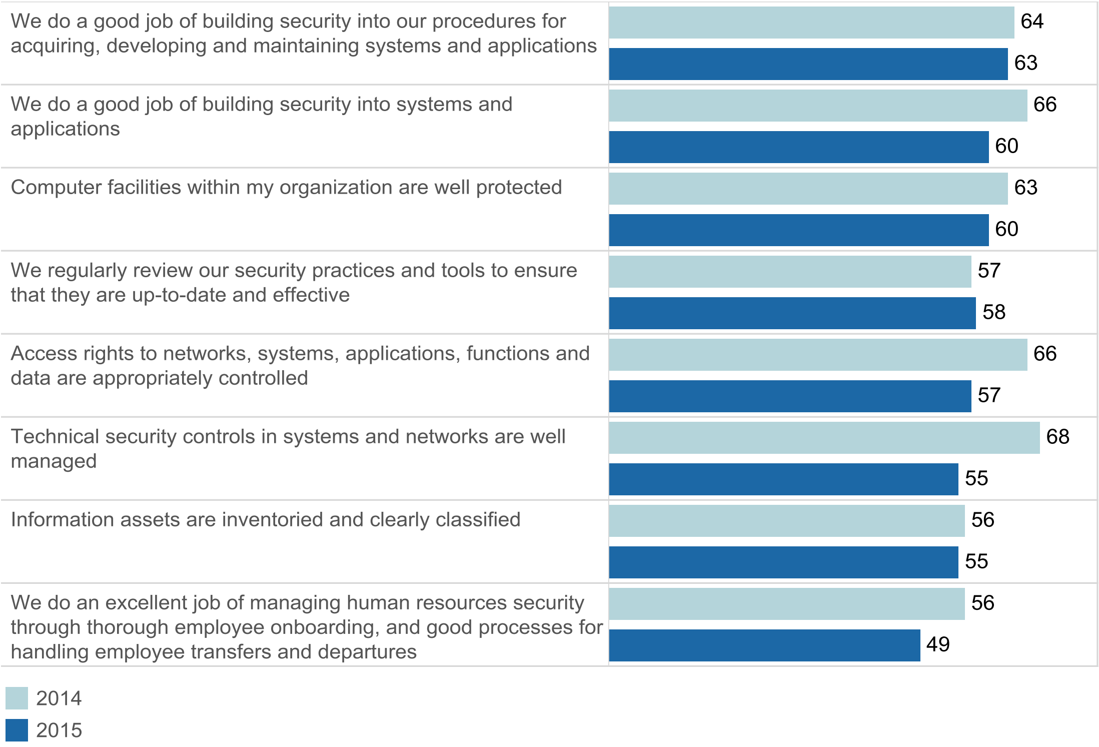
There is other evidence that telcos are striving to be more strategic about security. More telcos in 2015 reported that they have a written, formal, organizationwide security strategy that is reviewed regularly. The percentage of smaller telcos using this risk management strategy increased by 9 points from 2014.

However, the 2015 study also found that:

- Telcos were less likely to use processes for restoring affected systems to preincident levels. This decline includes patching and updating applications that were deemed vulnerable (a 13-point decline from 2014).
- Fewer telcos used processes to eliminate the causes of security incidents. The most dramatic decline was seen in the percentage of telcos using a process for long-term fix development. In 2014, 60 percent of telcos reported that they used this process. In 2015, only 38 percent of telcos had the same response. The reason for this change is not known. All other industries represented in the survey, which included financial services and healthcare, also saw a decline in this category from 2014 to 2015.

Telcos were also less optimistic about security policies in 2015 than they were 2014. (See Figure 5.) Here again, these findings are probably the result of growing security awareness among telcos. The more they understand the security challenges they face, the less confident they are about their ability to protect their organization and their infrastructure.

Figure 5. Percentages of Telcos Strongly Agreeing with Statements About Their Security Policies, 2014 and 2015

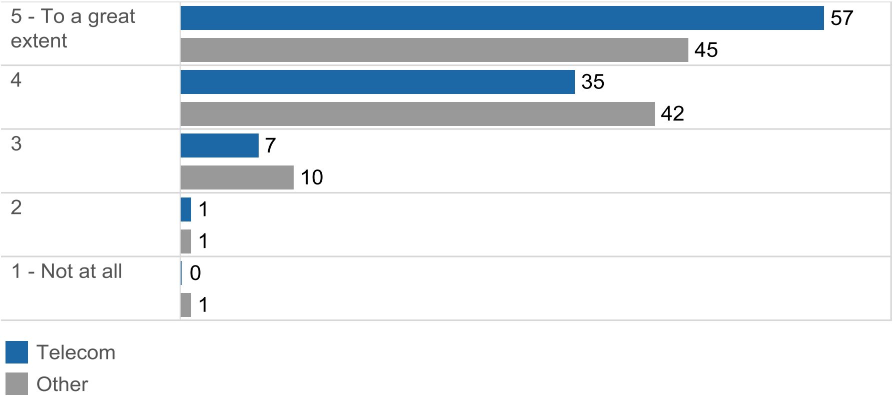


Telcos More Likely to Make Improvements and Outsource Following a Public Breach

Another factor for telcos' declining confidence about security: more of than half (57 percent) of these organizations reported in 2015 that they had suffered a breach that led to public scrutiny. Less than half of businesses in other industries (48 percent) reported that they experienced a similar breach.

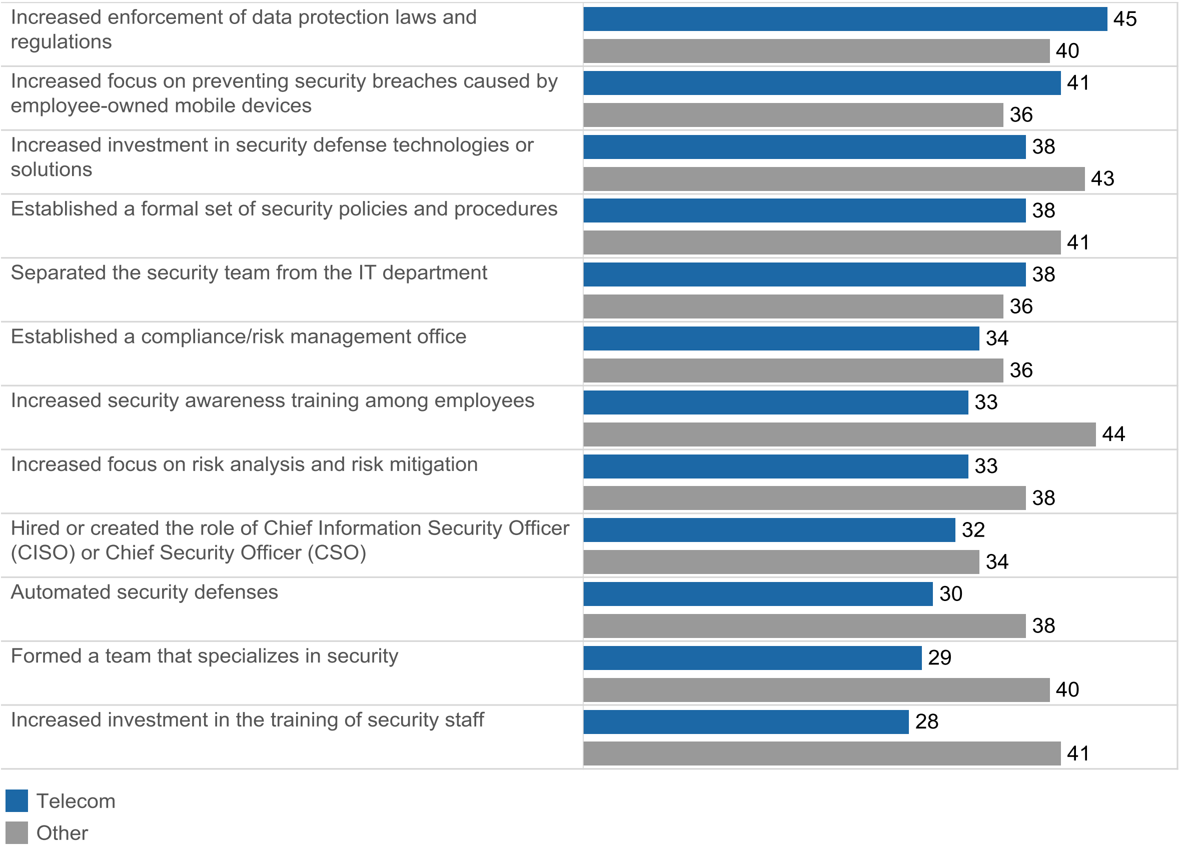
Telcos that have had to deal with public scrutiny after a breach also appear to be far more likely than organizations in other sectors to improve their security to a great extent. As Figure 6 shows, 57 percent of telcos reported making significant changes after a breach, compared with 45 percent of the other businesses in the study.

Figure 6. Extent to Which a Public Breach Drove Security Improvements, by Industry (in Percentages)



As Figure 7 shows, one of the main areas of improvement for publicly breached telcos is the enforcement of data protection laws and regulations. This postbreach increase suggests that these organizations are more aware of how disruptive breaches can be to their businesses—from losing customer confidence to facing costly fines.

Figure 7. Types of Improvements Made Following a Public Breach, by Industry (in Percentages)



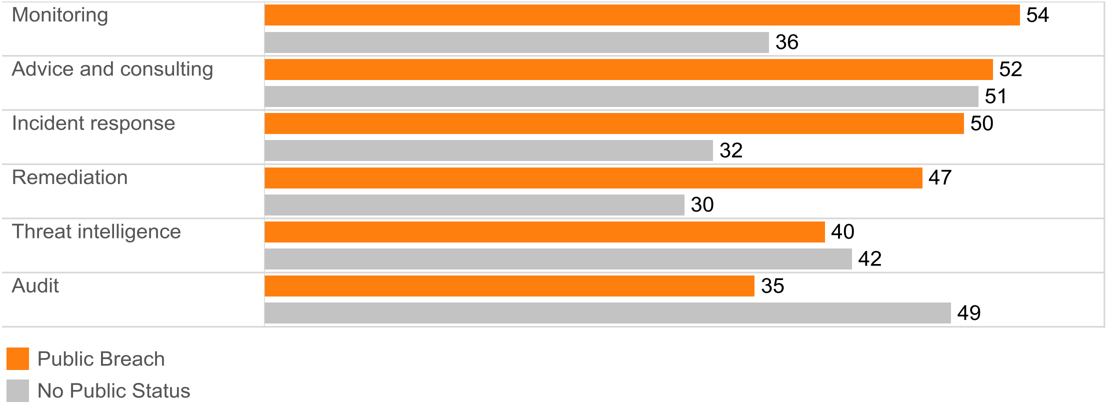
However, Figure 7 also shows that telcos lag behind other organizations in making other types of improvements following a breach. For instance, although 41 percent of other businesses increased their investment in security staff training after a public breach, just 28 percent of telcos reported that they made the same commitment. This discrepancy may be due to the fact that many telcos already have a sufficient number of security personnel. Fortyone percent of telcos reported that they have 50 or more employees dedicated to security. Findings were similar for financial services (44 percent) and government (43 percent).

Budget constraints may be a factor as well. Only 6 percent of telcos have their security budget completely separate from the IT budget, according to the 2015 study. Over half (58 percent) of the respondents in the telecom industry reported that their organization's security budget is entirely within the IT budget. Thirty-seven percent of respondents said that their security budget is partly within the IT budget, but that there is additional budget for security outside of IT.

A similar budget distribution is present in other industries. Few organizations have their security and IT budgets completely separated, while the majority have their security budget contained within the IT budget.

Findings for the 2015 study indicate another trend among telcos that have been publicly breached: They appear more likely to outsource security services. (See Figure 8.) About half of all publicly breached telcos reported that they rely on third-party resources for monitoring, advice and consulting, incident response, and remediation.

Figure 8. Percentages of Telcos Outsourcing Security Services, by Public Breach Status



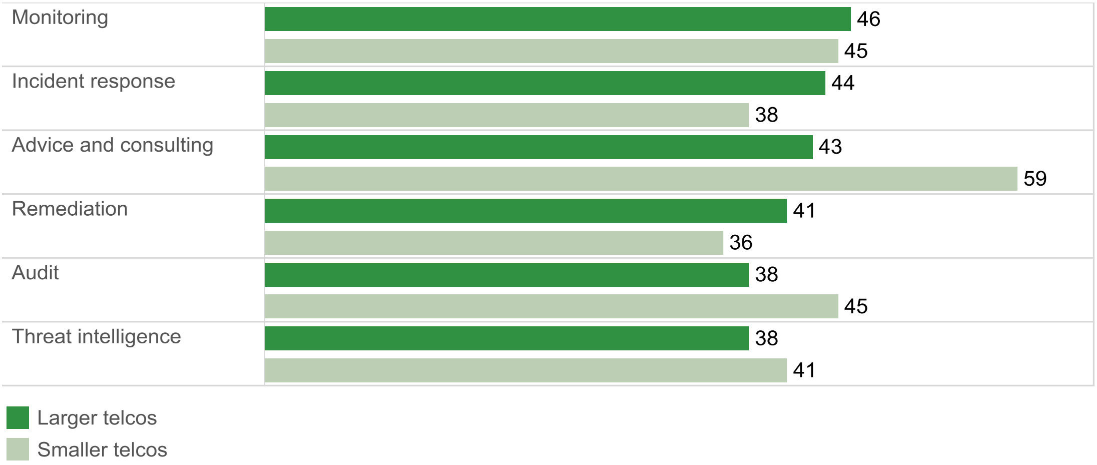
Telcos that have been publicly breached are also significantly less likely (35 percent) to outsource auditing than telcos that have not faced a similar breach (49 percent). It is likely that publicly breached telcos are more inclined to keep security auditing in-house as a way to assure they are effective at enforcing data protection laws and regulations in the organization and driving continuous improvement.

Smaller Telcos More Likely to Outsource Security Advice and Consulting and to Host Networks in the Cloud

The 2015 study also found that smaller telcos[3] are much more likely (59 percent) than larger telcos (43 percent) to rely on third-party resources for advice and consulting. (See Figure 9.)

[3] For this paper, smaller telcos are defined as having between 250 and 999 employees. Larger telcos consist of 1000 or more employees.

Figure 9. Percentages of Telecom Organizations Outsourcing Security Services, by Company Size



Smaller telcos also seem more inclined than larger telcos to use cloud-based defenses. For example, 35 percent of smaller telcos reported that they employ web security, while only 25 percent of larger telcos said they use web security through the cloud.

Both trends among smaller telcos are likely due to budget constraints. Outsourcing security services and deploying cloud-based defenses enable smaller telcos to improve their security posture while reducing costs and overhead.

Conclusion: Now Is the Time for Telcos to Set a High Standard for Security Sophistication

The telecom industry is a top target for threat actors, but the findings from our 2015 study suggest that many telcos are becoming even more aware of the need to protect their infrastructure as well as their customers. They are facing scrutiny from many stakeholders, from boards of directors to customers. In addition, telcos are facing pressure to comply with complex and ever-changing regulatory mandates around data protection.

Many telcos are concerned about keeping pace with all of these intense demands. Investing in the necessary security tools and processes can help; it will allow them to strengthen their security posture and grow more confident.

Larger telcos, in particular, have a real business opportunity with security: they can generate revenue from reselling to their customers the security services that they deploy. But to resell them successfully, these telcos must demonstrate that they excel at security themselves.

Both larger and smaller telcos should strive to:

- Become more proactive about detecting and remediating threats. Investing in technology and services that will help them to gain better visibility into their network is one strategy for improvement.

- Explore how outsourcing can help them to develop a more cohesive security approach and can serve to complement in-house strategies and resources. For telcos of all sizes, outsourcing can be an effective way to respond more swiftly to incidents before they become major breaches. Smaller telcos can especially benefit from this approach because they typically have less budget available for technology investments and for hiring in-house security personnel.

- Take a more balanced approach to preserving the confidentiality, integrity, and availability of data and services. Even though it is imperative for telcos to maintain the availability of services, preventing the loss of confidentiality and integrity are equally important. Data privacy is a top concern for all consumers of telecom services. Telcos must be vigilant in ensuring that no one can gain inappropriate access to sensitive information and that information is not altered by unauthorized parties.

Learn More

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

About the Cisco 2015 Security Capabilities Benchmark Study

The Cisco 2015 Security Capabilities Benchmark Study examines defenders across three dimensions: resources, capabilities, and sophistication. The study includes organizations across several industries in 12 countries. In total, we surveyed more than 2400 security professionals, including chief information security officers (CISOs) and security operations (SecOps) managers. We surveyed professionals in the following countries: Australia, Brazil, China, France, Germany, India, Italy, Japan, Mexico, Russia, the United Kingdom, and the United States. The countries in the survey were selected for their economic significance and geographic diversity.

To read findings from the broader Cisco Security Capabilities Benchmark Study, get the Cisco 2016 Annual Security Report at www.cisco.com/go/asr2016.

About This Series

A team of industry and country experts at Cisco analyzed the Cisco 2015 Security Capabilities Benchmark Study. They offer focused insight on the security landscape in 10 countries and four industries (financial services, healthcare, telecommunications, and transportation). The white papers in this series highlight the security landscape and challenges that organizations face in cybersecurity. This process helped to contextualize the findings of the study and bring focus to the relevant topics for each country and industry we analyzed.

About Cisco

Cisco is building truly effective security solutions that are integrated, automated, open, and simple to use. Drawing on unparalleled network presence as well as the industry's broadest and deepest technology and talent, Cisco delivers ultimate visibility and responsiveness to detect more threats and remediate them faster. By calling on Cisco Security, companies are poised to securely take advantage of a new world of digital business opportunities.

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.**