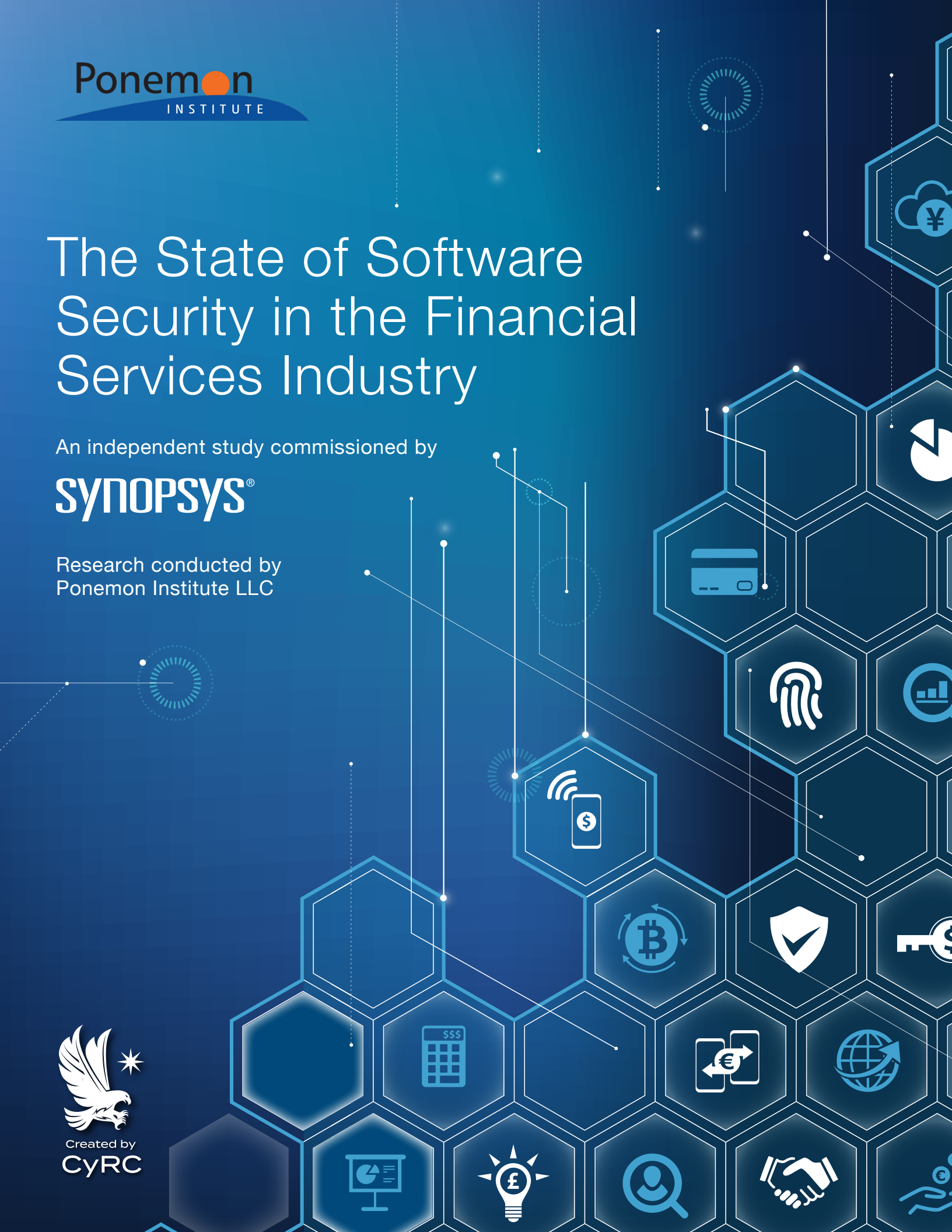
Ponemon INSTITUTE

The State of Software Security in the Financial Services Industry

An independent study commissioned by

SYNOPSYS®

Research conducted by
Ponemon Institute LLC



Created by
CyRC

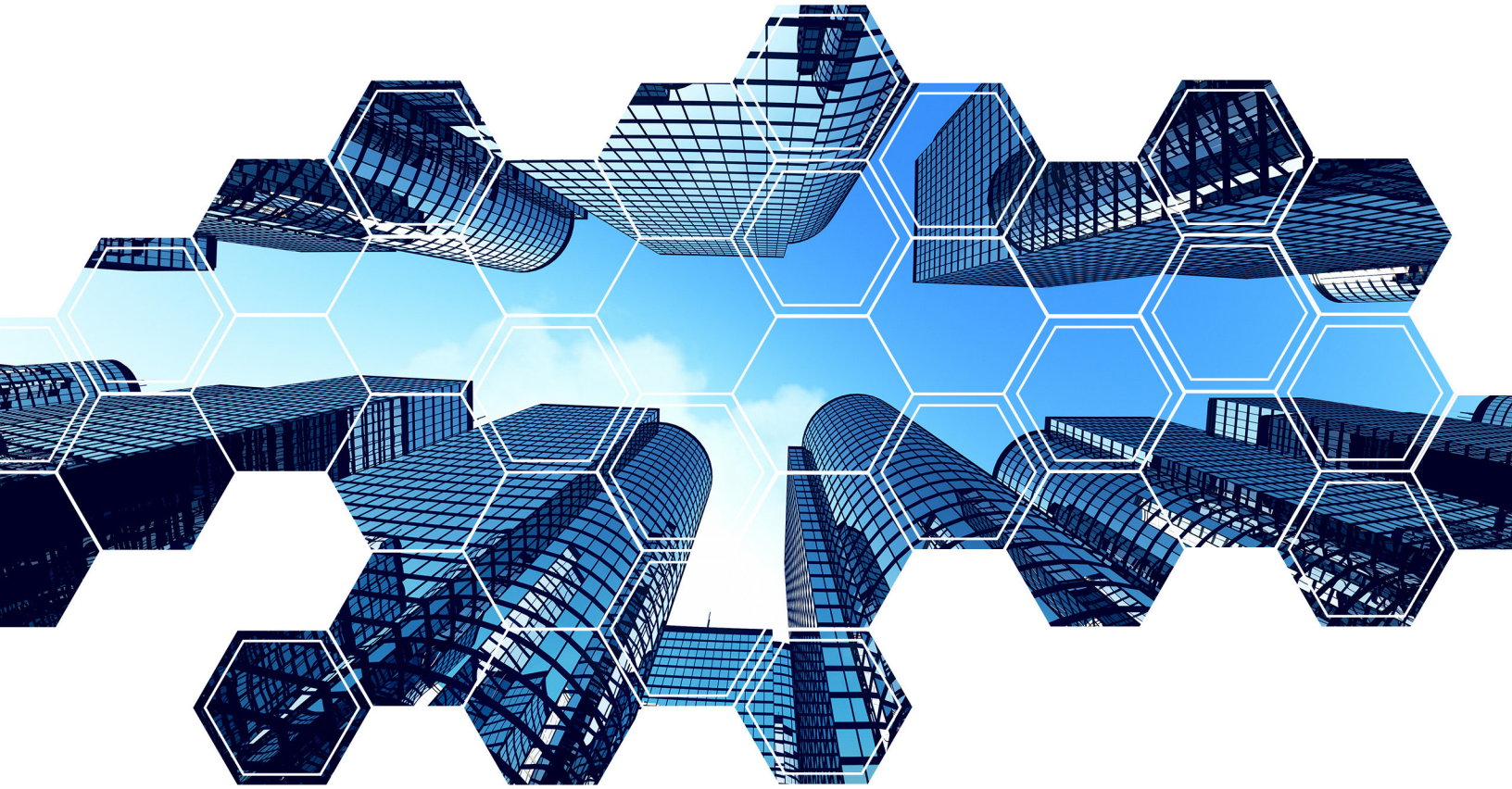
Table of Contents

About This Report

Under commission of the Synopsys Cybersecurity Research Center (CyRC), Ponemon Institute conducted an independent survey of current software security practices in the financial services industry (FSI) to understand the industry's software security posture and its ability to address security-related issues. This report, The State of Software Security in the Financial Services Industry (SS-FSI), is the result of that research.

Operating within the Synopsys charter of making software secure and high quality, CyRC regularly publishes research to support strong cybersecurity practices. Publications include the annual Open Source Security and Risk Analysis (OSSRA), a report providing an in-depth look at the state of open source security, compliance, and code quality risk in commercial software, and Securing the Modern Vehicle, a joint report issued by Synopsys and SAE International addressing software security risks inherent in connected, software-enabled vehicles.

For the SS-FSI report, Ponemon researchers surveyed over 400 IT security practitioners in various sectors of the financial services industry, including banking, insurance, mortgage lending/processing, and brokerage. Participant roles include installing and implementing financial applications, developing financial applications, and providing services to the financial services industry. See **Methods** and the **Appendix** for full information on survey methodologies and participants.



Executive Summary

A flood of new technology is racing toward the financial services industry—most notably, increased automation for internal processes to improve margins, as well as the development of new software to create a complete and seamless customer experience in traditional, online, and mobile banking.

Technology is deeply embedded in every FSI business. No bank or insurer could run without it. But as this report demonstrates, most FSI organizations are struggling to secure the technologies they already use. More than half of the FSI organizations surveyed for this report have experienced attacks resulting in customer data theft or system failure and downtime.

Clearly, cybersecurity is not keeping pace with technology advances in the financial services industry, and the issue will only worsen unless proactive steps are taken now.

Cybersecurity is a very real problem for FSI

Our report illustrates the need for FSI organizations to focus more on cybersecurity, secure coding training, automated tools to find defects and security vulnerabilities in source code, and software composition analysis (SCA) tools to identify open source components introduced by internal development teams or external suppliers.

FSI organizations are still building up needed software security skills and resources. While most provide some form of secure development training for software developers, only a small percentage require (or mandate) such training. In addition, to determine the effectiveness of their security programs, FSI organizations are more likely to rely on internal assessments than to use external assessment tools such as the BSIMM (Building Security In Maturity Model) or the SAMM (Software Assurance Maturity Model).

The most common factor that renders software vulnerabilities is vulnerability testing occurring too late in production. Yet we found that most FSI organizations conduct vulnerability assessments after software release, probably owing to a lack of application security expertise, concerns about costs, and a fear that security processes earlier in the software development life cycle (SDLC) might impede development and slow response to market conditions.

Less than half of survey respondents said security assessments occur during software design or development and testing, and only 25 percent of respondents were confident that their organizations can detect security vulnerabilities in their financial software and systems before release.

The FSI software supply chain presents a major risk

While most FSI organizations still develop their own software and systems, many are becoming reliant on third-party independent vendors to deliver the latest technology. While nearly three-quarters of respondents surveyed in our report are gravely concerned about the possibility of security vulnerabilities introduced by third-party suppliers, less than half of their organizations require third parties to adhere to specific cybersecurity requirements or to verify their security practices.

Few of the FSI organizations surveyed have an established process for inventorying and managing open source code either developed internally or delivered by third parties. The lack of open source management exposes organizations to additional risk from vulnerabilities in the open source components in their applications.

There's not one correct approach to securing FSI software and systems

No single method, tool, or service will ensure complete security coverage for any FSI organization.

Some organizations prefer lean security teams that take advantage of managed service providers; others prefer larger security teams with more in-house expertise.

Some organizations use a layered approach of automated tools, including SCA (software composition analysis); SAST, IAST, and DAST (static, interactive, and dynamic application security testing); and RASP (runtime application self-protection). Other strategies include manual planning and testing activities such as secure architecture design, security requirements definitions, threat modeling, code review, and fuzz testing to ensure security at every phase of the SDLC.

The only correct approach is the one that aligns with, supports, and protects the business. An interesting data point in this report is that the majority of respondents felt their organizations are much more effective in detecting and containing cyberattacks than in preventing those attacks. With a stronger focus on security, especially on injecting security earlier into the SDLC, FSI organizations will have a better chance of preventing attacks rather than dealing with the consequences and costs of those attacks.

Survey Findings in Detail

This section provides a deeper dive into the research findings, organized into the following topics:

- The software security posture of financial services companies
- Risks to financial software and applications
- Security practices in the design and development of financial service software and technologies

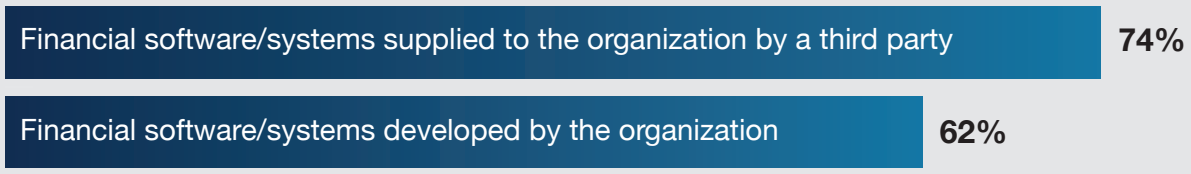
The complete audited findings are presented in the Appendix.

The Software Security Posture of Financial Services Companies

FSI organizations worry more about software and systems supplied by third parties than those they develop themselves.

Most financial services organizations use financial software and systems supplied by third parties and develop financial software and systems themselves. While the vast majority of respondents worry about security vulnerabilities introduced by third parties (see Figure 1), only 43 percent said their organizations require third parties to adhere to cybersecurity requirements or to verify their security practices.

Figure 1. How concerned are you about the cybersecurity posture of financial software and systems developed by your organization or supplied by a third party?
Shows responses of 7–10 on a scale from 1 = not concerned to 10 = very concerned

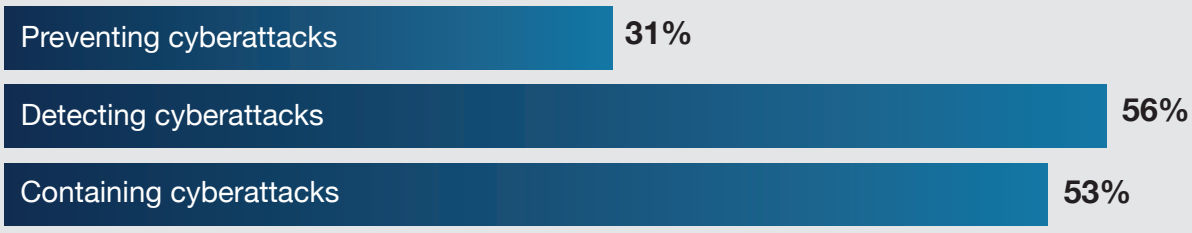


Respondents felt that their organizations are more effective in detecting and containing cyberattacks than in preventing attacks.

Respondents were asked to rate their effectiveness in preventing, detecting, and containing cyberattacks from a scale of 1 = ineffective to 10 = very effective.

As shown in Figure 2, the majority of respondents were confident in their organizations' effectiveness in detecting and containing attacks but less so in preventing an attack.

Figure 2. How effective is your organization in preventing, detecting, and containing cyberattacks?
Shows responses of 7–10 on a scale from 1 = ineffective to 10 = very effective



Most FSI organizations have a traditional IT cybersecurity program or team in place.

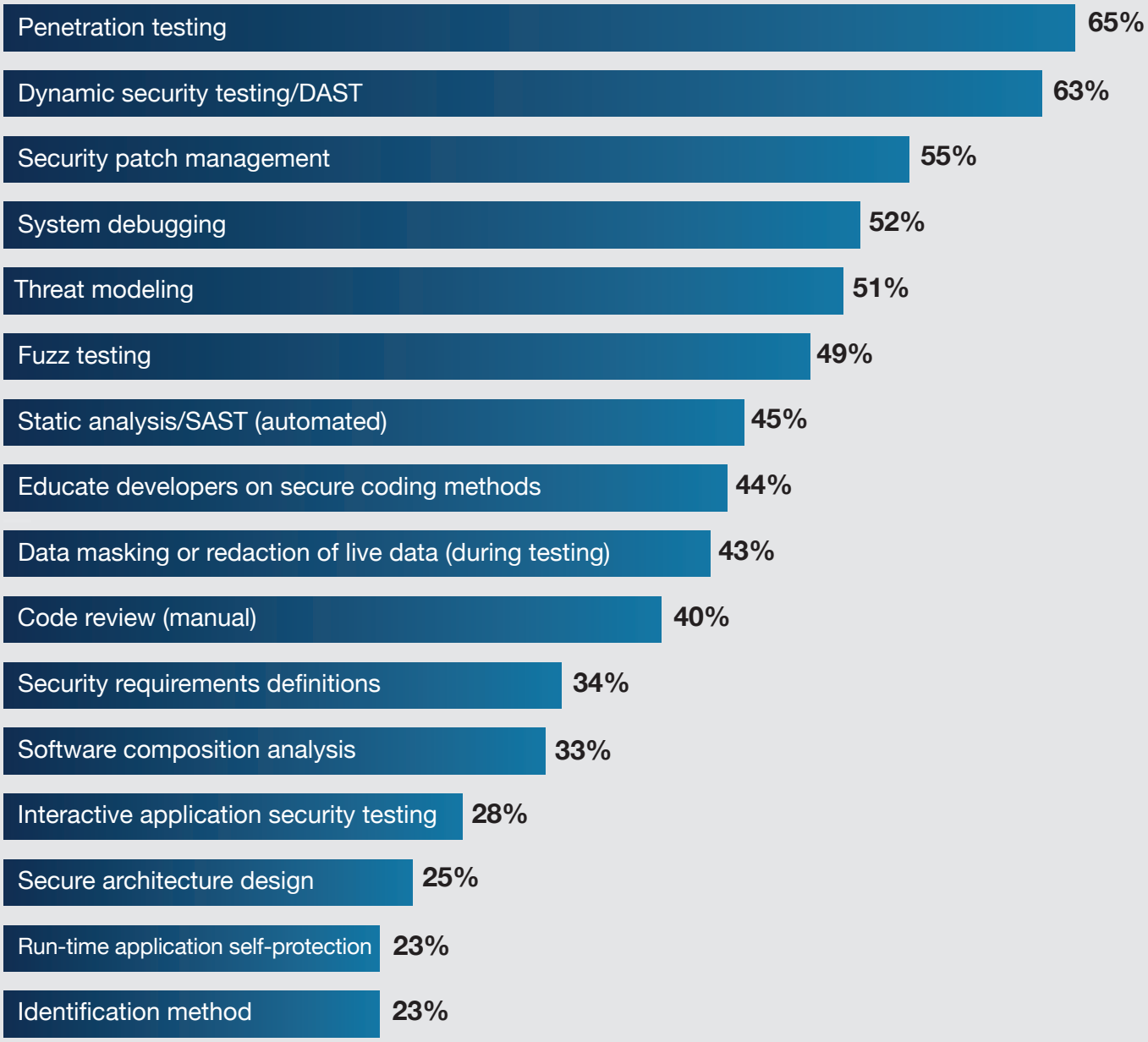
Sixty-seven percent of respondents said their organizations have a cybersecurity program or team. As shown in Figure 3, 60 percent said cybersecurity is part of the traditional IT cybersecurity team, and more than half (51 percent) said the cybersecurity team is decentralized, with cybersecurity experts attached to specific product development teams. Only 23 percent said cybersecurity is the responsibility of product development.

Figure 3. What is your organization's approach to cybersecurity?
Of the 67% of respondents whose organizations have a cybersecurity program or team
More than one response permitted

Respondents consider pen testing and dynamic security testing (DAST) to be the most effective in reducing cybersecurity risks.

Sixty-five percent of respondents said pen testing and 63 percent said dynamic security testing (DAST) are the most effective activities in reducing cybersecurity risks. Also noted as effective are security patch management, system debugging, and threat modeling.

Figure 4. What activities are most effective in reducing cybersecurity risks?
More than one response permitted



Respondents felt their organizations need more resources and in-house expertise to mitigate cybersecurity risks.

As shown in Figure 5, only 45 percent of respondents said they have adequate budget to address cybersecurity risks, and only 38 percent said their organizations have the necessary cybersecurity skills.

Figure 5. My organization allocates enough resources for cybersecurity and has the necessary cybersecurity skills

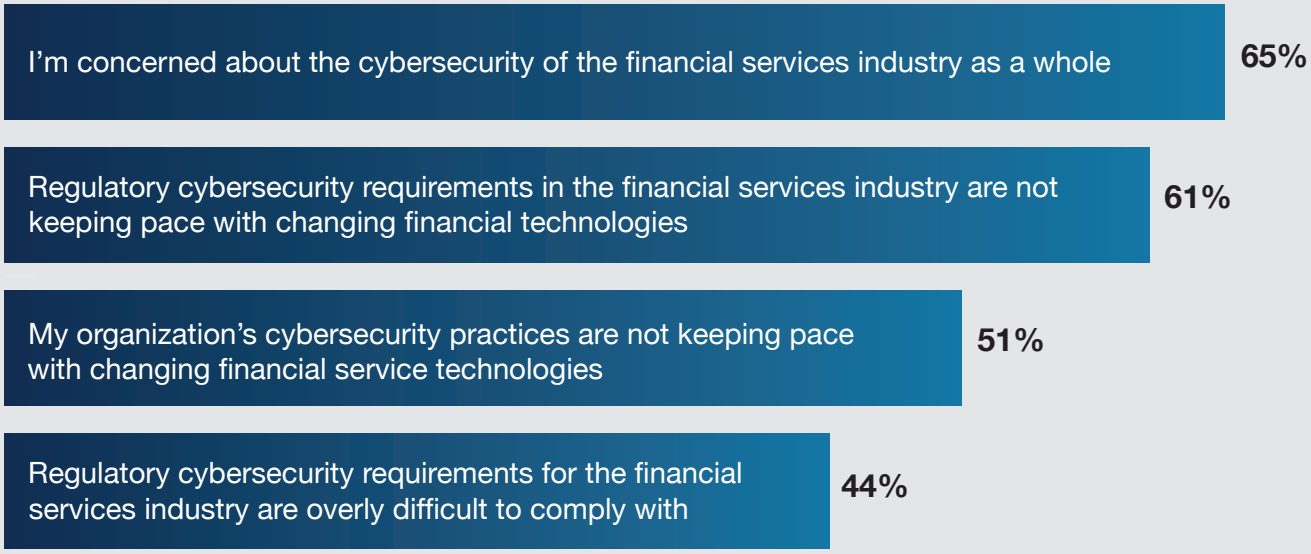
Shows responses of "Strongly agree" and "Agree"

Respondents are more concerned about the cybersecurity posture of the financial services industry than the difficulty of complying with regulations.

Respondents were asked to indicate their concern about cybersecurity risks on a scale of 1 = not concerned to 10 = very concerned. Figure 6 presents the very concerned responses (responses of 7–10 on the 10-point scale). As shown, 65 percent of respondents are very concerned about the cybersecurity posture of the financial services industry. Despite new regulations, such as the New York Department of Financial Services (NYDFS) Cybersecurity Regulation, 61 percent said regulatory requirements in the financial services industry are not keeping pace with changing financial technologies such as blockchain and open banking APIs.

Figure 6. Concerns about financial services cybersecurity

Shows responses of 7–10 on a scale from 1 = not concerned to 10 = very concerned



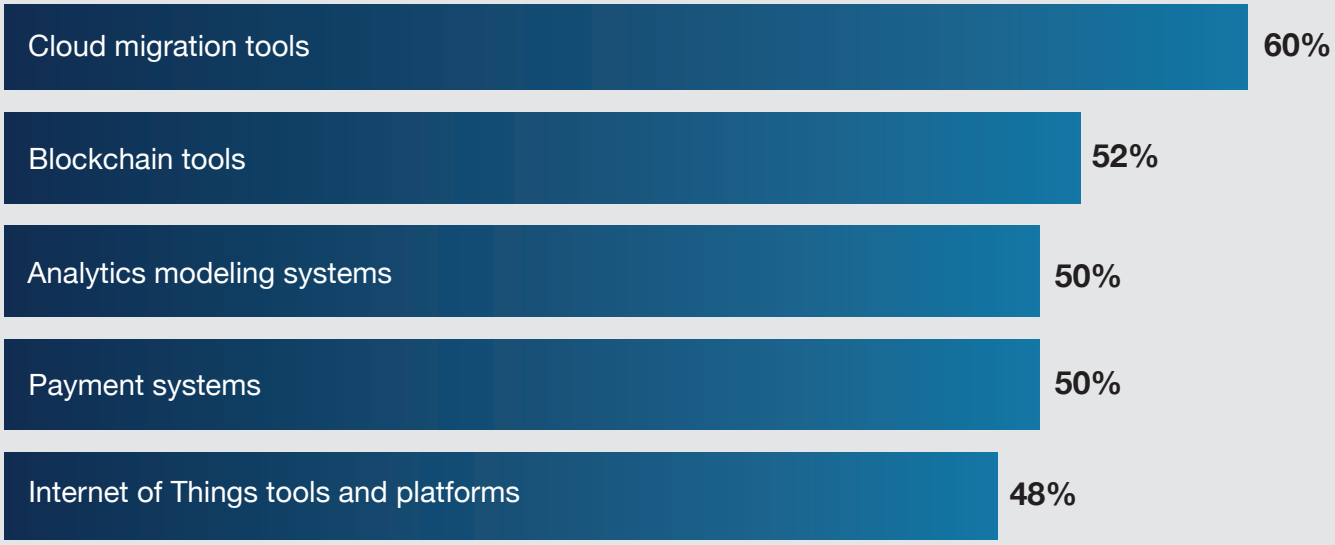
Risks to Financial Software and Applications

Respondents feel that cloud migration tools pose the greatest cybersecurity risk.

Figure 7 presents the software and technologies that respondents felt pose the greatest cybersecurity risk to financial services companies. As shown, 60 percent of respondents said cloud migration tools, followed by blockchain tools (52 percent), create the greatest risk.

Figure 7. Which software and technologies pose the greatest cybersecurity risk to financial services companies?

More than one response permitted



The threat of malicious actors is motivating companies to apply cybersecurity-related controls in financial software and technologies.

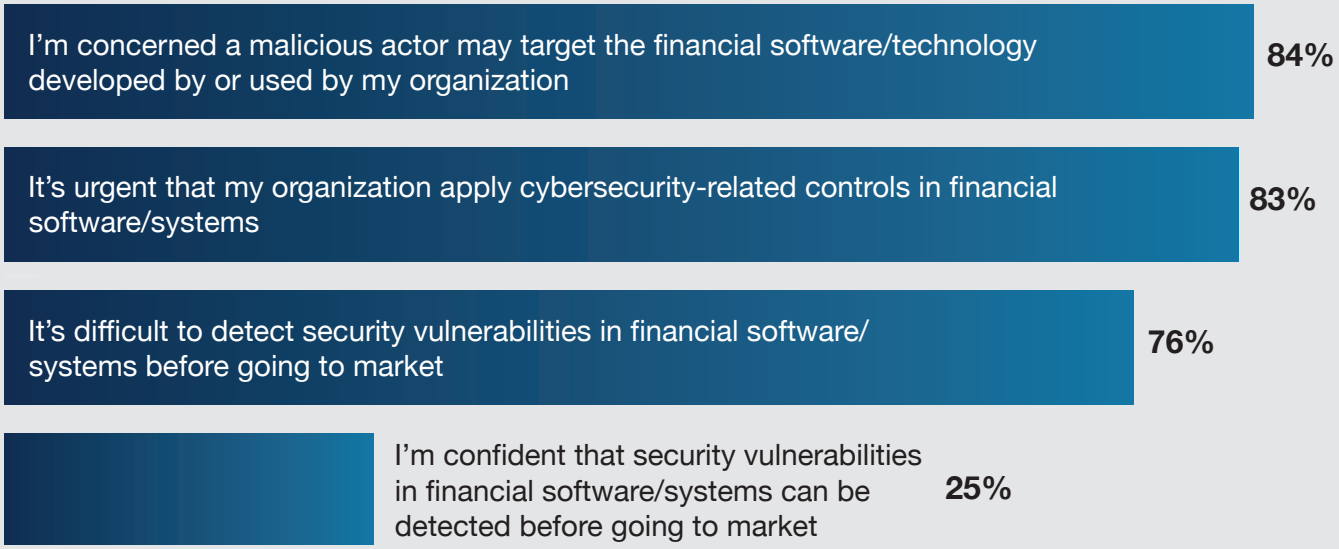
As shown in Figure 8, 84 percent of respondents said their organizations are very concerned (responses of 7–10 on a scale of 1 = not concerned to 10 = very concerned) that a malicious actor may target the financial software and technology developed by or used by their organizations.

Often the attack surface comprises internet-exposed financial applications, where attackers can take advantage of software vulnerability weaknesses such as cross-site scripting, cross-site request forgery, and SQL injection flaws to access sensitive data such as credit card information.

Eight-three percent of respondents said there is a very high urgency (responses of 7–10 on a scale of 1 = low urgency to 10 = high urgency) to apply cybersecurity-related controls in financial software and systems. Only 25 percent were confident that they can detect security vulnerabilities in financial software and systems before going to market (responses of 7–10 on a scale of 1 = not confident to 10 = very confident).

Figure 8. Concerns about vulnerabilities in financial software technologies

Responses of 7–10 on a scale from 1 = not concerned to 10 = very concerned

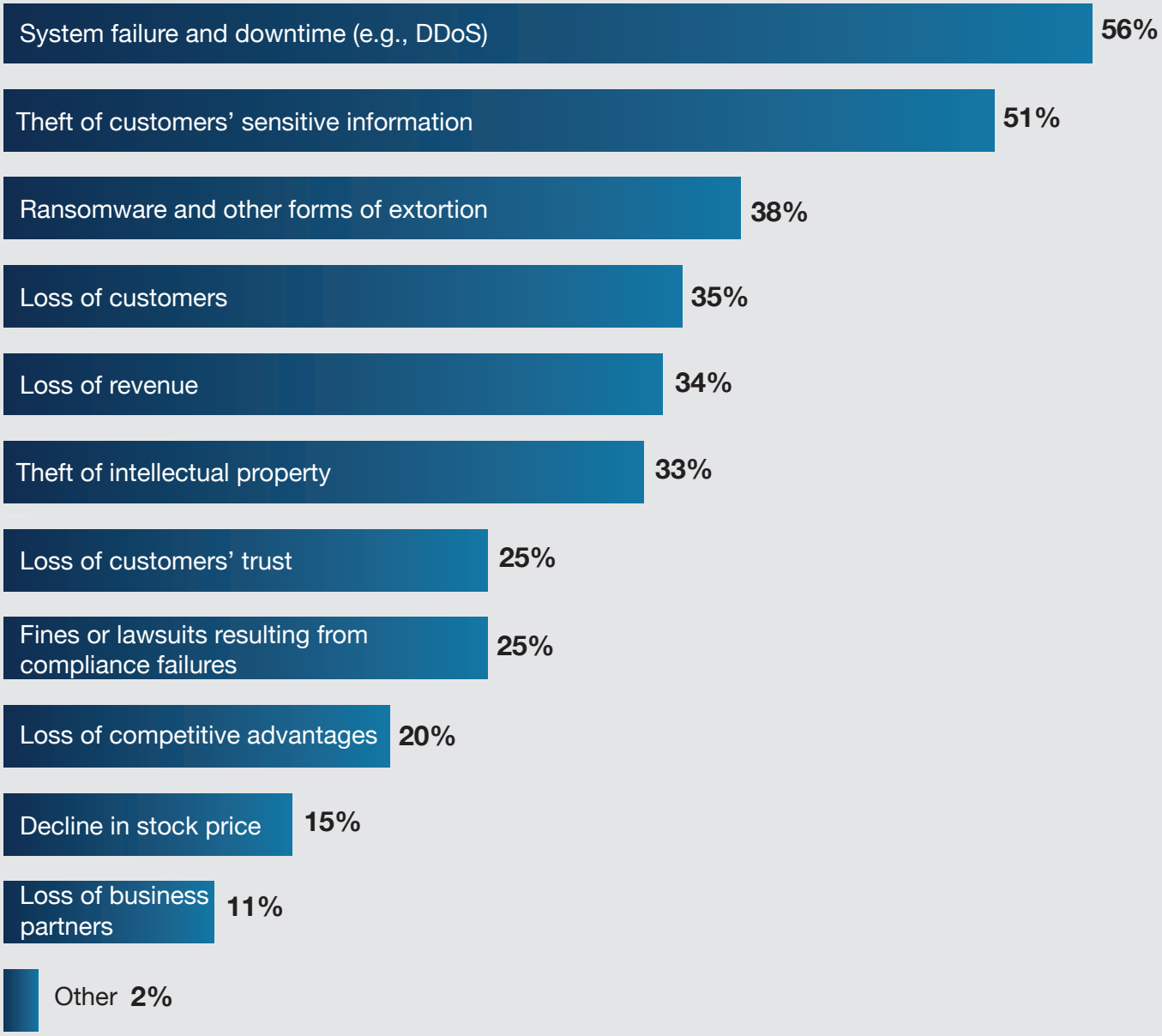


Unsecured software and technology can cause many negative business impacts, but system downtime happens most frequently.

Figure 9 presents 11 negative business impacts that can result from unsecured financial services software and technology. According to 56 percent of respondents, their organizations have experienced system failure, and more than half (51 percent) said their customers' sensitive information has been stolen.

Figure 9. Has your organization experienced any negative business impacts caused by unsecured financial services software and technology?

More than one response permitted

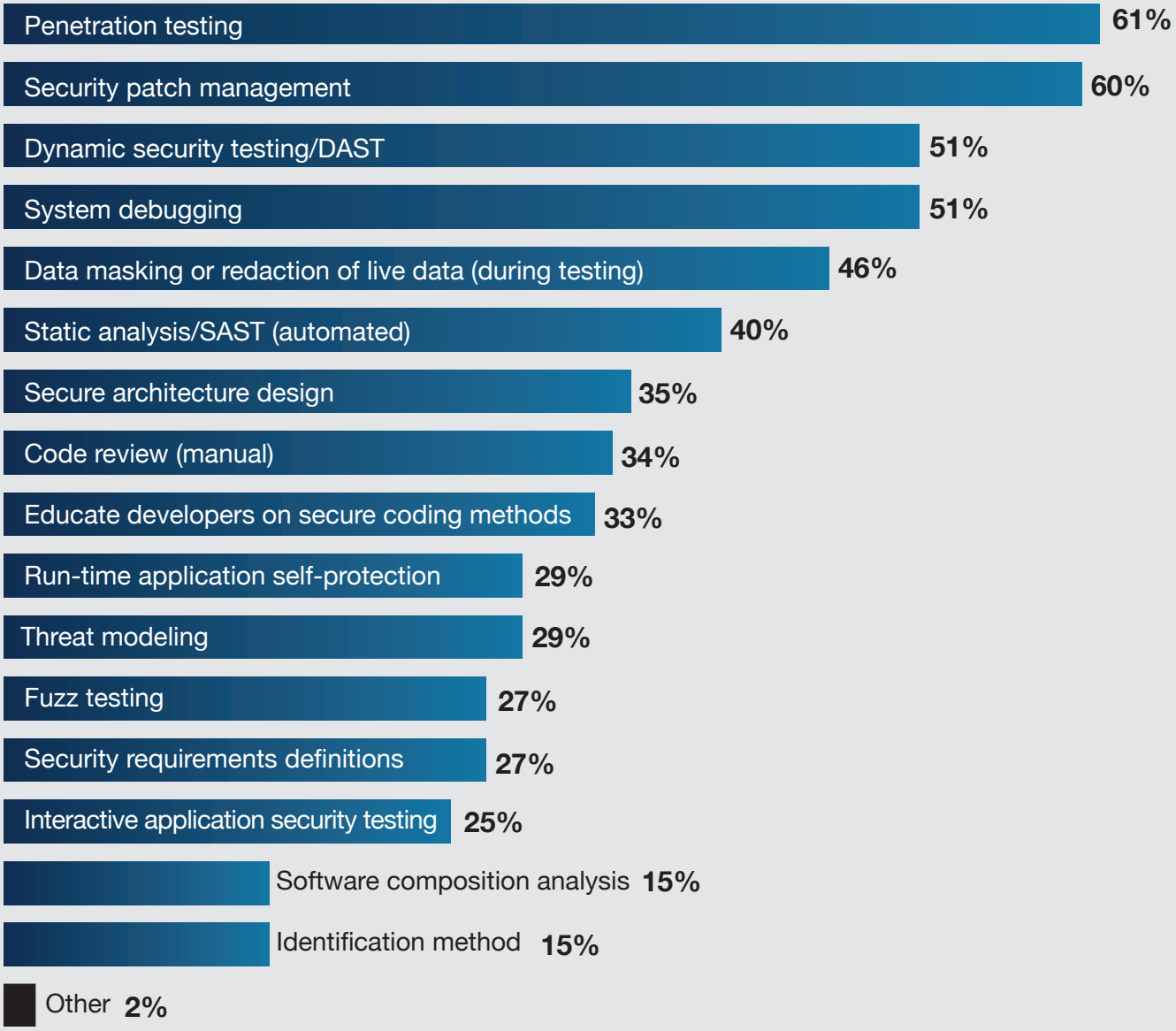


Organizations are securing their financial software and technology with penetration testing and security patch management.

Figure 10 presents 16 activities organizations do to secure their financial software and technology. Sixty-one percent of respondents said their organizations conduct pen testing, and 60 percent said their organizations patch security vulnerabilities.

Some organizations also use a layered approach of combining automated tools (e.g., SAST, SCA, IAST, DAST, and RASP) with manual planning and testing activities (e.g., secure architecture design, security requirements definitions, threat modeling, code review, and fuzz testing) to ensure security at every phase of the SDLC.

Figure 10. How does your organization secure its financial software and technology?
More than one response permitted



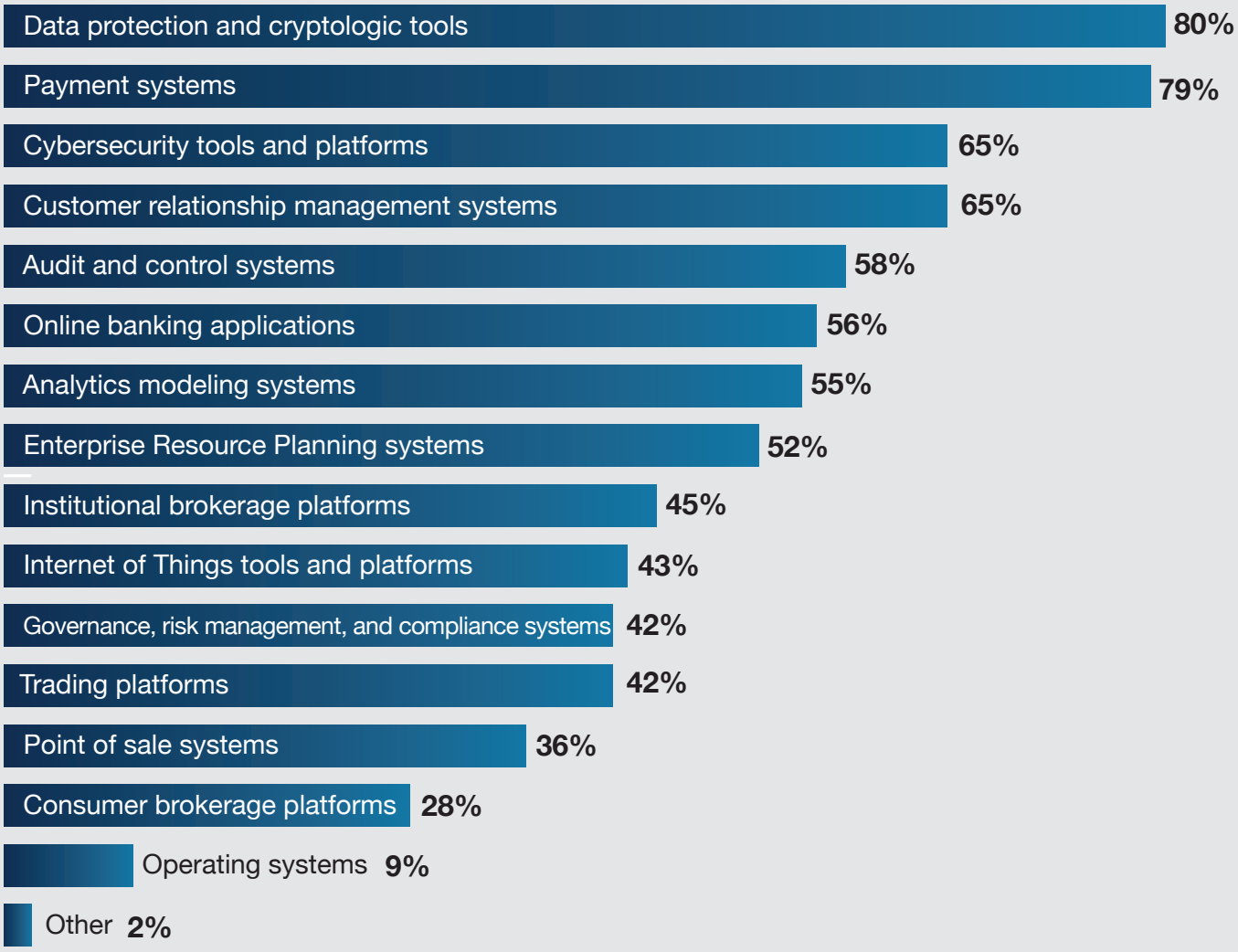
Security Practices in the Design and Development of Financial Service Technologies

Financial services companies design and develop a variety of software and technologies.

Figure 11 presents 15 different types of financial service software and technologies respondents noted their organizations design and develop. Eighty percent of respondents said their organizations design and develop data protection and cryptologic tools, followed by 79 percent who said they design and develop payment systems. These are followed by cybersecurity tools and platforms and customer relationship management systems (both 65 percent).

Figure 11. What types of financial service software and technologies does your organization design and develop?

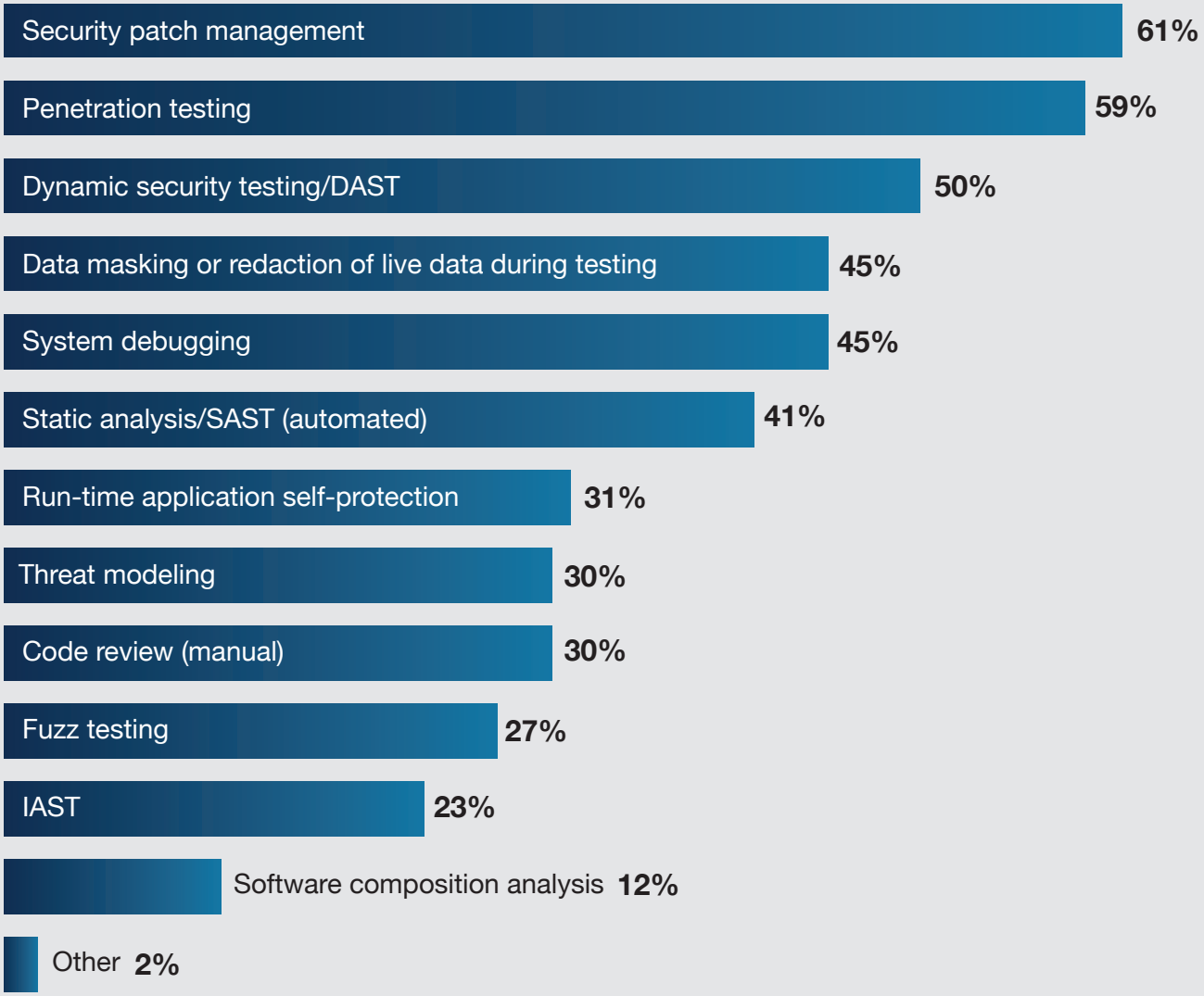
More than one response permitted



For quality assurance, organizations rely on security patch management and pen testing.

According to Figure 12, 61 percent of respondents said their organizations patch vulnerabilities, and 59 percent said they do pen testing, followed by 50 percent who perform dynamic security testing.

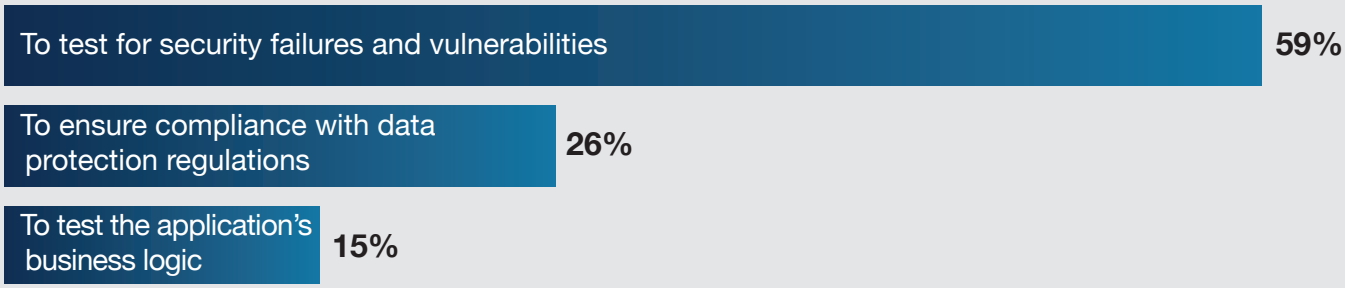
Figure 12. What security testing tools does your organization use for quality assurance?
More than one response permitted



For the respondents who said their organizations use pen testing for quality assurance purposes, the primary reasons (Figure 13) are to test for security failures and vulnerabilities (59 percent) and to ensure compliance with data protection regulations (26 percent). Only 15 percent said they perform pen testing to test the application's business logic.

Figure 13. Why do you use pen testing?

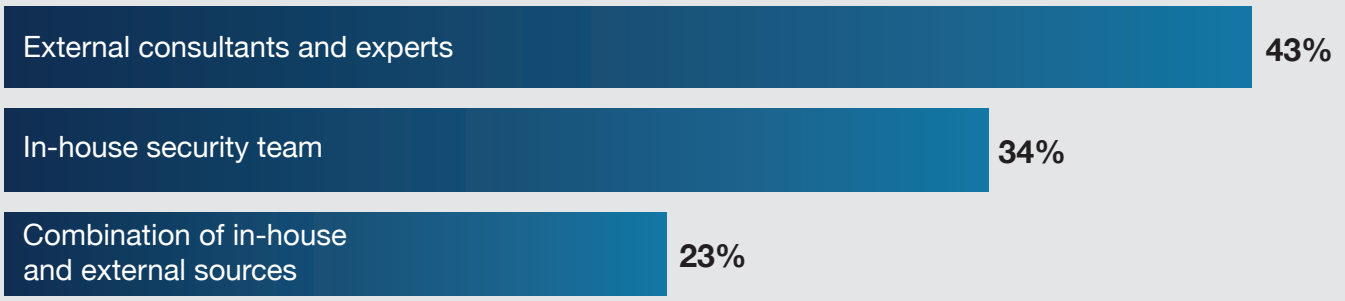
Of the 59% of respondents whose organizations perform pen testing



For the respondents who said they implement threat modeling, it is usually performed by external consultants and experts (43 percent) or an in-house security team (34 percent), as seen in Figure 14.

Figure 14. How do you implement threat modeling?

Of the 30% of respondents whose organizations implement threat modeling

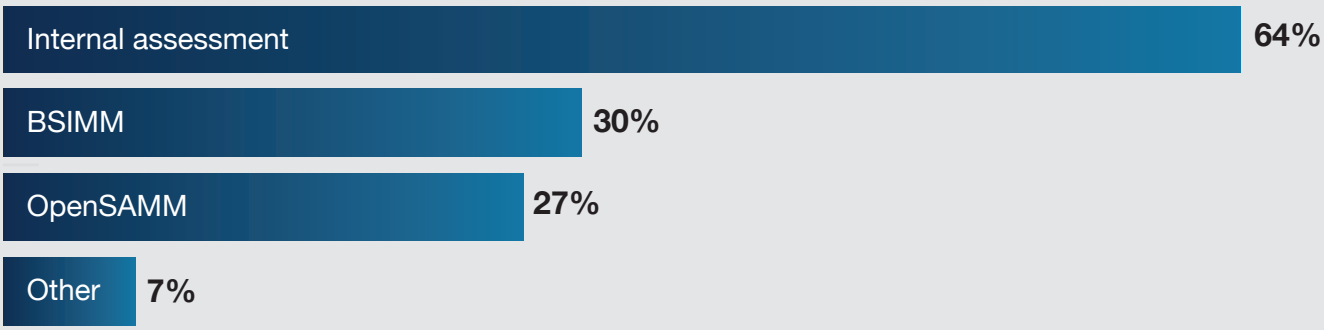


Most organizations conduct internal assessments to determine the effectiveness of their security programs.

As shown in Figure 15, 64 percent of respondents said their organizations use internal assessments to evaluate their security program. Only 30 percent said they use the BSIMM, followed by OpenSAMM (27 percent).

Figure 15. What tools do you use to assess your organization's security program?

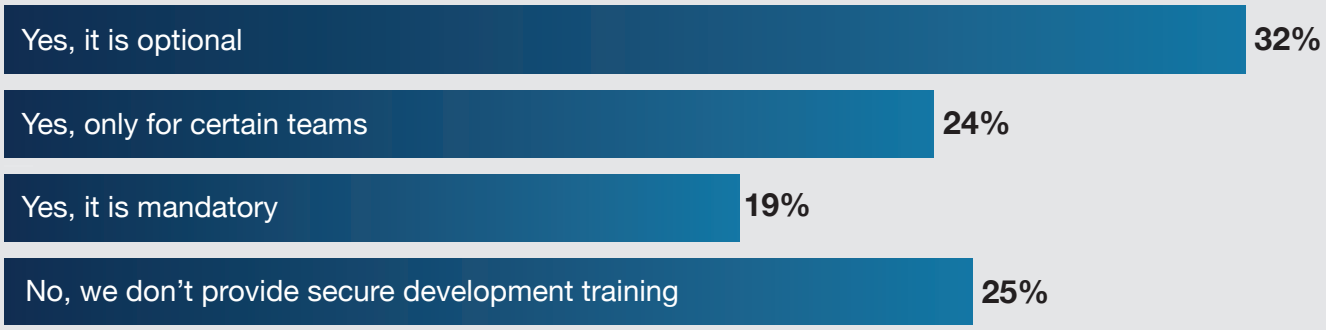
More than one response permitted



Most organizations provide secure development training for their software developers, but only 19 percent of respondents said it is mandatory.

As shown in Figure 16, 75 percent of organizations provide some level of training. However, 32 percent of respondents said it is optional, and 24 percent said it is only for certain teams. Only 19 percent said their organizations require such training.

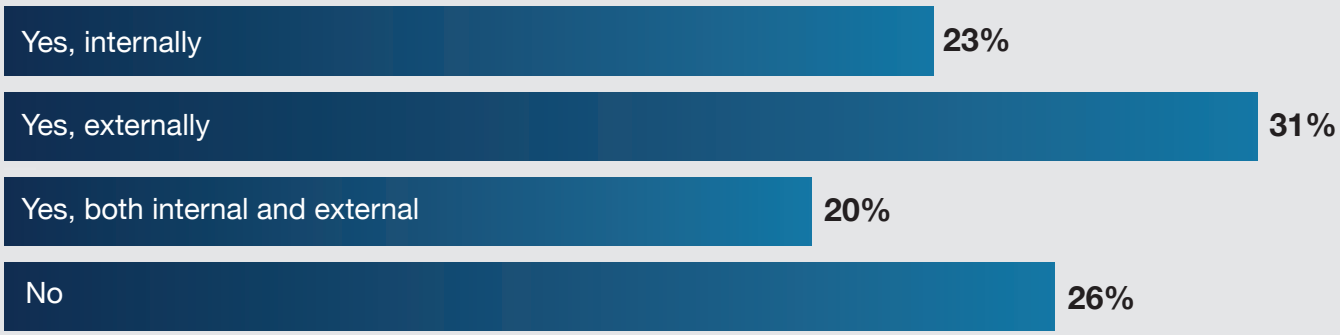
Figure 16. Does your organization provide secure development training for its software developers?



Most organizations follow a published secure software development life cycle (SSDLC) process.

As shown in Figure 17, 74 percent of respondents said their organizations follow an SSDLC process internally (23 percent), externally (31 percent), or both (20 percent). However, on average, organizations are testing only 34 percent of all financial software/technology for cybersecurity vulnerabilities.

Figure 17. Does your organization follow a published secure software development life cycle process?

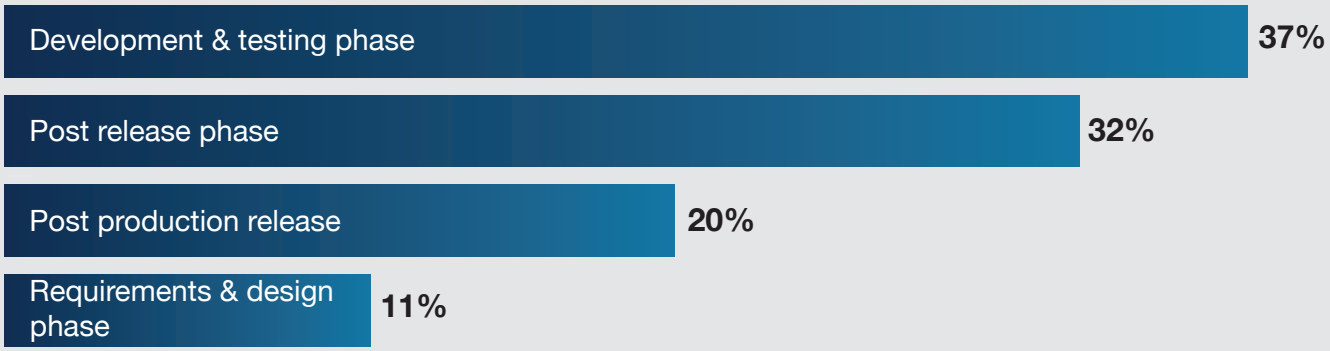


Organizations most often perform cybersecurity vulnerability assessments only after releasing the software.

As shown in Figure 18, 52 percent of respondents said cybersecurity vulnerability assessments occur in the post release phase (32 percent) or in the post production release phase (20 percent). Less than half (48 percent) said they occur when their organizations are designing the software (11 percent) or developing and testing the software (37 percent).

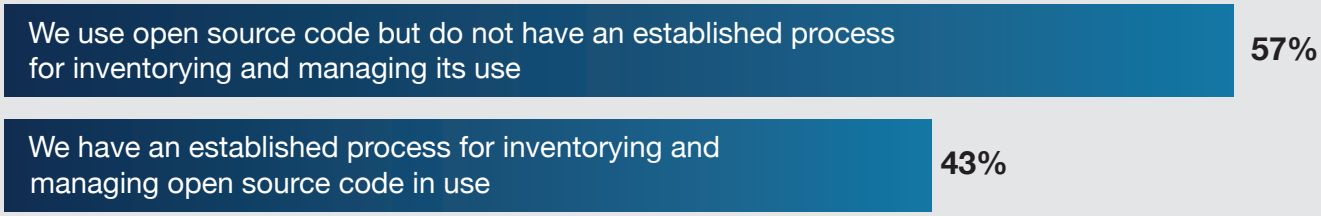
Figure 18. Where in the development life cycle does your organization assess cybersecurity vulnerabilities?

More than one response permitted



Most organizations do not have an established process for inventorying and managing their use of open source code. Only 43 percent of respondents said they have an established process for inventorying and managing open source code in use.

Figure 19. What defines your organization's use of open source code in the financial software and technology developed by your organization?



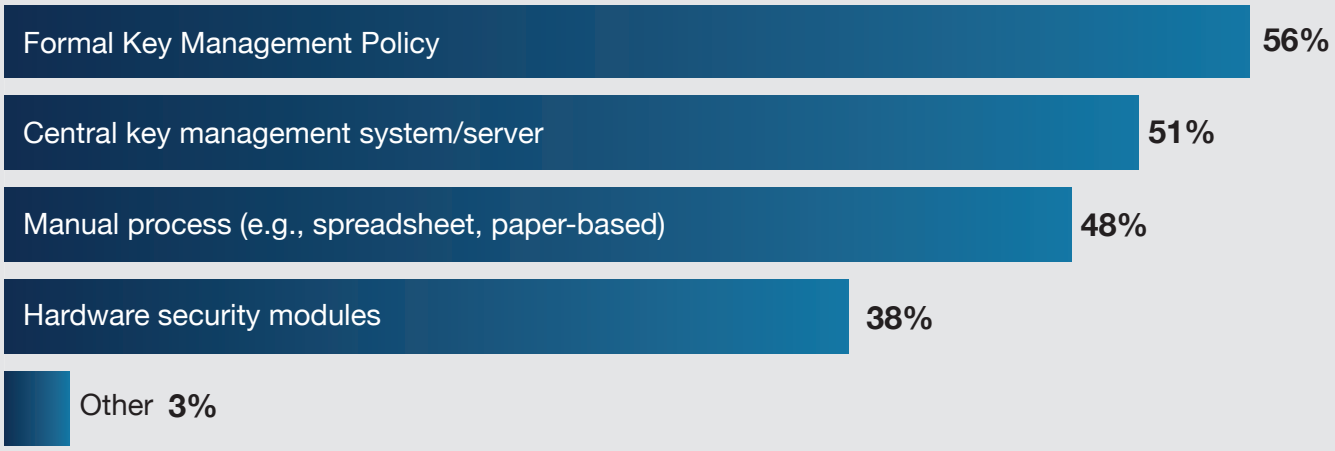
Organizations using key management systems mostly have a formal key management policy in place.

Almost half of organizations (48 percent of respondents) said they use key management systems for software, technology, and components used in the development or manufacturing process. The main systems they use are formal key management policies (56 percent) and central key management systems or servers (51 percent), as shown in Figure 20.

Figure 20. What key management systems does your organization use?

Of the 48% of respondents whose organizations use key management systems

More than one response permitted



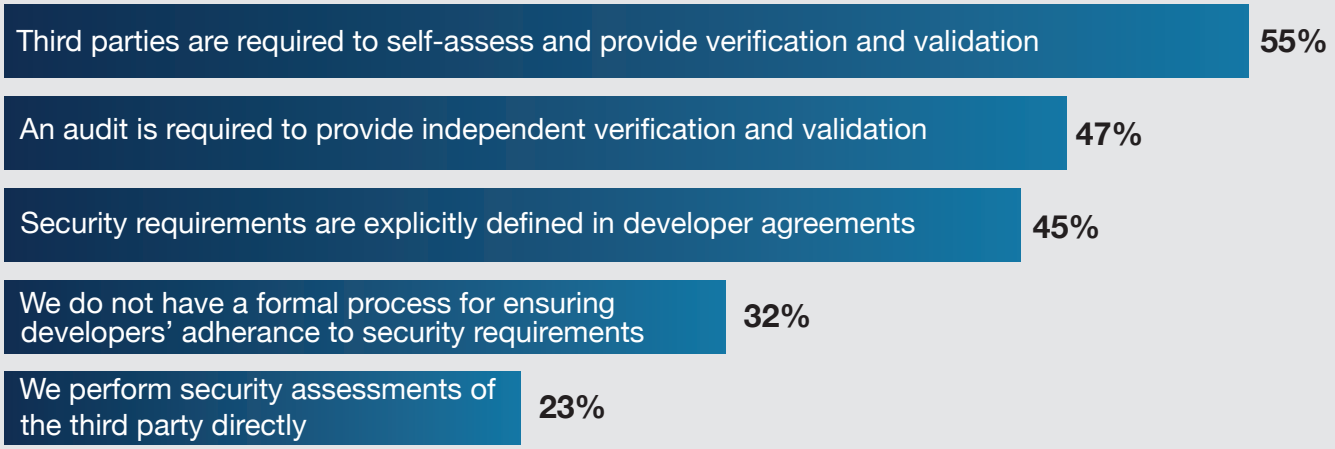
Organizations are concerned about third-party risks, but the majority don't require adherence to their cybersecurity requirements.

Only 43 percent of respondents said their organizations ask third parties involved in the financial software technology development process to verify their security practices. As shown in Figure 21, 55 percent require the third party to self-assess and provide verification and validation. Only 23 percent of organizations perform security assessments of the third party directly.

Figure 21. How does your organization ensure that third-party developers follow security requirements?

Of the 43% of respondents whose organizations impose cybersecurity requirements

More than one response permitted



Conclusion and Recommendations

Risk and Mitigation Strategies

Given that many FSI organizations rely on software supplied by third parties, it should be of concern that less than half of the organizations surveyed require third-party suppliers to adhere to software security practices.

Most survey respondents noted that even when such requirements are in place, their organizations have third-party suppliers provide their own verification and validation rather than conducting such reviews themselves. Requiring the vendor to incorporate an outside, independent maturity model, such as the Building Security In Maturity Model (BSIMM), would provide a mechanism to assess the security maturity of suppliers of third-party software.

Bugs, flaws, and weaknesses in software code are common. FSI organizations can add a layer of software security and reduce their risk by using (or requiring third parties to use) automated SAST (static application security testing) tools to detect and report weaknesses that can lead to security vulnerabilities.

Many of the FSI organizations surveyed do not have an established process for inventorying and managing open source code. As the 2019 Synopsys Open Source Security and Risk Analysis (OSSRA) report notes, of the 1,200+ codebases reviewed by the Synopsys Black Duck Audit Services team in 2018, 60 percent contained at least one open source vulnerability. Over 40 percent contained high-risk vulnerabilities, and 68 percent contained components with license conflicts.

Organizations using open source often overlook associated security and license risks. FSI organizations might not review incoming third-party code (or code developed internally) for potential security and legal issues. A comprehensive software composition analysis (SCA) solution for managing security, quality, and license compliance risk enables organizations to manage open source use across the software supply chain and throughout the application life cycle.

According to survey respondents, system failure and downtime is the most frequent business impact to FSI organizations from cyberthreats. Of more concern is that over half of respondents said that sensitive customer information has been stolen from their organizations at some point.

Based on their experience, respondents consider penetration testing and DAST (dynamic application security testing) to be the most effective activities in reducing cybersecurity risk. Also noted as effective are security patch management, system debugging, and threat modeling.

It's clear, however, that no single method, tool, or service will ensure complete software security coverage. Some organizations may use a layered approach of automated tools, including SAST, SCA, IAST (interactive application security testing), DAST, and RASP (runtime application security testing). Other strategies include manual planning and testing activities such as secure architecture design, security requirements definitions, threat modeling, code review, and fuzz testing to ensure security at every phase of the SDLC.

The consensus among respondents to the survey is that cloud migration tools, followed by blockchain tools, are the technologies that pose the current greatest cybersecurity risk to FSI organizations.

While blockchain adoption started slow, the pace is accelerating, similar to the adoption of cloud technologies a decade ago. As with the cloud, there are still security unknowns with blockchain, but its use by FSI is likely to mirror the SWIFT (Society for Worldwide Interbank Financial Telecommunications) system, a messaging network that financial institutions use to securely transmit information and instructions through a standardized system of codes.

But blockchain platforms are still vulnerable to intrusions from the periphery network infrastructure, unauthorized users, and insider threats, which could compromise blockchain credentials and expose sensitive data. As blockchain-based networks grow, with organizations leaving and new ones joining, there are likely to be ambiguities over data sharing, ownership, and data governance with regulatory implications.

Leveraging Managed Services to Supplement In-House Resources

The majority of survey respondents want more resources and in-house expertise to mitigate risks. Given that many groups—IT security or otherwise—feel that their budget will always be inadequate, one strategy to mitigate resource issues is to outsource security testing. Using organizations that provide services such as pen testing and DAST on demand is often a more cost-effective solution than using a dedicated, in-house team.

While the survey results indicate that most FSI organizations provide secure development training for software developers, only 19 percent of respondents said that such training is mandatory, an extremely low figure. Mandating cybersecurity skills in product development can help mitigate the issue. Security champions on product development teams can evangelize security best practices and support other team members in addressing and remediating code vulnerabilities.

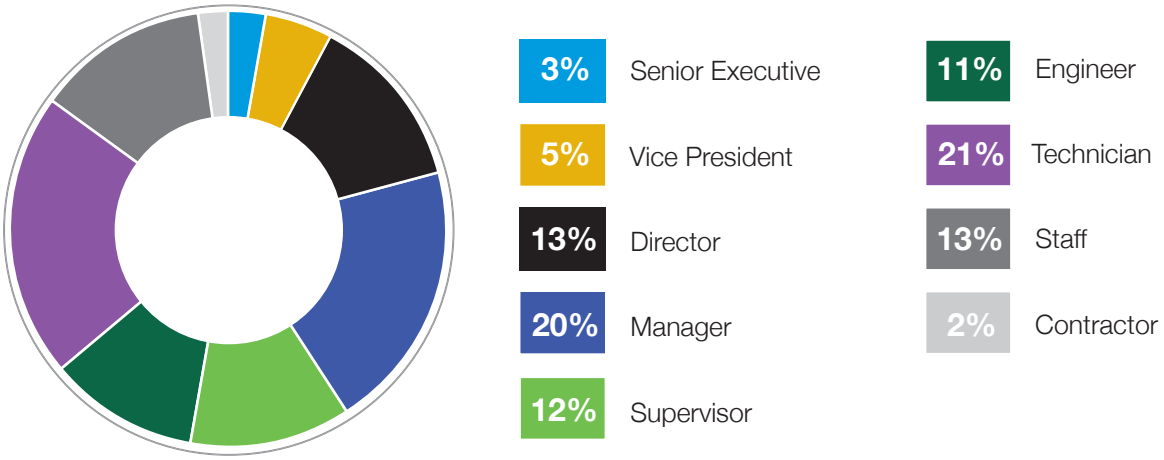
Other strategies include (1) providing development teams with SAST tools that integrate contextual eLearning and offer detailed advice on how to fix vulnerabilities and (2) offering instructor-led security training code development sessions on a regular basis.

Methods

The sampling frame is composed of 11,450 IT and IT security practitioners in all sectors of the financial services industry. As shown in Table 1, 463 respondents completed the survey. Screening removed 49 surveys. The final sample was 414 surveys, resulting in a 3.6 percent response rate.

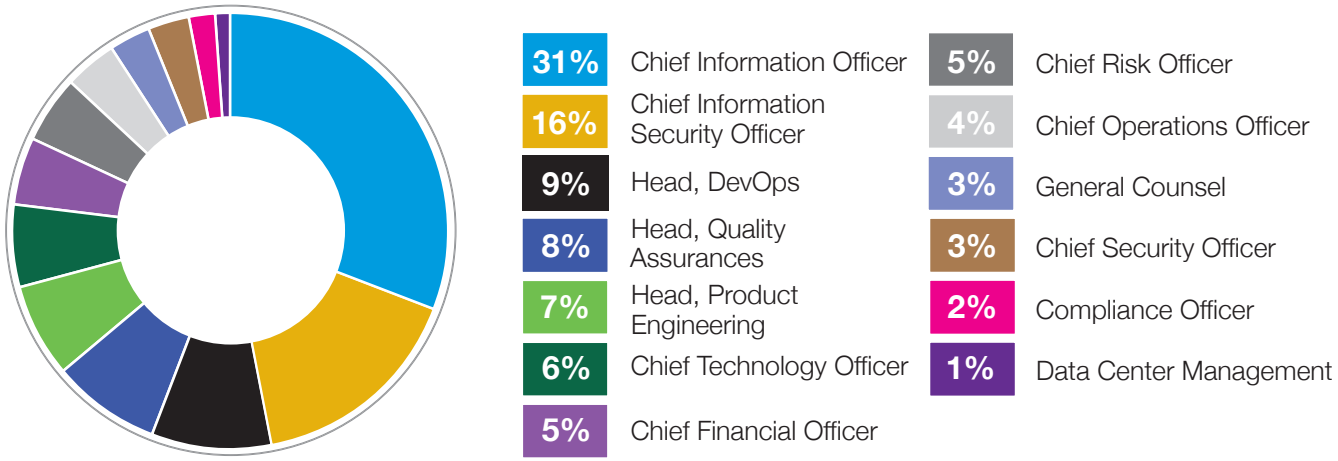
Table 1. Sample response	Freq.	Pct%
• Total sampling frame	11,450	100.0%
• Total returns	463	4.0%
• Rejected surveys	49	0.4%
• Final sample	414	3.6%

Pie Chart 1 reports the current position or organizational level of the respondents. More than half of respondents (53 percent) reported their current position as supervisory or above. Thirty-four percent reported their current position as technician or staff.



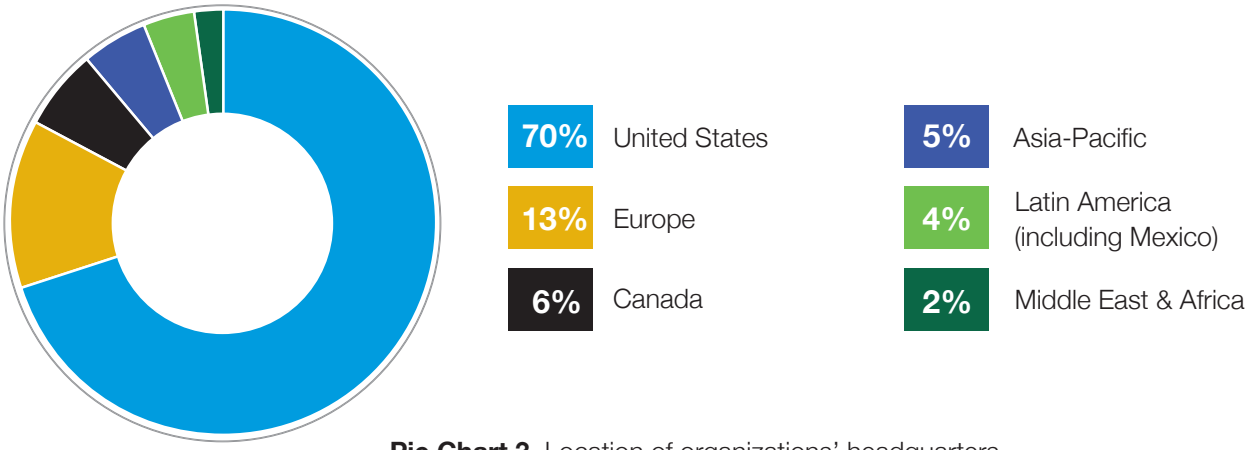
Pie Chart 1. Respondents' current position or organizational level

As shown in Pie Chart 2, 31 percent of respondents indicated they report to the chief information officer, 16 percent to the chief information security officer, 9 percent to the head of DevOps, and 8 percent to the head of quality assurances.



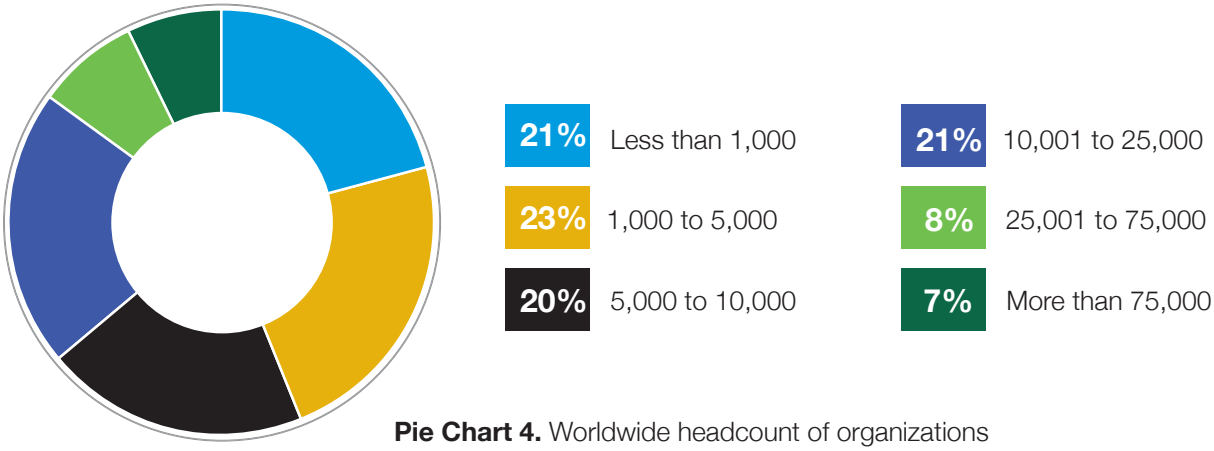
Pie Chart 2. Respondents' direct manager

Seventy percent of respondents are from organizations with headquarters located in the United States, as shown in Pie Chart 3. Thirteen percent are from organizations with headquarters in Europe, followed by Canada (6 percent), Asia-Pacific (5 percent), Latin America (4 percent), and the Middle East and Africa (2 percent).



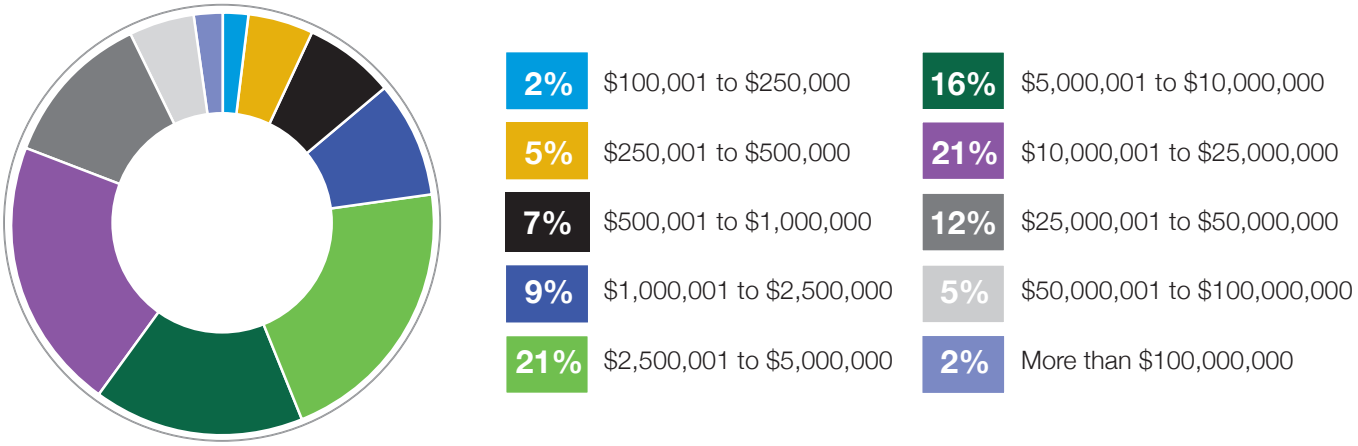
Pie Chart 3. Location of organizations' headquarters

According to Pie Chart 4, more than half of the respondents (56 percent) are from organizations with a global headcount of over 5,000 employees.



Pie Chart 4. Worldwide headcount of organizations

As shown in Pie Chart 5, more than half of respondents (58 percent) spend between $2.5 million and $25 million on cybersecurity, which includes total investment in terms of technologies, personnel, managed or outsourced services, and other related cash outlays.



Pie Chart 5. Distribution of respondents according to cybersecurity spending.
Extrapolated average value = $16,544,750.

Caveats to this study

There are inherent limitations to survey research that need to be carefully considered before drawing inferences from findings. The following items are specific limitations that are germane to most Web-based surveys.

- Non-response bias: The current findings are based on a sample of survey returns. We sent surveys to a representative sample of IT and IT security practitioners in all sectors of the financial services industry, resulting in a large number of usable returned responses. Despite non-response tests, it is always possible that individuals who did not participate are substantially different in terms of underlying beliefs from those who completed the instrument.

- Sampling-frame bias: The accuracy is based on contact information and the degree to which the list is representative of individuals who are IT and IT security practitioners from various organizations. Because we used a Web-based collection method, it is possible that non-Web responses by mailed survey or telephone call would result in a different pattern of findings.

- Self-reported results: The quality of survey research is based on the integrity of confidential responses received from subjects. While certain checks and balances can be incorporated into the survey process, the possibility remains that a subject did not provide accurate responses.

Appendix: Detailed Survey Results

The following tables provide the frequency or percentage frequency of responses to all survey questions contained in this study. All survey responses were captured from January 12 to February 9, 2019.

Sample response	Freq.	Pct%
• Total sample frame	11,450	100.00%
• Total returns	463	4.04%
• Rejected surveys	49	0.43%
• Final sample	414	3.62%

Part 1. Screening

S1a. Do you have any role or involvement in assessing the security of financial applications within your organization?	• Yes, significant involvement	44%
	• Yes, some involvement	40%
	• Yes, minimal involvement	16%
	• No involvement (Stop)	0%
	Total	100%
S1b. If you are involved, how many years have you spent assessing the security of applications?	• Less than 1 year	2%
	• 2 to 4 years	15%
	• 5 to 7 years	28%
	• 8 to 10 years	30%
	• More than 10 years	25%
	• Cannot determine (Stop)	0%
	Total	100%
	Extrapolated value	7.85
S2. What best describes your organization's role in the development of financial applications?	• Develop & manufacture financial applications	27%
	• Install and implement financial applications	45%
	• Provide services to the financial services industry	23%
	• Other (please specify)	5%
	• None of the above (Stop)	0%
	Total	100%
S3. What best describes your organization's role in the development of financial applications?	• Banking	40%
	• Insurance	19%
	• Brokerage	12%
	• Investment management	7%
	• Payment processor	5%
	• Mortgage lending/processing	15%
	• Other (please specify)	2%
	• None of the above (Stop)	0%
	Total	100%

Part 2. General questions

Q1. Using the following 10-point scale, please rate your organization's effectiveness in **preventing** cyberattacks. 1 = ineffective and 10 = very effective.	• 1 to 2	11%
	• 3 to 4	24%
	• 5 to 6	34%
	• 7 to 8	16%
	• 9 to 10	15%
	Total	100%
	Extrapolated value	5.50
Q2. Using the following 10-point scale, please rate your organization's effectiveness in **detecting** cyberattacks. 1 = ineffective and 10 = very effective.	• 1 to 2	5%
	• 3 to 4	10%
	• 5 to 6	29%
	• 7 to 8	35%
	• 9 to 10	21%
	Total	100%
	Extrapolated value	6.64
Q3. Using the following 10-point scale, please rate your organization's effectiveness in **containing** cyberattacks. 1 = ineffective and 10 = very effective.	• 1 to 2	8%
	• 3 to 4	11%
	• 5 to 6	28%
	• 7 to 8	28%
	• 9 to 10	25%
	Total	100%
	Extrapolated value	6.52
Q4. What types of financial service software/technologies does your organization design and develop? Please select all that apply.	• Enterprise Resource Planning (ERP) systems	52%
	• Online banking applications	56%
	• Trading platforms	42%
	• Consumer brokerage platforms	28%
	• Institutional brokerage platforms	45%
	• Customer relationship management (CRM) systems	65%
	• Payment systems	79%
	• Internet of Things (IoT) tools and platforms	43%
	• Point of sale systems	36%
	• Governance, risk management and compliance (GRC) systems	42%
	• Analytics modeling systems	55%
	• Audit and control systems	58%
	• Cybersecurity tools and platforms	65%
	• Data protection and cryptologic tools	80%
	• Operating systems	9%
	• Other (please specify)	2%
	Total	757%

Q5a. Does your organization have a cybersecurity program or team?	• Yes	67%
	• No	33%
	Total	100%

Q5b. If yes, what is your organization's approach to cybersecurity?	• Cybersecurity is part of the traditional IT cybersecurity team (typically under a global CISO)	60%
	• Cybersecurity is part of the functional safety team	34%
	• The cybersecurity team is centralized (i.e., center of excellence) that guides and supports multiple product development teams	47%
	• The cybersecurity team is decentralized, with cybersecurity experts attached to specific product development teams	51%
	• Cybersecurity is the responsibility of product development	23%
	• Other (please specify)	3%
	Total	218%

Q6. My organization allocates enough resources to cybersecurity (i.e., budget and personnel).	• Strongly agree	15%
	• Agree	30%
	• Unsure	17%
	• Disagree	31%
	• Strongly disagree	7%
	Total	100%

Q7. My organization has the necessary cybersecurity skills in product development.	• Strongly agree	12%
	• Agree	26%
	• Unsure	18%
	• Disagree	32%
	• Strongly disagree	12%
	Total	100%

Part 3. Perceptions about software security risk

Q8. Which software/technologies pose the greatest cybersecurity risk to financial services companies? Please select the top five (5) choices.	• Enterprise Resource Planning (ERP) systems	10%
	• Customer relationship management (CRM) systems	38%
	• Payment systems	50%
	• Point of sale systems	45%
	• Blockchain tools	52%
	• Internet of Things (IoT) tools and platforms	48%
	• Governance, risk management and compliance (GRC) systems	21%
	• Analytics modeling systems	50%
	• Audit and control systems	16%
	• Cybersecurity tools and platforms	28%
	• Data protection and cryptologic tools	35%
	• Cloud migration tools	60%
	• Operating systems	45%
	• Other (please specify)	2%
	Total	500%

Q9. Which of the following negative business impacts caused by unsecured financial services software/technology either developed by or used by your organization have you experienced? Please select all that apply.	• Theft of customers' sensitive information	51%
	• Theft of intellectual property	33%
	• System failure and downtime (e.g., DDoS)	56%
	• Ransomware and Other (please specify) forms of extortion	38%
	• Fines or lawsuits resulting from compliance failures	25%
	• Loss of revenue	34%
	• Loss of customers	35%
	• Loss of business partners	11%
	• Loss of customers' trust	25%
	• Decline in stock price	15%
	• Loss of competitive advantages	20%
	• Other (please specify)	2%
	Total	345%

Q10. Are you aware if any of your organization's customers had their identity stolen that was caused by unsecured financial services software/technology?	• Yes	23%
	• No	77%
	Total	100%

Please rate the following statements using the 10-point scale from 1 = not concerned to 10 = very concerned.

Q11. How concerned are you about the cybersecurity posture of financial software/systems developed by your organization?	• 1 or 2	5%
	• 3 or 4	8%
	• 5 or 6	25%
	• 7 or 8	27%
	• 9 or 10	35%
	Total	100%
	Extrapolated value	7.08

Q12. How concerned are you about the cybersecurity posture of financial software/systems supplied to your organization by a third party?	• 1 or 2	3%
	• 3 or 4	7%
	• 5 or 6	16%
	• 7 or 8	32%
	• 9 or 10	42%
	Total	100%
	Extrapolated value	7.56

Q13. How concerned are you about the cybersecurity of the financial services industry as a whole?	• 1 or 2	7%
	• 3 or 4	5%
	• 5 or 6	23%
	• 7 or 8	35%
	• 9 or 10	30%
	Total	100%
	Extrapolated value	7.02
Q14. How concerned are you that your organization's cybersecurity practices are not keeping pace with changing financial service technologies?	• 1 or 2	8%
	• 3 or 4	10%
	• 5 or 6	31%
	• 7 or 8	25%
	• 9 or 10	26%
	Total	100%
	Extrapolated value	6.52
Q15. How concerned are you that regulatory cybersecurity requirements in the financial services industry are not keeping pace with changing financial technologies?	• 1 or 2	2%
	• 3 or 4	9%
	• 5 or 6	32%
	• 7 or 8	29%
	• 9 or 10	32%
	Total	104%
	Extrapolated value	7.32
Q16. How concerned are you that regulatory cybersecurity requirements for the financial services industry are overly difficult to comply with?	• 1 or 2	10%
	• 3 or 4	14%
	• 5 or 6	32%
	• 7 or 8	29%
	• 9 or 10	15%
	Total	100%
	Extrapolated value	6.00
Q17. How concerned are you that a malicious actor may target the financial software/technology developed by or used by your organization?	• 1 or 2	2%
	• 3 or 4	6%
	• 5 or 6	8%
	• 7 or 8	30%
	• 9 or 10	54%
	Total	100%
	Extrapolated value	8.06

Please rate the following statements using the 10-point scale from 1 = not confident to 10 = very confident.

Q18. How confident are you that security vulnerabilities in financial software/systems can be detected before going to market?	• 1 or 2	13%
	• 3 or 4	27%
	• 5 or 6	35%
	• 7 or 8	13%
	• 9 or 10	12%
	Total	100%
	Extrapolated value	5.18

Please rate the following statements using the 10-point scale from 1 = not difficult to 10 = difficult.

Q19. How difficult is it for your organization to detect security vulnerabilities in automotive software/technology/components before going to market?	• 1 or 2	1%
	• 3 or 4	8%
	• 5 or 6	15%
	• 7 or 8	33%
	• 9 or 10	43%
	Total	100%
	Extrapolated value	7.68

Please rate the following statements using the 10-point scale from 1 = not urgent to 10 = very urgent.

Q20. How urgent is it for your organization to apply cybersecurity-related controls in financial software/systems?	• 1 or 2	3%
	• 3 or 4	5%
	• 5 or 6	9%
	• 7 or 8	37%
	• 9 or 10	46%
	Total	100%
	Extrapolated value	7.86

Part 4. Security practices in the SDLC

Q21a. Does your organization provide secure development training for its software developers?	• Yes, it is optional	32%
	• Yes, it is mandatory	19%
	• Yes, only for certain teams	24%
	• No, we don't provide secure development training	25%
	Total	100%

Q21b. If yes, how effective is your organization's secure development training?	• Very effective	17%
	• Effective	21%
	• Somewhat effective	28%
	• Not effective	34%
	Total	100%

Q22. Does your organization follow an internally or externally published Secure Software Development Life Cycle (SSDLC) process for financial software/ technology creation?	• Yes, internally	23%
	• Yes, externally	31%
	• Yes, both internal and external	20%
	• No	26%
	Total	100%
Q23. On average, what percentage of financial software/ technology developed by or in use by your organization is tested for cybersecurity vulnerabilities?	• None	12%
	• Less than 25%	25%
	• 26% to 50%	43%
	• 51% to 75%	12%
	• 76% to 100%	8%
	Total	100%
	Extrapolated value	34%
Q24. Where in the development life cycle does your organization assess cybersecurity vulnerabilities? Please check all that apply.	• Requirements & design phase	11%
	• Development & testing phase	37%
	• Post release phase	32%
	• Post production release	20%
	Total	100%
Q25. What activities does your organization employ to secure financial software/technology? Please select all that apply.	• Educate developers on secure coding methods	33%
	• Secure architecture design	35%
	• Threat modeling	29%
	• Identification method	15%
	• Security requirements definitions	27%
	• Code review (manual)	34%
	• Static analysis/SAST (automated)	40%
	• System debugging	51%
	• Fuzz testing	27%
	• Software composition analysis	15%
	• Dynamic security testing/DAST	51%
	• Interactive application security testing (IAST)	25%
	• Penetration testing	61%
	• Data masking or redaction of live data (during testing)	46%
	• Security patch management	60%
	• Run-time application self-protection (RASP)	29%
	• Other (please specify)	2%
	Total	580%

Q26. What activities are the most effective in mitigating cybersecurity risks in the financial services industry? Please select all that apply.	• Educate developers on secure coding methods	44%
	• Secure architecture design	25%
	• Threat modeling	51%
	• Identification method	23%
	• Security requirements definitions	34%
	• Code review (manual)	40%
	• Static analysis/SAST (automated)	45%
	• System debugging	52%
	• Fuzz testing	49%
	• Software composition analysis	33%
	• Dynamic security testing/DAST	63%
	• Interactive application security testing (IAST)	28%
	• Penetration testing	65%
	• Data masking or redaction of live data (during testing)	43%
	• Security patch management	55%
	• Run-time application self-protection (RASP)	23%
	• Other (please specify)	0%
	Total	673%
Q27. What defines your organization's use of open source code in the financial software/ technology developed by your organization?	• We have an established process for inventorying and managing open source code in use.	43%
	• We use open source code but do not have an established process for inventorying and managing its use.	57%
	Total	100%
Q28. Does your organization have a patch management process in place (i.e. a policy with defined roles and responsibilities and established guidelines for the patching process)?	• Yes	51%
	• No	49%
	Total	100%
Q29a. Does your organization use key management systems for software/technology/components used in the development or manufacturing process?	• Yes	48%
	• No	52%
	Total	100%

Q29b. If yes, what key management systems does your organization presently use? Please check all that apply.	• Formal Key Management Policy (KMP)	56%
	• Manual process (e.g., spreadsheet, paper-based)	48%
	• Central key management system/server	51%
	• Hardware security modules	38%
	• Other (please specify)	3%
	Total	196%

Q30a. Does your organization impose cybersecurity requirements for contractors, business partners and other (please specify) third parties involved in the financial software/ technology development process?	• Yes	43%
	• No	57%
	Total	100%

Q30b. If yes, how does your organization ensure that third-party developers adhere to security requirements? Please check all that apply.	• Third parties are required to self-assess and provide verification and validation	55%
	• An audit is required to provide independent verification and validation	47%
	• We perform security assessments of the third party directly	23%
	• Security requirements are explicitly defined in developer agreements	45%
	• We do not have a formal process for ensuring developers' adherence to security requirements	32%
	Total	202%

Part 5. Technology trends

Q31. Has your organization adopted rapid development methodologies such as DevOps and CI/CD?	• Yes	35%
	• No, but we plan to in the next year	23%
	• No, but we plan to in the next 24 months	12%
	• We have no plans to adopt such methodologies	30%
	Total	100%

Q32. If yes, have you implemented security into your DevOps and/or CI/CD workflow?	• Yes	50%
	• No, but we plan to in the next year	16%
	• No, but we plan to in the next 24 months	11%
	• We have no plans to implement security	23%
	Total	100%

Q33. How familiar are you with the NYDFS regulation for financial service companies?	• Very familiar	27%
	• Familiar	44%
	• Not familiar (skip to Q36a)	23%
	• No knowledge (skip to Q36a)	6%
	Total	100%

Q34a. Has your organization achieved compliance with NYDFS?	• Yes, fully compliant	20%
	• Yes, partially compliant	32%
	• No, but we will achieve compliance this year	25%
	• No, we are not certain when we will achieve compliance	23%
	Total	100%
Q34b. If yes, how difficult was it for your organization to achieve compliance on a scale from 1 = not difficult to 10 = very difficult?	• 1 to 2	2%
	• 3 to 4	5%
	• 5 to 6	10%
	• 7 to 8	50%
	• 9 to 10	33%
	Total	100%
	Extrapolated value	7.64
Q35. In your opinion, how does compliance with NYDFS cybersecurity regulations affect the effectiveness of your organization's overall cybersecurity posture?	• Very significant improvement	21%
	• Significant improvement	30%
	• Nominal improvement	29%
	• No improvement	20%
	Total	100%
Q36a. Is your organization required to comply with the EU's General Data Protection Regulation (GDPR), which went into effect May 25, 2018?	• Yes	64%
	• No (skip to Q39a)	36%
	Total	100%
Q36b. If yes, has your organization achieved compliance with GDPR?	• Yes, fully compliant	27%
	• Yes, partially compliant	54%
	• We have not achieved compliance as yet (skip to Q39a)	19%
	Total	100%
Q37. How difficult was it for your organization to achieve compliance with GDPR from a scale of 1 = not difficult to 10 = very difficult?	• 1 to 2	0%
	• 3 to 4	3%
	• 5 to 6	8%
	• 7 to 8	52%
	• 9 to 10	37%
	Total	100%
	Extrapolated value	7.96

Q38. In your opinion, how will compliance with GDPR affect the effectiveness of your organization's cybersecurity posture?	• Very significant improvement	24%
	• Significant improvement	31%
	• Nominal improvement	30%
	• No improvement	15%
	Total	100%

Part 6. Other (please specify) industry practices

Q39a. What security testing tools does your organization use for quality assurance? Please select all that apply.	• Code review (manual)	30%
	• Static analysis/SAST (automated)	41%
	• System debugging	45%
	• Fuzz testing	27%
	• Software composition analysis	12%
	• Dynamic security testing/DAST	50%
	• IAST	23%
	• Penetration testing (skip to Q39b)	59%
	• Data masking or redaction of live data during testing	45%
	• Security patch management	61%
	• Run-time application self-protection (RASP)	31%
	• Threat modeling (skip to Q39c)	30%
	• Other (please specify)	2%
	Total	456%
Q39b. If you selected pen testing, why do you use it?	• To ensure compliance with data protection regulations	26%
	• To test for security failures and vulnerabilities	59%
	• To test the application's business logic	15%
	• Other (please specify)	0%
	Total	100%
Q39c. If you selected threat modeling, how is it implemented?	• In-house security team	34%
	• External consultants and experts	43%
	• Combination of in-house and external sources	23%
	Total	100%
Q39d. What percentage of applications utilize threat modeling?	• Less than 10%	54%
	• 10% to 25%	22%
	• 26% to 50%	10%
	• 51% to 75%	9%
	• 76% to 100%	5%
	Total	100%
	Extrapolated value	20%

Q40. What tools do you use to assess your organization's security program?	• BSIMM	30%
	• OpenSAM	27%
	• Internal assessment	64%
	• Other (please specify)	7%
	Total	128%

Part 7. Demographics

D1. What organizational level best describes your current position?	• Senior Executive	3%
	• Vice President	5%
	• Director	13%
	• Manager	20%
	• Supervisor	12%
	• Engineer	11%
	• Technician	21%
	• Staff	13%
	• Contractor	2%
	• Other (please specify)	0%
	Total	100%

D2. Check the **Primary Person** you or your leader reports to within the organization.	• Chief Financial Officer	5%
	• Chief Operations Officer	4%
	• General Counsel	3%
	• Head, DevOps	9%
	• Head, Product Engineering	7%
	• Head, Quality Assurances	8%
	• Chief Information Officer	31%
	• Chief Technology Officer	6%
	• Chief Information Security Officer	16%
	• Chief Security Officer	3%
	• Compliance Officer	2%
	• Data Center Management	1%
	• Chief Risk Officer	5%
	• Other (please specify)	0%
	Total	100%

D3. Where is your company headquartered?	• United States	70%
	• Canada	6%
	• Europe	13%
	• Middle East & Africa	2%
	• Asia-Pacific	5%
	• Latin America (including Mexico)	4%
	Total	100%

D4. What is the worldwide headcount of your company?	• Less than 1,000	21%
	• 1,000 to 5,000	23%
	• 5,000 to 10,000	20%
	• 10,001 to 25,000	21%
	• 25,001 to 75,000	8%
	• More than 75,000	7%
	Total	100%

D5. Approximately, how much does your organization spend on cybersecurity in the current year? Please choose the range that best approximates the total investment in terms of technologies, personnel, managed or outsourced services and Other (please specify) cash outlays.	• None	0%
	• $1 to $100,000	0%
	• $100,001 to $250,000	2%
	• $250,001 to $500,000	5%
	• $500,001 to $1,000,000	7%
	• $1,000,001 to $2,500,000	9%
	• $2,500,001 to $5,000,000	21%
	• $5,000,001 to $10,000,000	16%
	• $10,000,001 to $25,000,000	21%
	• $25,000,001 to $50,000,000	12%
	• $50,000,001 to $100,000,000	5%
	• More than $100,000,000	2%
	Total	100%
	Extrapolated value (US$)	16,544,750

Advancing Responsible Information Management

Ponemon Institute is dedicated to independent research and education that advances responsible information and privacy management practices within business and government. Our mission is to conduct high quality, empirical studies on critical issues affecting the management and security of sensitive information about people and organizations.

We uphold strict data confidentiality, privacy and ethical research standards. We do not collect any personally identifiable information from individuals (or organization identifiable information in our business research). Furthermore, we have strict quality standards to ensure that subjects are not asked extraneous, irrelevant or improper questions.

Please contact research@ponemon.org or call us at 800.887.3118 if you have any questions.