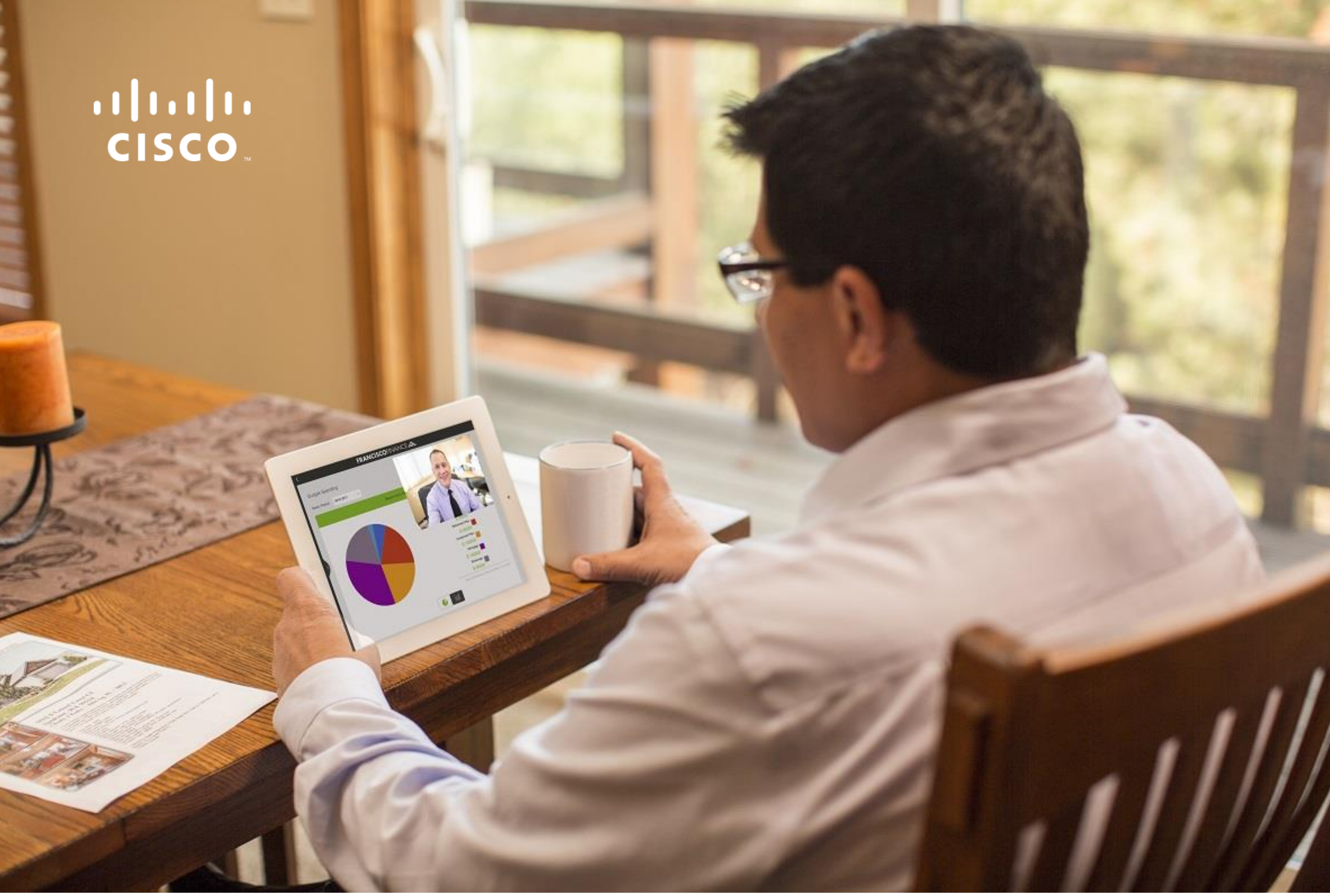


Security in Financial Services: Managing the Complexity of Digital Transformation

Financial services organizations are seeking opportunities to use technology to define, differentiate, or enable their business strategies. They view digital transformation as a way to capture business value, disrupt the market, and pull ahead of competitors. However, with digital ability comes complexity. The growth of digital tools increases the likelihood that competing security forces will arise within organizations that do not work in unison to fight cybersecurity risks.

Financial services organizations need to manage complexity by rethinking security strategies to better align with the speed of change in this dynamic market:

- Because security in organizations lags behind growth and innovation initiatives, line-of-business (LOB) managers are taking more control of IT. Their unauthorized projects create “shadow IT” implementations that cause security difficulties.
- To meet the challenges of a complex digital environment, financial services organizations are increasing their use of outside security experts. It’s a sign that the industry’s security professionals are choosing expert help to address their concerns.

Major Findings

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

- Line-of-business managers are taking on more responsibility for security. In 2014, 46 percent of our respondents said that their line-of-business managers contributed to security policies and procedures; in 2015, that number rose to 59 percent.
- The industry recognizes the value of outside expertise in improving security defenses. Businesses increased their outsourcing of external incident response and analysis teams. In 2014, 33 percent used them, compared with 43 percent in 2015.
- Financial services organizations are decreasing their use of tools to help detect and block threats. In 2014, 57 percent of survey respondents said they used access control and authorization tools. The number dropped to 48 percent in 2015. In 2014, 43 percent said they used network forensics tools, but only 32 percent used them in 2015.
- Financial services organizations recognize that people are as essential to improving security as technology tools are. They are therefore acknowledging the value of training. Forty-four percent of chief information security officers (CISOs) said they have increased security awareness training among employees and also increased investment in training for security staff.

Security Adapts to Complex Digital Environments

Digital growth is now seen as essential to financial services success. If organizations possess digital business ability, they can detect threats quickly, before those threats can restrict new market opportunities. Financial services executives recognize the value of digitization: According to our recent study, “Cybersecurity as a Growth Advantage,” 69 percent of executives across all industries said digitization is very important to their current growth strategy.[2]

However, they also recognize that poor security can wreak havoc with these ambitious plans. In the same Cisco study, 71 percent of executives said that concerns over cybersecurity are impeding innovation in their organizations. Thirty-nine percent said that they had halted mission-critical initiatives because of cybersecurity issues.

These views were echoed in a recent survey of public companies by NYSE Governance Services: 43 percent of company directors said ensuring the security of new products and services was one of the main barriers to keeping up with the pace of innovation in their industry.[3] If financial services businesses are to invest in digitization successfully, they must also invest in security to protect digital processes and data.

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

[2] “Cybersecurity as a Growth Advantage,” Cisco, April 2016: http://www.connectedfuturesmag.com/CyberSecurity/

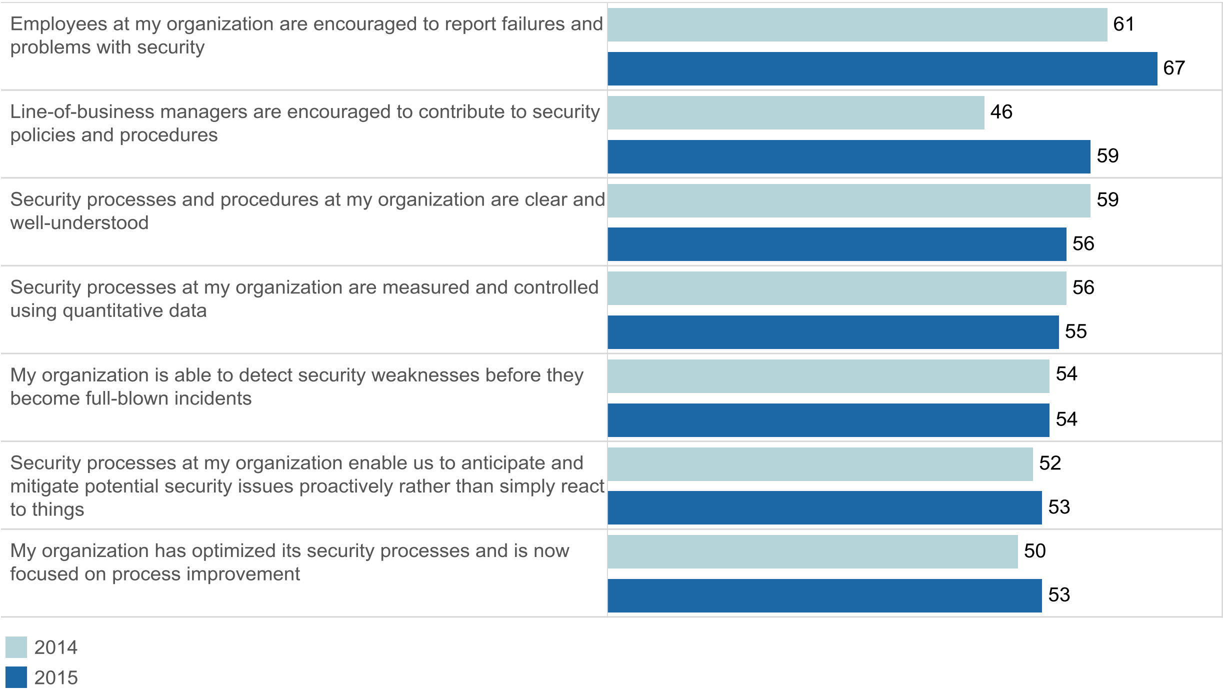
[3] *Cybersecurity in the Boardroom*, NYSE Governance Services, May 2015: https://www.nyse.com/publicdocs/VERACODE_Survey_Report.pdf

Line-of-Business Managers Adopt a Greater Role in Security

To keep up with the demands of digitization, business units sometimes try to manage security issues on their own, without direction from security leaders. These attempts lead to the “shadow IT” problem. For example, in an effort to improve the customer experience or to change business processes more quickly, lines of business (LOBs) often implement technology without the consent or support of the IT or security team. However, such practices can affect visibility into the extended network and affect the security team’s ability to enforce policies on every server, application, and device. These practices can also damage the ultimate goals of digital agility, including a hyperawareness of changes in a business environment.

Because a breach caused by an LOB-installed device can damage an entire business, it is important that departments understand the downside of “shadow IT” operations. The good news is that in a growing number of financial services organizations, line-of-business managers are taking on more responsibility for securing the business. In 2014, 46 percent of our survey respondents said that their line-of-business managers were encouraged to contribute to security policies and procedures. In 2015, that number rose to 59 percent (Figure 1).

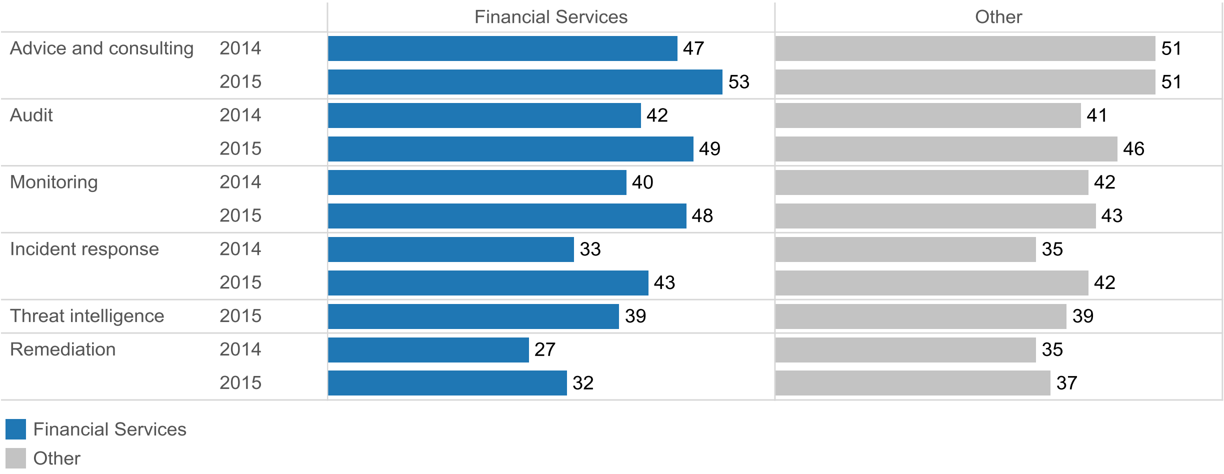
Figure 1. Percentages of Organizations Agreeing with Various Statements About Their Organizations’ Security Processes, 2014 and 2015



Outsourced Expertise Helps Close Gaps in Security Defenses

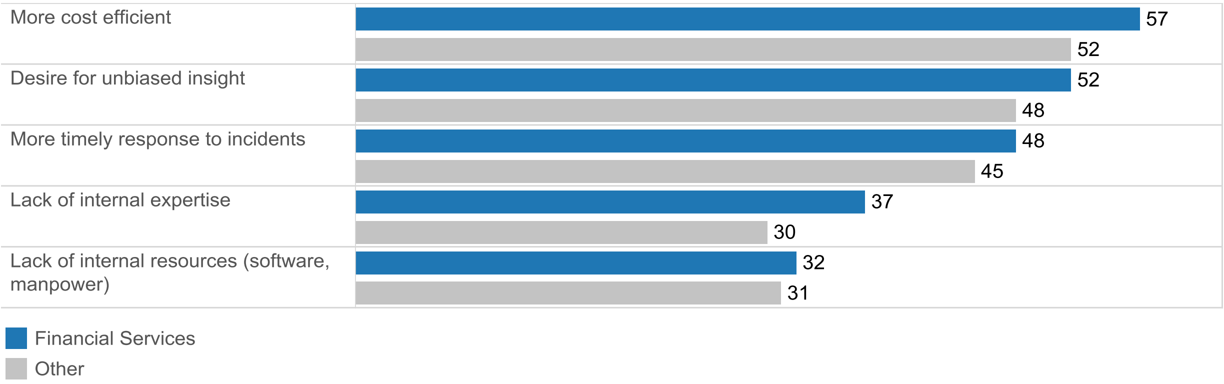
If financial services organizations are committed to growth through digital offerings, they must also recognize that cybersecurity is the foundation for this growth. “Secure digitizers” understand that digitization is a path to success, not simply a defensive tactic. They also understand that digitization raises complex questions. How, for example, can a business extend value to customers while protecting its data? Accessing outsourced tools and experts is on the increase in financial services organizations. In 2015, these organizations appeared more prone to outsource security services than they were in 2014. For example, they increased their use of external incident response. In 2014, 33 percent used an outside team, compared with 43 percent in 2015 (Figure 2).

Figure 2. Percentages of Organizations Outsourcing Various Security Services, 2014 and 2015



This industry increasingly recognizes that it needs outside help. Respondents in 37 percent of the organizations that outsource security services mentioned they lacked internal expertise. Only 30 percent in other industries said the same (Figure 3).

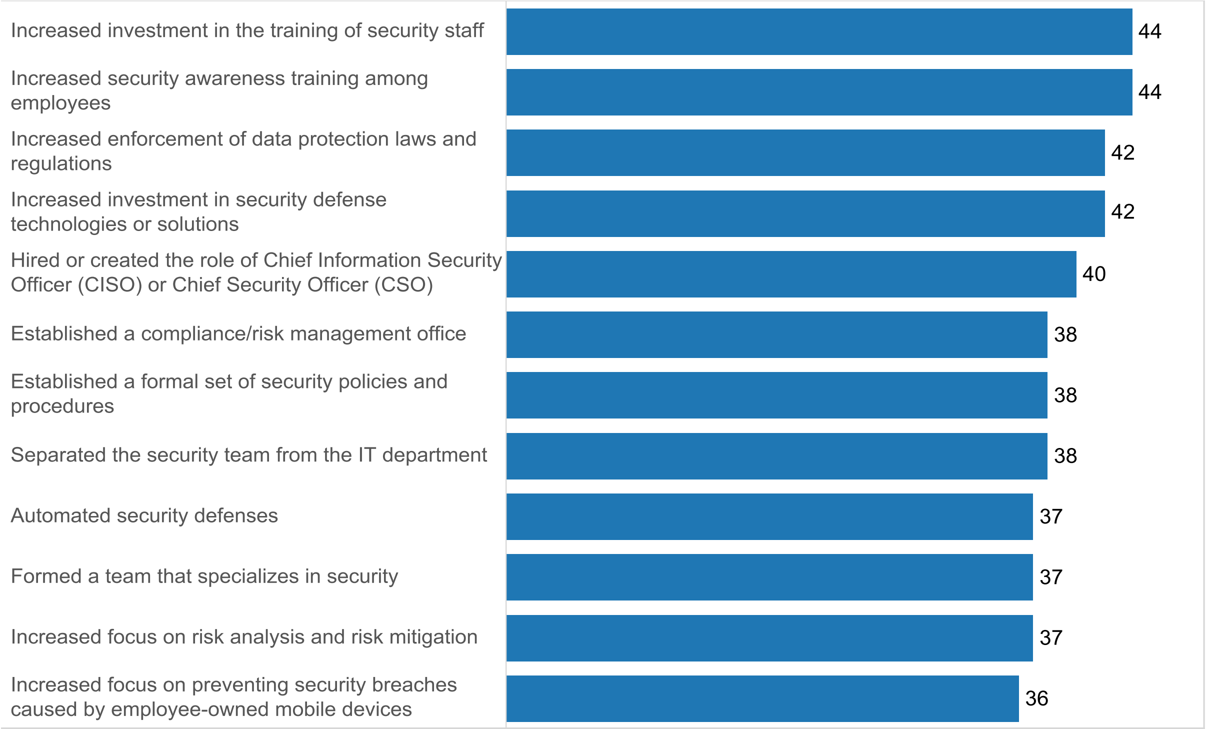
Figure 3. Reasons Why Financial Services Organizations Outsource Security Services



Training Addresses the Need for Skilled Personnel

Training staff both inside and outside the security team helps fight threats to security agility. Financial services organizations are increasing their training sessions. It’s a smart move, because fighting threats requires skilled personnel as well as integrated technologies. For example, in the organizations that dealt with public scrutiny due to a data breach, 44 percent of the respondents said they have increased security awareness training among employees and also increased their investment in training for security staff (Figure 4).

Figure 4. Percentages of Organizations Taking Various Steps to Strengthen Their Security

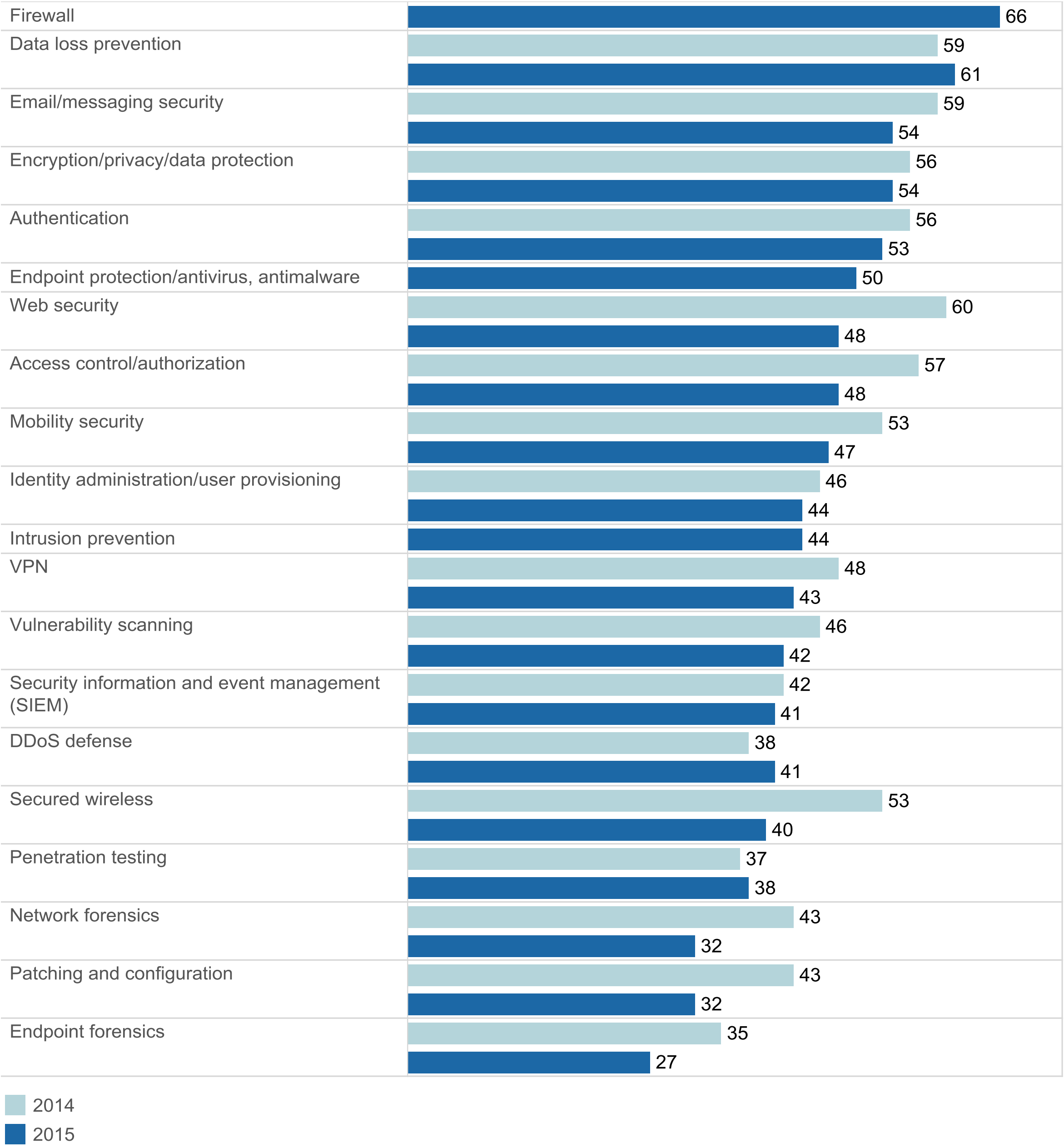


Consolidating the Use of Threat Defense Tools

As financial services organizations view cybersecurity as a competitive advantage and call on experts to build a security architecture framework, they may be less likely to rely on separate security tools. On the other hand, a consolidation in the use of threat defense tools could mean that financial services organizations are not fully responding to complex security needs.

In 2014, 57 percent of survey respondents said they used access control and authorization tools, but the number dropped to 48 percent in 2015. In 2014, 43 percent said they used network forensics tools, while only 32 used them in 2015 (Figure 5).

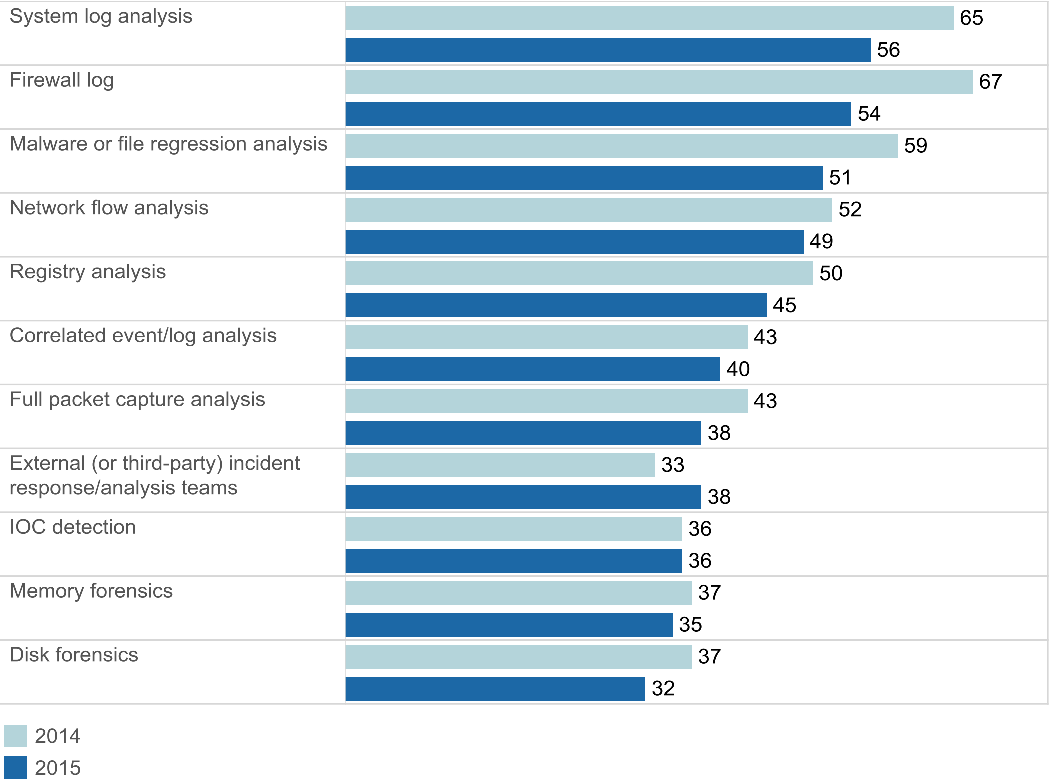
Figure 5. Percentages of Organizations Using Key Security Threat Defenses, 2014 and 2015



Note: Firewall, intrusion prevention, and endpoint protection/antivirus and anti-malware were added as independent items in 2015. Therefore, 2014 percentages are not available for those defenses.

Financial services organizations also show a decline in their use of processes to analyze compromises and eliminate the causes of security incidents. In 2014, 65 percent of financial services organizations used system log analysis; in 2015, only 56 percent did (Figure 6). Also in 2014, 49 percent used reimaging tools to restore systems to their previous state; in 2015, only 39 percent did.

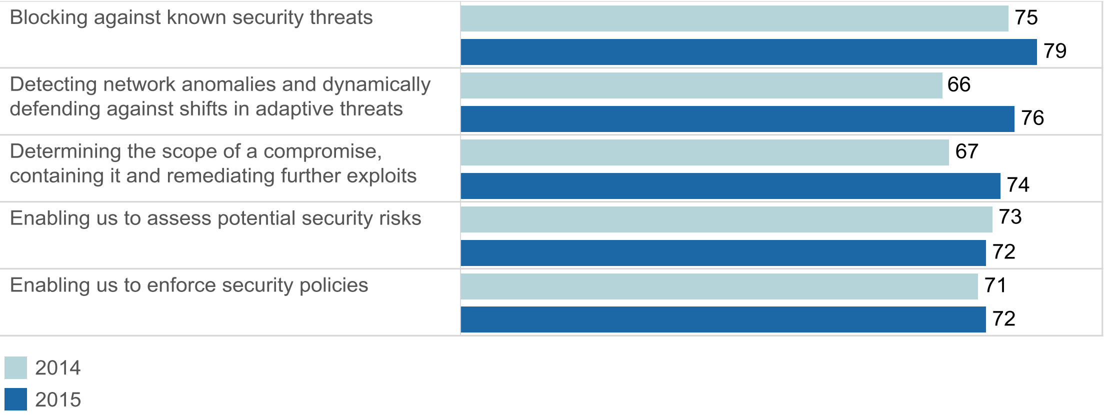
Figure 6. Percentages of Orgs. Using Various Processes to Analyze Compromises and Eliminate Incident Causes



Higher Confidence in Security Effectiveness

Financial services organizations need to continuously improve the integration and sophistication of their threat defenses. Their currently stronger focus on training and reliance on outside experts may contribute to a growing confidence in their security capabilities. In 2014, 66 percent said their systems were highly effective in detecting network anomalies and defending against shifts in threats. In 2015, that number rose to 76 percent. Likewise, in 2014, 67 percent said that their security tools were highly effective in determining the scope of a compromise. That number rose to 74 percent in 2015 (Figure 7).

Figure 7. Percentages of Respondents Confident in the Effectiveness of Their Security Tools for Various Tasks



Conclusion: Build Security into the Ground Level of Digital Initiatives

There are signs that financial services organizations are staking their success on digital business models and are building security into the foundation of their plans. However, there are also signs that indicate danger for businesses–such as "shadow IT" operations and a decline in the use of common threat defense tools.

Innovation and agility are essential to competitiveness in the financial services world. When done well, security plays as much of a role in market position as products, customer service, and leadership. Security is crucial to compliance and to smooth, efficient business operations. To reach the point where security is an enabler of success, financial services need to lay the groundwork with consistent, sophisticated technologies and processes, as well as capable people. These three elements need to work in harmony. This ideal state is more achievable if security is part of the original plan when organizations adopt a new technology.

By building in security from the beginning of a corporate initiative, financial services organizations can avoid fragmented security elements and potential gaps. Financial services security professionals should:

- Place threat intelligence at the center of their defense strategy in order to gain the hyperawareness needed for success and to allow for fast, intelligent decision making about threats
- Evaluate the use of outsourced expertise to overcome the issues of complexity on the path to digitization
- Work closely with line-of-business managers for a unified and consistent approach to security, and share with them the importance of security as a growth enabler

Accelerating Toward Secure Digitization

Security enhancements should be considered as part of the same conversation about digitalization plans. Here are some best practices for using security as a competitive differentiator:

- Mitigate risk by choosing projects with a high opportunity-to-risk ratio, not just a low-risk profile. Secure digitizers take more risks, but the rewards outweigh the costs.
- Re-engineer digital processes using cybersecurity as the foundation. Identify insecure technologies and the business processes they enable. Replace these technologies by others that integrate cybersecurity from the start
- Improve cybersecurity expertise at all levels of the organization. The same proactive measures that help companies excel in cybersecurity can also boost product development, risk resilience, threat analysis, and response in other parts of the business.

To find out more about the importance of security to organizations' competitive posture, read the "Cybersecurity as a Growth Advantage" report at www.connectedfuturesmag.com/cybersecurity.

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.**