White Paper

Security for Financial Services: Addressing the Perception Gaps in a Dynamic Landscape

Financial services organizations have a unique relationship with technology: electronic data and transactions are the core of this industry. Financial services firms remain vigilant because they are constantly under attack. Hackers that gain access to customer accounts or financial data can profit either by using it themselves or by selling it to other criminal organizations.

- There are many differences between perception and reality when it comes to security in this industry. For example, its emphasis on fraud prevention creates the perception that financial services is highly evolved in terms of its security readiness. However, this study finds that financial services firms' security is on a par with the security of firms in other industries.
- Regulations may lead to change and investments, but they also take time to take effect. Organizations should not wait for such requirements before they make improvements. Neither should they assume that compliance gives them full protection. Regulations cannot cover every aspect in such a fast-paced environment.

Major Findings

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

- Financial services firms that have suffered public breaches show less confidence in their security processes but more confidence in the tools they adopt.
- Financial services firms are less likely to use cloud-based security tools than firms in other industries. For example, 28 percent of the organizations in other industries use cloud-based vulnerability scanning, compared with 18 percent of financial services businesses.

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

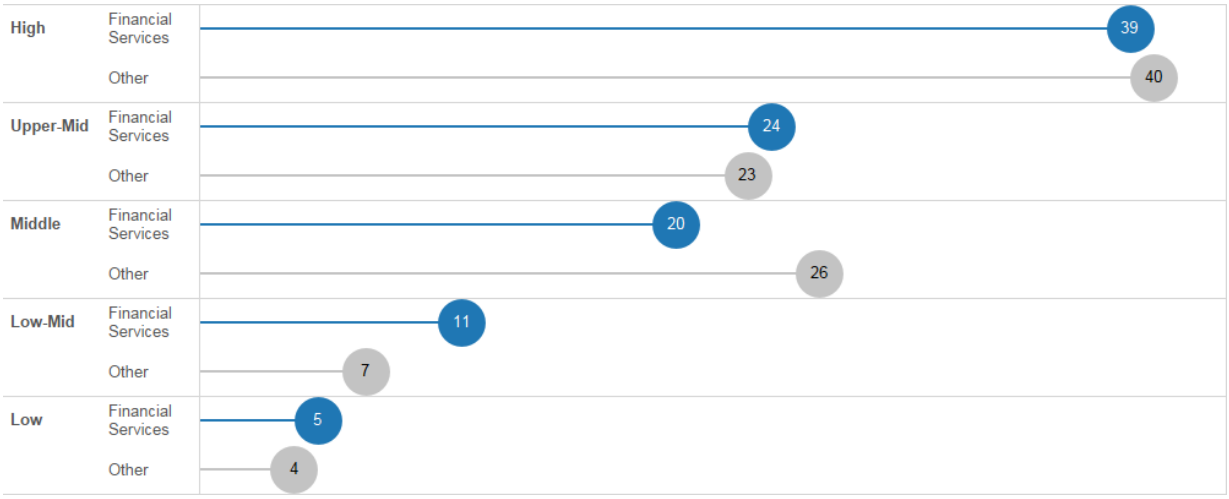
- Financial services firms are less likely to outsource security services: 28 percent say they do not outsource any functions to third parties, compared with 20 percent of firms in other industries.
- Contrary to security-industry perceptions, financial services firms show about the same level of security readiness as organizations in other industries. We categorized 63 percent of financial services organizations as either upper-middle or high in terms of security sophistication.
- Financial services organizations are as likely as, or slightly less likely than, other organizations to use certain security tools. For example, 39 percent of all other organizations we surveyed use penetration testing, compared with 37 percent of financial services firms.

Extending Security Sophistication beyond Fraud Prevention and Regulations

The perception of financial services is that of an industry with a highly evolved stance on security. This perception may be due to the industry's strong stand on fraud protection, an aspect that is very visible to end customers. Financial services organizations focus on ensuring that authentication and login procedures give only the right people access to their accounts. If they manage these procedures poorly, the financial losses could be damaging to both customers and providers.

However, the financial services sector shows about the same level of security sophistication as other industries we surveyed. Based on the responses of chief information security officers (CISOs) and security operations (SecOps) managers, we categorized 63 percent of financial services organizations as either upper-middle or high in terms of their security sophistication: that is, their level of advanced security operations and procedures (Figure 1).

Figure 1. Perceived Level of Security Sophistication (by Percentage of Respondents)



Multiple compliance guidelines and regulations apply to financial services organizations. However, these organizations cannot assume that complying with the many regulations provides sufficient defenses. Even though these regulations can spark change in the sector, they are not all encompassing and not systematically effective across all subsectors in all countries. In addition, it takes time for them to take effect.

Because online criminals are constantly targeting this industry, security professionals need to adapt faster than new regulations can be written. Otherwise businesses will face an impact on their financial performance and reputation. In 2015, the average cost of a successful data breach was $3.79 million, according to the Ponemon

Institute. Each record lost or stolen costs, in average, $154. However, for financial institutions, the cost per record is higher, at $215.[2]

With the stakes being so high for financial services firms, the gap that this survey identifies can be a warning that they still have work to do. The best strategy is to aim to be ahead of criminals.

Some industry bodies in this sector have already perceived the need to rethink its IT infrastructures. In 2013, the Basel Committee on Banking Supervision (BCBS) issued its principle for data aggregation and risk reporting, the BCBS 239.[3] The regulation will take effect for some financial institutions in January 2016. This regulation addresses how major banking organizations manage, aggregate, and report risk data, and it requires high investments in IT. The goal is not only to preserve the integrity of risk data but also to improve the way this data travels across the organization at various levels and how it supports decision making. The changes required by the principle will help banking organizations to transform IT into a business enabler and benefit their security readiness.

Even though the BCBS 239 applies only to a few banking organizations, other bodies across the financial services industry should follow its lead.

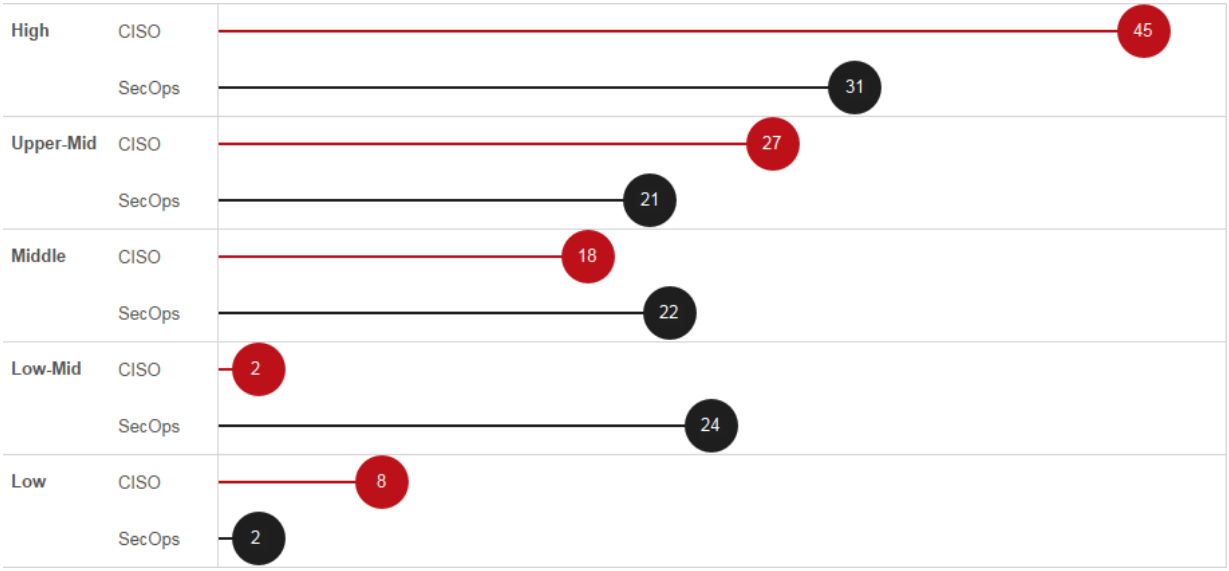
Gap in Perceptions between CISOs and SecOps Managers

As part of the security study, we surveyed CISOs and SecOps managers to compare their responses and to highlight the sometimes differing perceptions of their ability to protect their networks. Based on the CISO responses, we categorized 72 percent of financial services organizations as being in the top two levels of sophistication. On the other hand, only 52 percent of the responses from SecOps managers were at these same levels (Figure 2). The explanation for this gap may be that SecOps managers deal with more day-to-day security incidents, and therefore may be less confident about their company's security sophistication. On the other hand, CISOs work at a higher level and are somewhat distanced from the workday activities of their security teams. This gap, which is consistent with other industries, suggests that for more effective security operations, CISOs and SecOps managers should communicate better as well as regularly review and rank their security stance to identify possible gaps and close them.

[2] "Cost of Data Breach Study: Global Analysis", Ponemon Institute, May 25, 2015: http://www.ponemon.org/library/2015-cost-of-data-breach-global

[3] "Principles for Effective Data Risk Aggregation and Risk Reporting," Basel Committee on Banking Supervision, January 2013: http://www.bis.org/publ/bcbs239.pdf

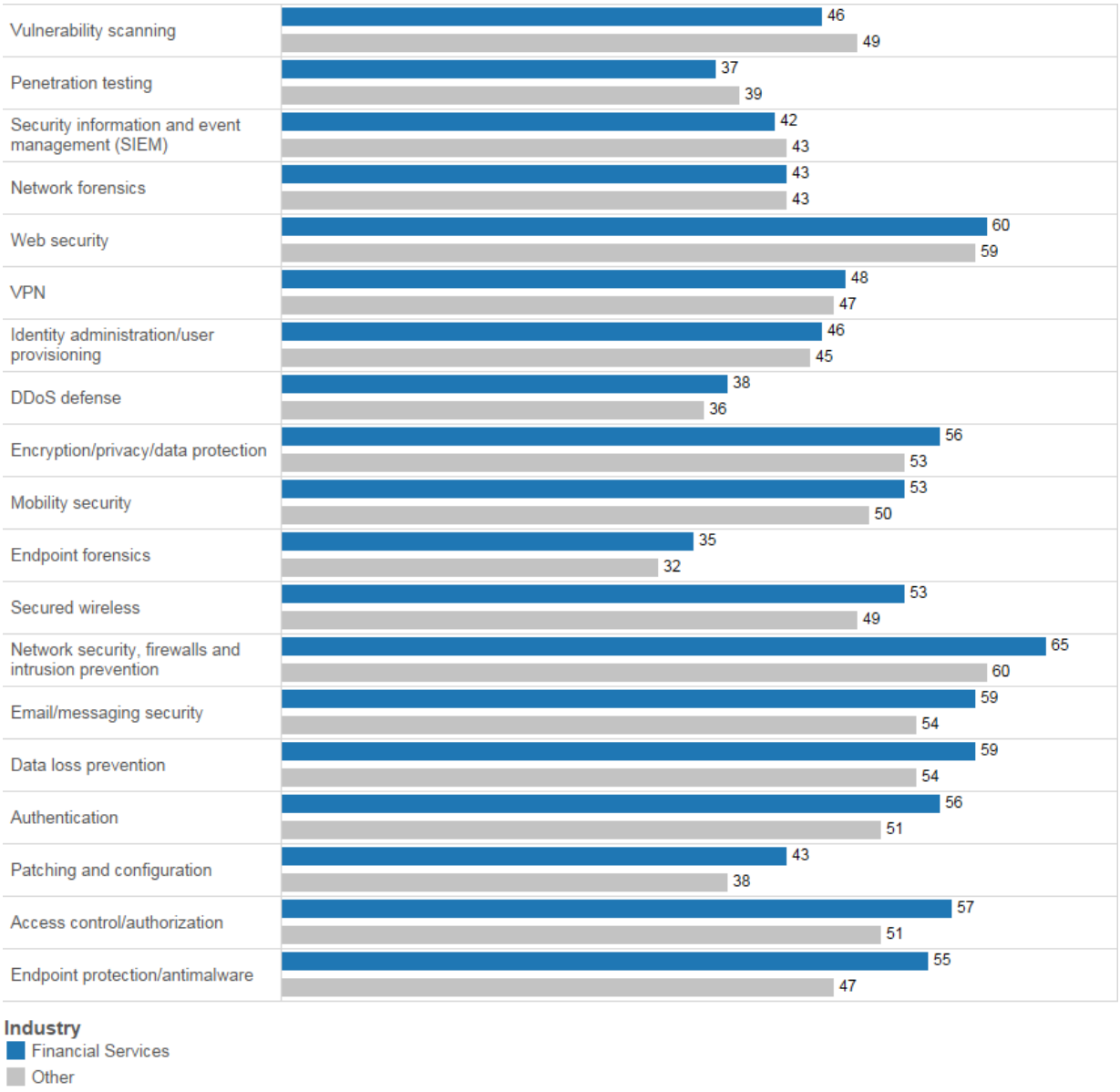
Figure 2. Perceived Level of Security Sophistication in Financial Services, by Role



Lower Deployment of Security Defenses

An important part of the financial services industry is managing transactions and customer information. Since these transactions and their associated information generate massive amounts of valuable data, financial services organizations are targeted by financially motivated cybercriminals. During a 12-month period between 2013 and 2014, hackers stole 500 million financial records in the United States, according to the FBI.[4] The financial losses from attacks against financial services firms can be higher than in other industries. Despite the higher stakes, financial services organizations' security defenses are similar to those in other industries (Figure 3).

Figure 3. Use of Various Threat Defenses (in Percentages)



[4] "Increasing Cyberthreats Pose Massive Challenge for Financial Firm," *InformationWeek*, January 8, 2015: www.wallstreetandtech.com/security/increasing-cyberthreats-pose-massive-challenge-for-financial-firms/d/d-id/1318144

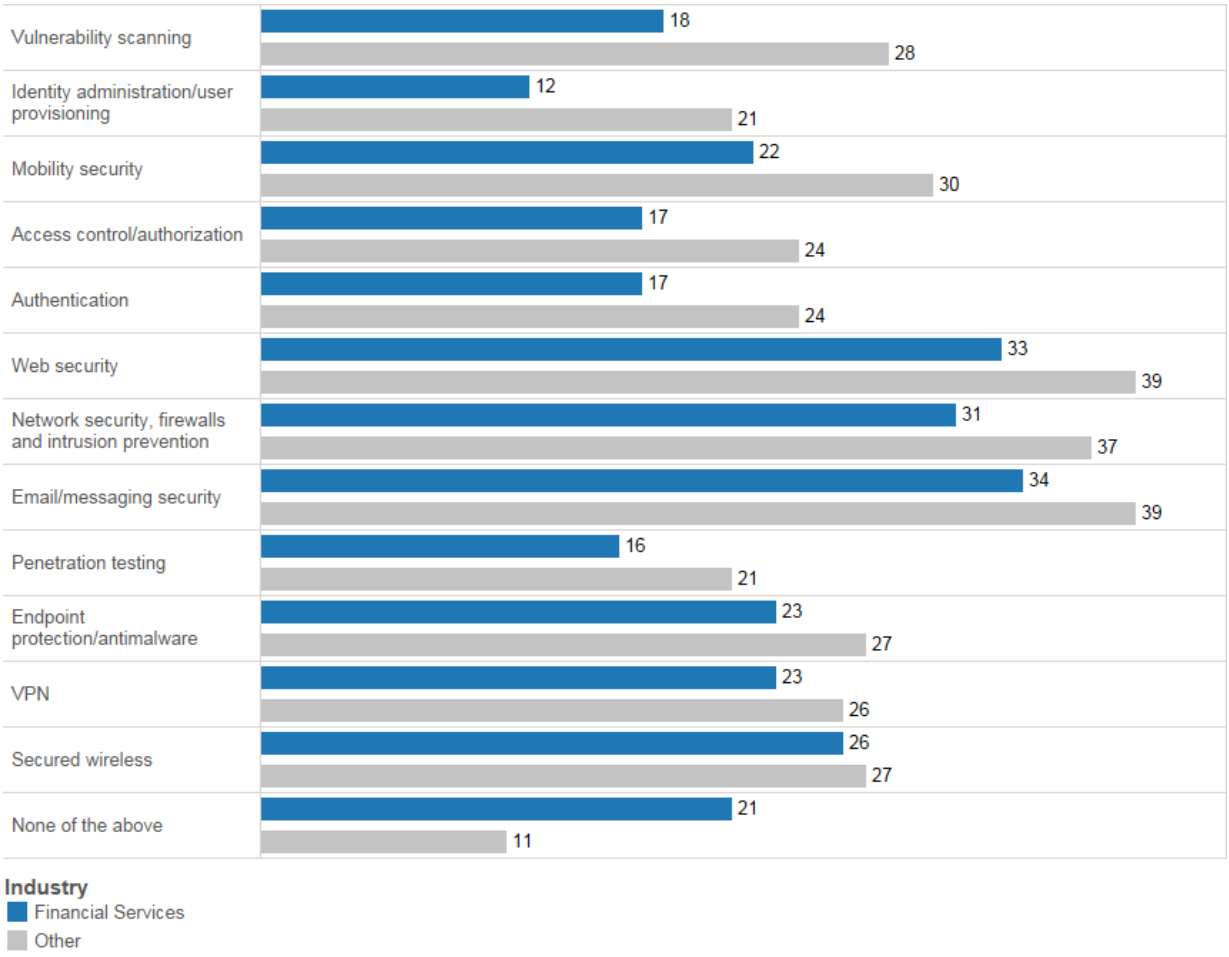
In a few cases, financial services organizations showed slightly higher use of threat defenses. For example, 55 percent use endpoint protection and antimalware, compared with 47 percent of organizations in other industries.

Lower Use of Cloud-Based Security Defenses

When it comes to security defenses, financial services organizations seem less likely to use the cloud than those in other industries. Twenty-eight percent of the organizations in other industries use cloud-based vulnerability scanning, compared with 18 percent of financial services organizations. In addition, 21 percent of the organizations in other industries use cloud-based identity administration and user provisioning, but only 12 percent of financial organizations do (Figure 4).

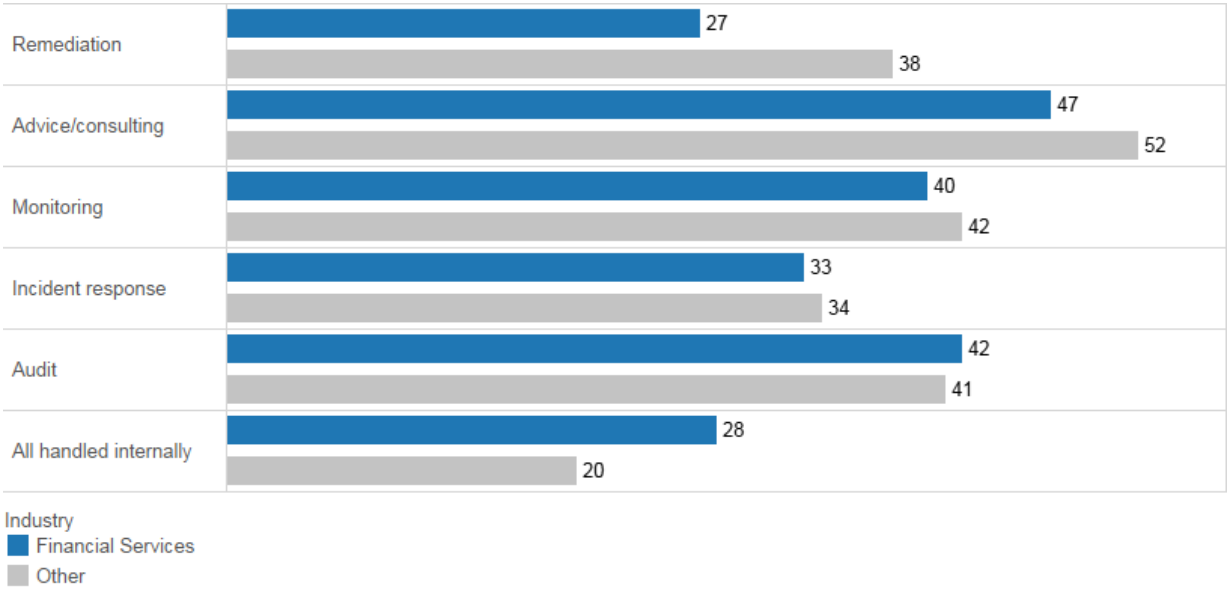
The conservative nature of financial services firms may be one of the reasons they are slow to adopt cloud defenses.

Figure 4. Adoption of Various Cloud-Based Defenses (in Percentages)



The industry's preference for maintaining control over data may also explain why financial services firms are less likely to outsource security services. Twenty-seven percent of financial services firms outsource security remediation, compared with 38 percent of organizations in other industries. In addition, 28 percent of financial services firms say they do not outsource any security functions to third parties, compared with 20 percent of firms in other industries (Figure 5).

Figure 5. Outsourcing of Various Security Functions (in Percentages)



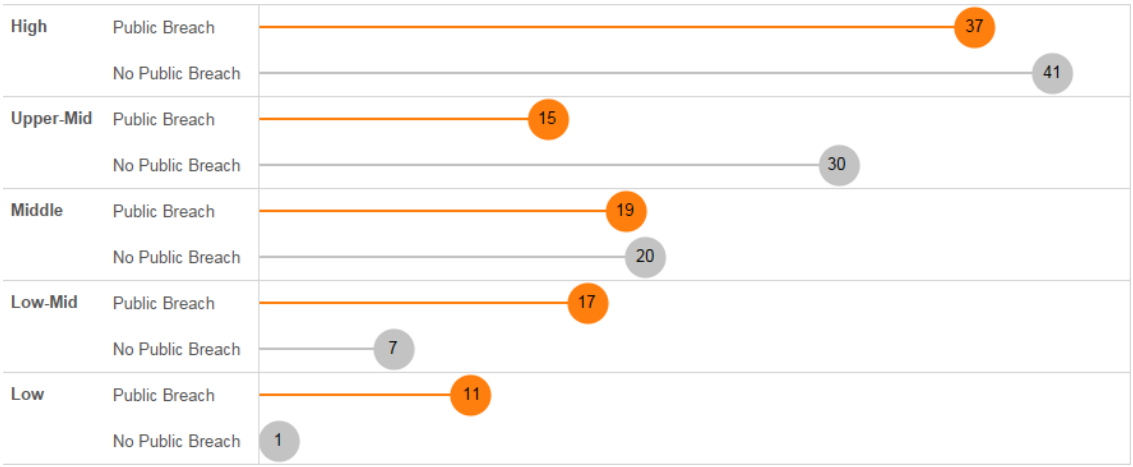
Public Breaches Affect Perceptions of Security Sophistication

Public breaches suffered by large financial services firms often receive widespread attention from the media and regulators, not only because the breaches involve sensitive financial data but also because they can affect the lives of many customers and damage a company's reputation. Perhaps for this reason, organizations in this industry become less optimistic about their security sophistication after a breach that results in public scrutiny, and they are more likely to adopt up-to-date security tools in response to the breaches.

In fact, based on their survey responses, we categorized 71 percent of non-publicly-breached firms in the upper-middle to high levels of sophistication, compared with 52 percent of publicly breached firms (Figure 6). On the other hand, 74 percent of publicly breached organizations believe their security infrastructure is up to date and constantly upgraded with new technologies, while only 65 percent of non-publicly-breached firms believe the same.

These results suggest that publicly breached financial organizations may have greater faith in their security tools instead of their processes. It is also likely that publicly breached companies simply believe that they have protected themselves from at least a few known attack vectors.

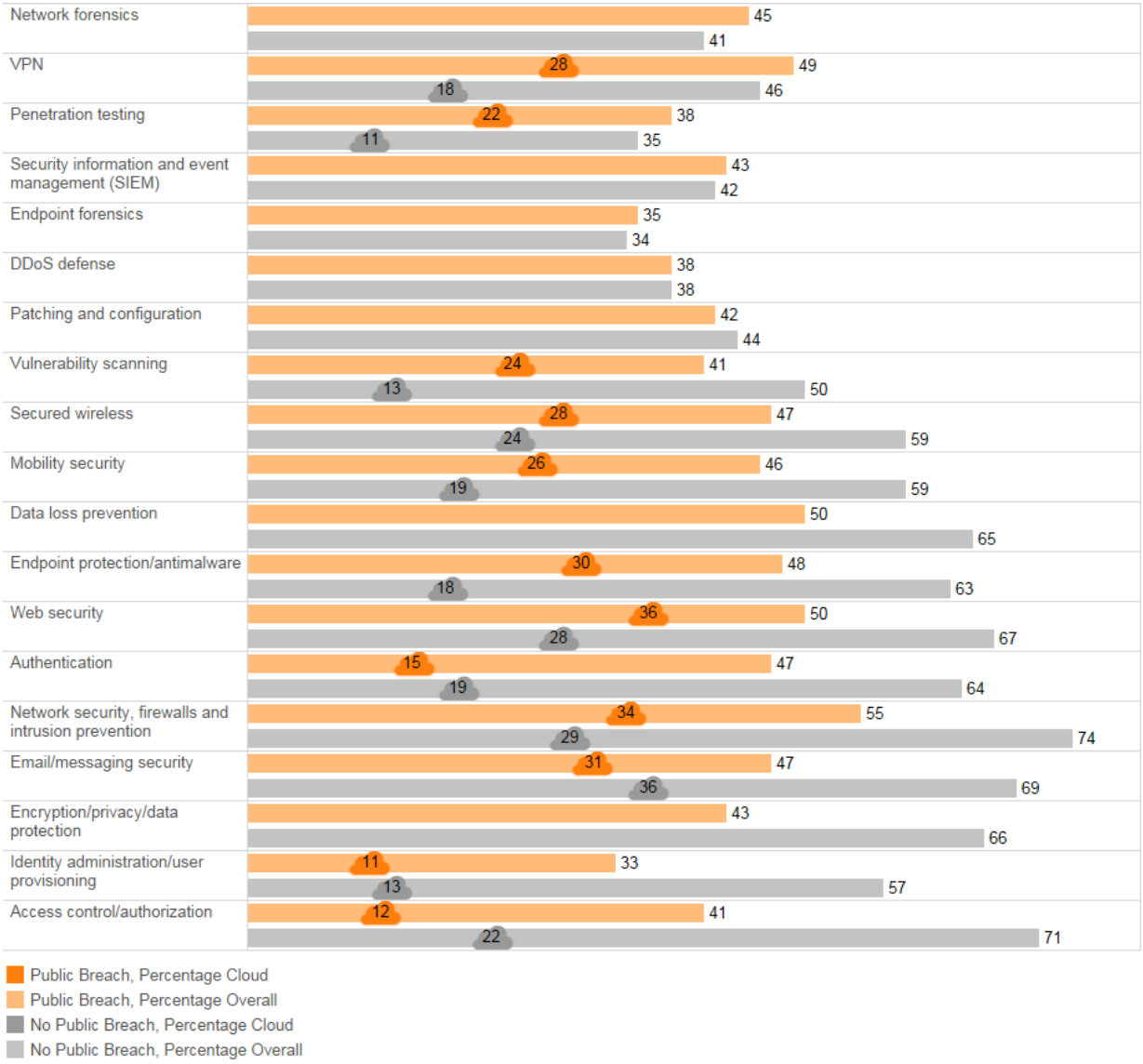
Figure 6. Security Sophistication as Perceived by Publicly Breached and Non-Publicly-Breached Organizations (in Percentages)



Interestingly, financial services firms that have suffered public scrutiny following a breach appear less likely to use threat defenses than those companies that have not suffered a public breach. For example, 50 percent of non-publicly-breached firms use vulnerability scanning, compared with 41 percent of publicly breached firms. In addition, 63 percent of non-publicly-breached firms use endpoint protection and antimalware solutions, compared with 48 percent of firms that have suffered a public breach (Figure 7).

External cloud-based security tools appear to be more widely adopted among financial services firms that have dealt with a public breach. For example, 30 percent of publicly breached firms use cloud-based endpoint protection and antimalware tools, compared with 18 percent of non-publicly-breached firms. In addition, 24 percent of publicly breached firms use cloud-based vulnerability scanning, compared with 13 percent of non-publicly-breached firms (Figure 7).

Figure 7. Use of Various Security Tools, by Public Breach (in Percentages)



Publicly breached financial services firms are also less likely to use processes that help eliminate the causes of security incidents. For example, 67 percent of non-publicly-breached financial services firms use root cause analysis, compared with 50 percent of publicly breached firms. Additionally, 62 percent of non-publicly-breached firms use tools that stop malware communication, compared with 50 percent of firms that have suffered a public breach (Figure 8).

Figure 8. Use of Various Tools to Identify Causes of Security Incidents, by Public Breach (in Percentages)

Conclusion: Adapting to the Changing Threat Landscape

The security landscape changes rapidly, and organizations must keep up with new technologies to combat evolving threats. Although the financial services industry is at a similar level of security readiness as other industries, the stakes are especially high in this industry, and the cross-industry survey results suggest there is room for improvement, especially given the fact that online criminals perennially target this industry.

Financial services security professionals should:

- Increase the focus of their security strategy beyond fraud prevention—for example, they should implement vulnerability scanning, penetration testing, and security information and event management
- Consider tools and processes that build agility into the security infrastructure, such as cloud tools, and rely more on third-party consulting services
- Improve the collaboration between CISOs and SecOps managers in order to improve their overall security protection posture
- Improve collaboration between the CISO, CEO, and board of directors to help ensure that the security protection posture matches the organizational tolerance for risk
- Examine pre-breach and post-breach security postures across the security landscape.

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