Certificate lifecycle management, PKI, and software supply chain security in financial services

Sponsored by DigiCert

Independently conducted by Ponemon Institute LLC
Publication Date: October 2024

Part 1. Introduction

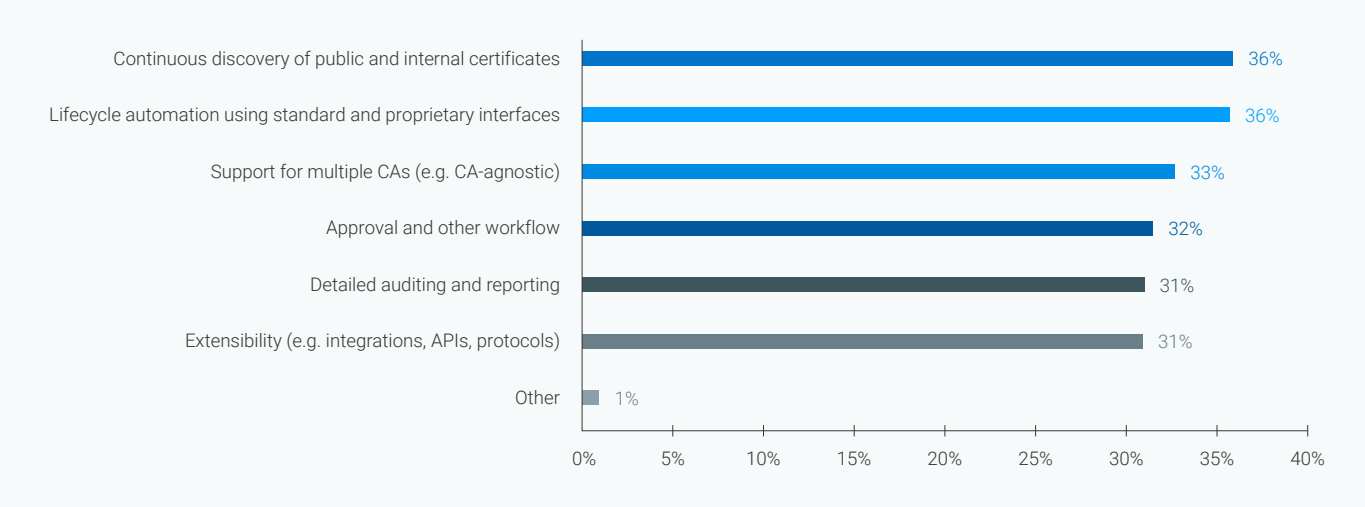
The purpose of this research is to determine how effective the financial services industry is in managing the certificate lifecycle, PKI and securing the software supply chain. As shown in this research, 62 percent of respondents say their organizations experienced one or more outages or security incidents due to an issue with digital certificates that resulted in diminished service quality or availability. Forty-eight percent of respondents say their organizations have been impacted by one or more software supply chain attacks or exploits in the past year. Some of the adverse consequences included putting customers at risk due to a system compromise and prolonged disruption to operations.

Sponsored by DigiCert, Ponemon Institute surveyed 2,546 IT and IT security practitioners in the United States (507 respondents), the United Kingdom (295 respondents), Canada (272 respondents), DACH (Germany and Switzerland 363 respondents), France (361 respondents), Australia (237 respondents), Japan (252 respondents) and Singapore (259 respondents). Forty-eight percent of respondents work in banking and 52 percent are in the insurance industry.

All respondents are familiar with their organization's PKI and involved in certificate lifecycle management (CLM). Ninety-six percent of respondents either have responsibility (47 percent) or share responsibility with others (49 percent) in setting and/or implementing their organizations' software supply chain security strategy.

Conducting inventories to identify every certificate is critical for crypto-agility and becoming quantum-ready. A key takeaway from the research is that *more than half of respondents (51 percent) say their organizations are not taking an inventory to identify every certificate within the organization. Similarly, 51 percent of respondents do not know how many digital certificates, including private root or privately signed, their organizations have. Thirty-six percent of respondents agree, according to Figure 1, the most important feature of a CLM solution is the continuous discovery of public and internal certificates. Another 36 percent of respondents say lifecycle automation using standard and proprietary interfaces is another top two important feature.*

Figure 1. What are the two most important features when choosing a CLM solution?
Two responses permitted



The following research findings describe the current state of CLM, PKI and software supply chain security.

- **Most organizations are in the dark about their certificate inventory and the kind of certificates they have.** As discussed above, *a key takeaway from the research is that more than half of respondents (51 percent) say their organizations are not taking an inventory to identify every certificate within the organization. Similarly, 51 percent of respondents do not know how many digital certificates, including private root or privately signed, their organizations have.* Without this visibility, organizations are at risk because of unsecured certificates within their organization.

- **A CLM solution must support multiple CAs to allow for redundancy and to accommodate the decentralized nature of PKI within enterprises.** *Thirty-three percent of respondents say support for multiple CAs is one of the most important features when choosing a CLM solution.*

- **Certificate outages are common mostly due to expirations or revocations, which can be solved by a CLM solution.** *Sixty-two percent of respondents say their organizations experienced one or more outages due to an issue with digital certificates.* These outages were mainly due to expired certificates, revoked certificates and misconfigured certificates. These risks can be mitigated with an automated CLM system which streamlines the process of CLM through a variety of automated workflows done within a single platform.

- **The most important feature of PKI solutions is the ability to consolidate management of public CA and private CA certificates.** *According to respondents, the most important feature when choosing a PKI, is a single vendor for public CA and private CA certificates (46 percent of respondents). Also important is scalability and performance (46 percent of respondents. The PKI technologies most often used are service provider/cloud provider managed private PKI (44 percent of respondents), internal private PKI (42 percent of respondents) and managed PKI service (e.g. SaaS PKI or PKI as a service) (29 percent of respondents).*

- **Digital certificates** are also known as a public key certificate and used to cryptographically verify the ownership of a public key. Digital certificates are for sharing public keys to be used for encryption and authentication. *According to the research, the most important use case for digital certificates is user authentication for WiFi, VPN or other network access (59 percent of respondents). Authenticating cloud workloads (55 percent of respondents) indicates progress in modernizing digital certificate security. Another important use case is digital signatures for electronic documents (54 percent of respondents).*

- **Software supply chain attacks are growing, primarily from security issues with open source software.** *Forty-eight percent of respondents say their organizations have been impacted by one or more software supply chain attacks in the past year. Most of these attacks were caused by malware, vulnerabilities or other threats in open source software. The two top consequences were customers at risk due to a system compromise and prolonged disruption to operations.*

Part 2. Key Findings

In this section, we provide a deeper dive into the global findings. The complete research findings are presented in the Appendix of the report.

Following are the topics covered in this research.

- Certificate lifecycle management (CLM) and PKI strategies
- Digital certificate security
- Code signing operations
- Securing the software supply chain
- Country and regional differences

Certificate lifecycle management and PKI strategies

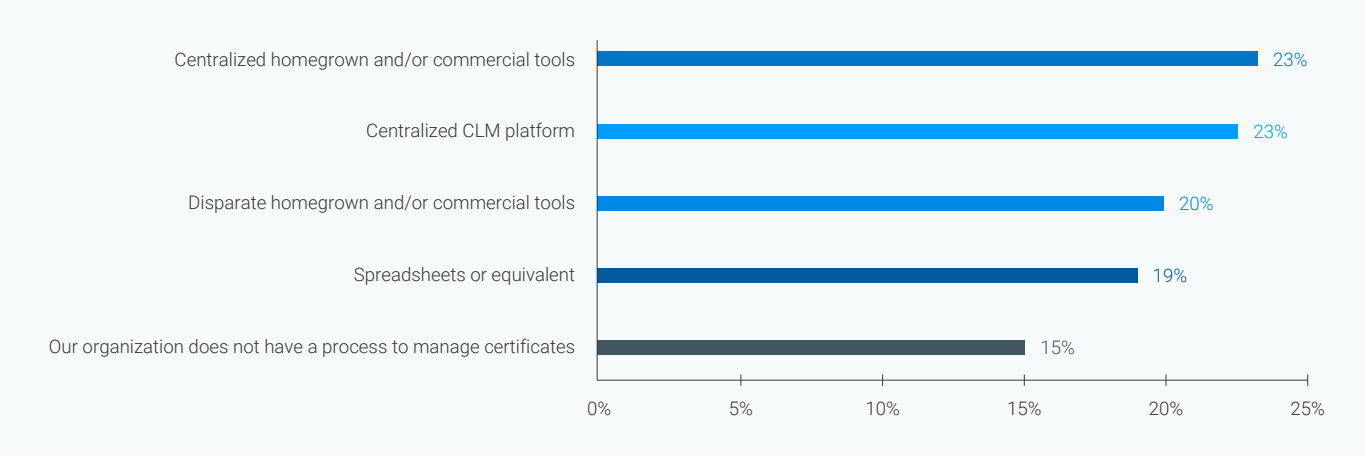
Certificate lifecycle management (CLM) refers to the activities required to ensure digital trust for organizations. CLM best practices for digital certificates include consistent use of tools that provide certificate discovery, access controls to the certificate manager, reporting and certificate lifecycle automation.

Public key infrastructure (PKI) governs the issuance of digital certificates to protect sensitive data, provide unique digital identities for users, devices and applications and secure end-to-end communications.

Most organizations do not have a centralized approach to managing certificates. *According to Figure 2, only 46 percent of respondents say their organizations have centralized management homegrown and/or commercial tools (23 percent) or centralized CLM platform (23 percent).*

The benefits of a centralized approach are that visibility and management across the organization into a single view offers visibility into what may be missing, as well as the status, owner and needs of each asset.

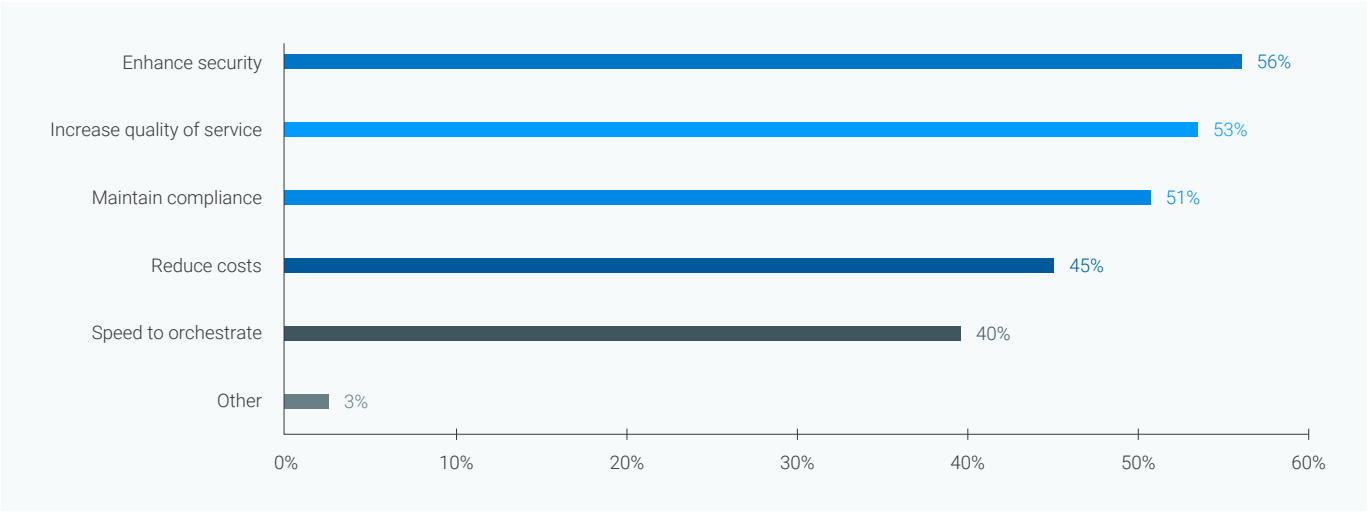
Figure 2. How does your organization manage its certificates?
Only one choice permitted



According to the research, respondents believe that automation increases quality of service and is especially important in highly regulated industries to maintain compliance. In contrast to automation, a manual approach can be inefficient and error prone. The steps taken through automation are certificate discovery, certificate provisioning, certificate monitoring, certificate renewals and certificate revocations and replacements.

CLM automation streamlines operations and enables the ability for swift adaptation to cybersecurity changes. All respondents are involved at some level in CLM. *As shown in Figure 3, the benefits of automating CLM are to enhance security (56 percent of respondents), increase quality of service (53 percent of respondents) and to maintain compliance (51 percent of respondents).*

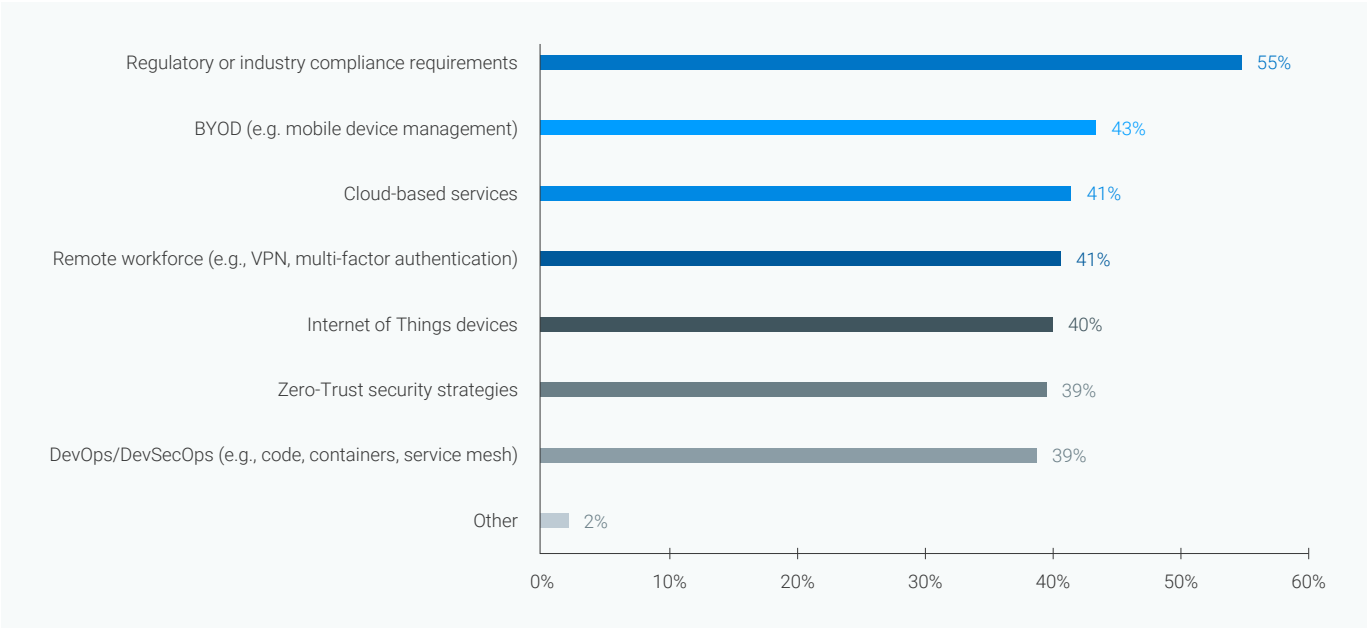
Figure 3. What are the benefits of automating certificate lifecycle management?
More than one response permitted



Regulatory or industry compliance is the most important trend driving deployment of PKI. Financial services is one of the most highly regulated industries. Some regulations include compliance with PCI-DSS, Sarbanes Oxley (SOX) and General Data Protection Regulation (GDPR).

Therefore, it is understandable that *the most important trend to deploying PKI, certificates and other secrets is regulatory of industry compliance (55 percent of respondents), BYOD (43 percent of respondents), remote workforce (41 percent of respondents) and cloud-based services (41 percent of respondents), according to Figure 4.*

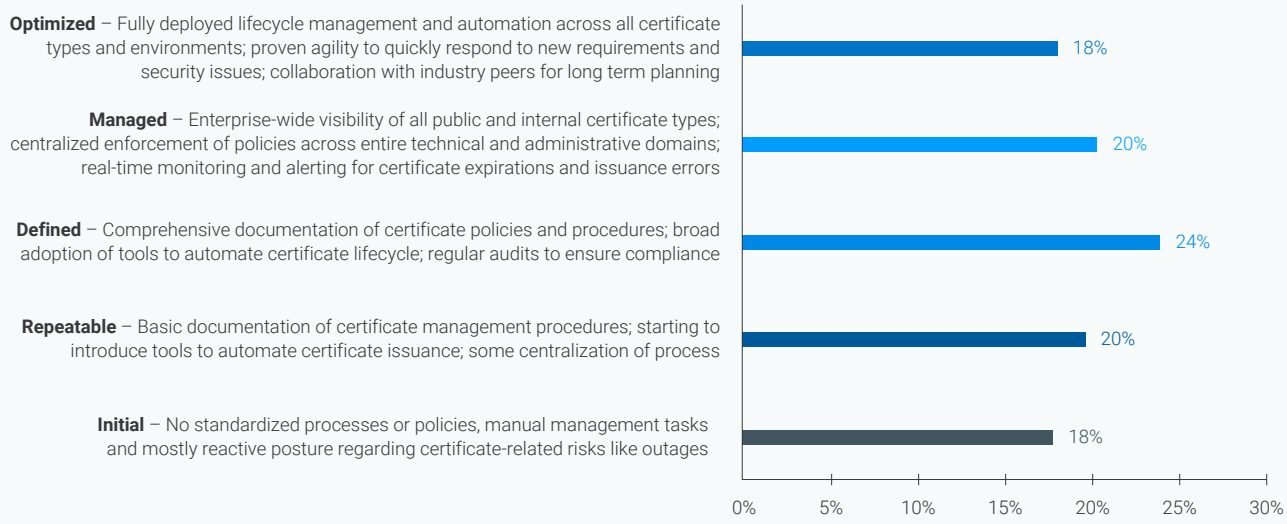
Figure 4. What are the three most important trends that are driving the deployment of PKI, certificates and other secrets?
Three responses permitted



Most organizations have not achieved a high level of CLM maturity. Although respondents recognize the benefits of automating CLM, According to Figure 5, *only 18 percent of respondents say their organizations' CLM is fully optimized and have a fully deployed lifecycle management and automation across all certificate types and environments, proven agility to quickly respond to new requirements and security issues and collaboration with industry peers for long-term planning.*

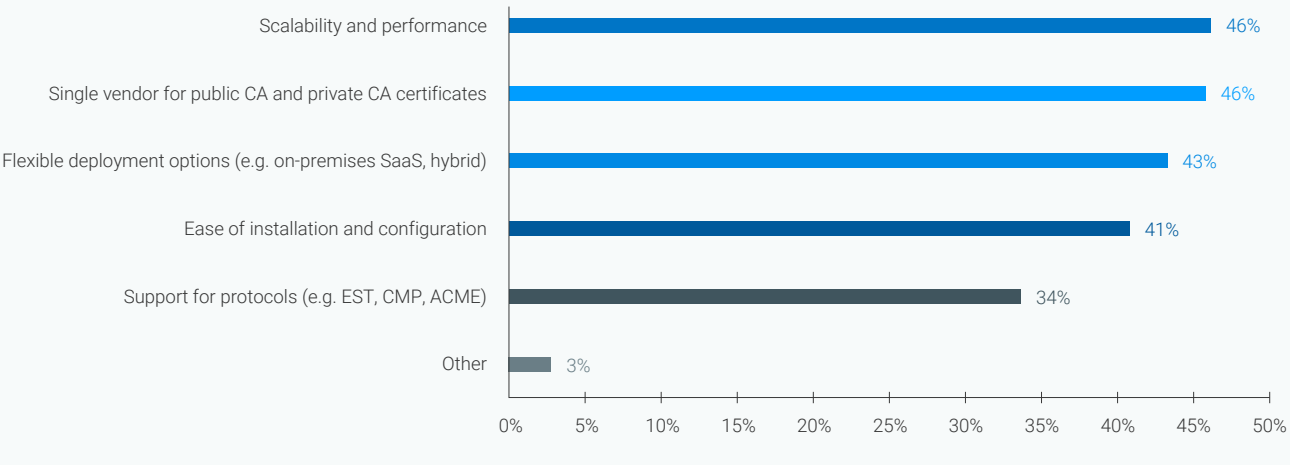
Twenty percent of respondents say the CLM is managed with enterprise-wide visibility of all public and internal certificate types; centralized enforcement of policies across entire technical and administrative domains; real-time monitoring and alerting for certificate expirations and issuance errors.

Figure 5. What best describes the maturity of your organization's CLM?



The most important feature of a PKI is single vendor for public CA and private CA certificates. Also important is scalability and performance, as shown in Figure 6. *The PKI technologies most often used are a service provider/cloud provider managed PKI (44 percent of respondents), internal private PKI (42 percent of respondents) and managed PKI service (e.g. SaaS PKI as a service) (29 percent of respondents).*

Figure 6. What are the most important features when choosing a PKI solution?
More than one response permitted



Crypto agility is the capacity for an information security system to adopt an alternative to the original encryption method or cryptographic primitive without significant change to system infrastructure.

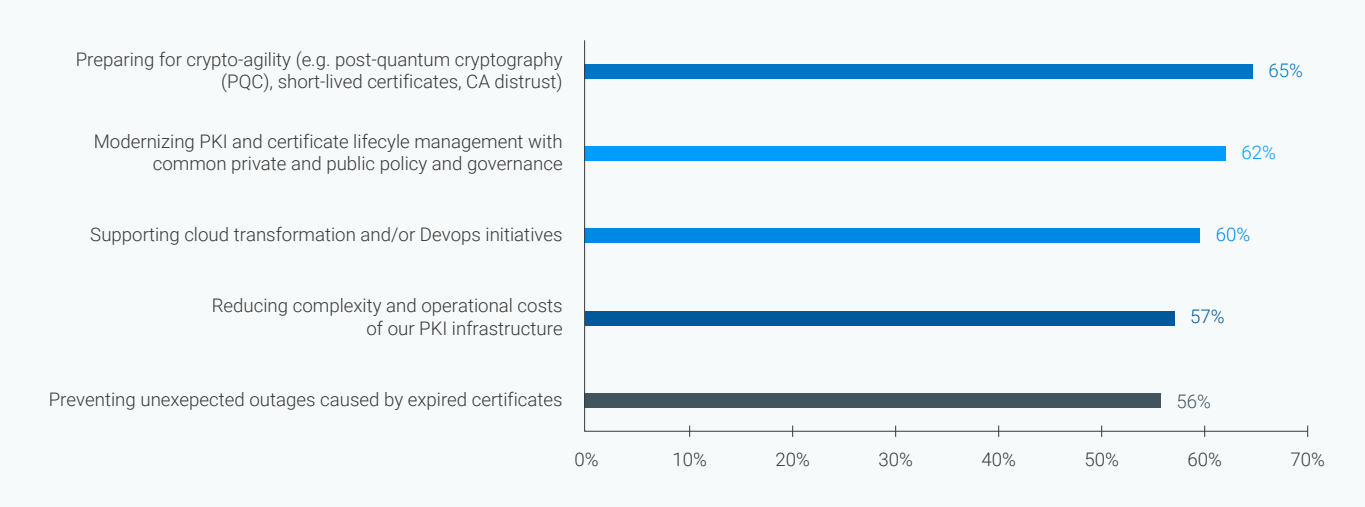
Fifty-six percent of respondents say the risk associated with the inability to adapt to changes in cryptography such as algorithm deprecation and quantum computing is very high.

Organizations are prioritizing preparing for crypto agility. As shown in Figure 7, *the primary priority for organizations' cryptography strategy is to prepare for crypto agility (65 percent of respondents). Modernizing PKI and CLM with common private and public policy and governance (62 percent of respondents) is a priority for cryptography.*

Automating PKI is designed to streamline and secure the entire lifecycle of digital certificates. Automating processes such as generation, validation, issuance, renewal and revocation of certificates are a more effective approach to CLM. This can help organizations enhance their security posture, reduce human error and ensure compliance with industry regulations, thereby creating a more efficient and secure digital environment.

Sixty percent of respondents say supporting cloud transformation and/or DevOps initiatives is a priority. Fifty-seven percent of respondents say a priority is reducing complexity and operational costs of the PKI infrastructure.

Figure 7. What are your three strategic priorities for cryptography within your organization?
Three responses permitted

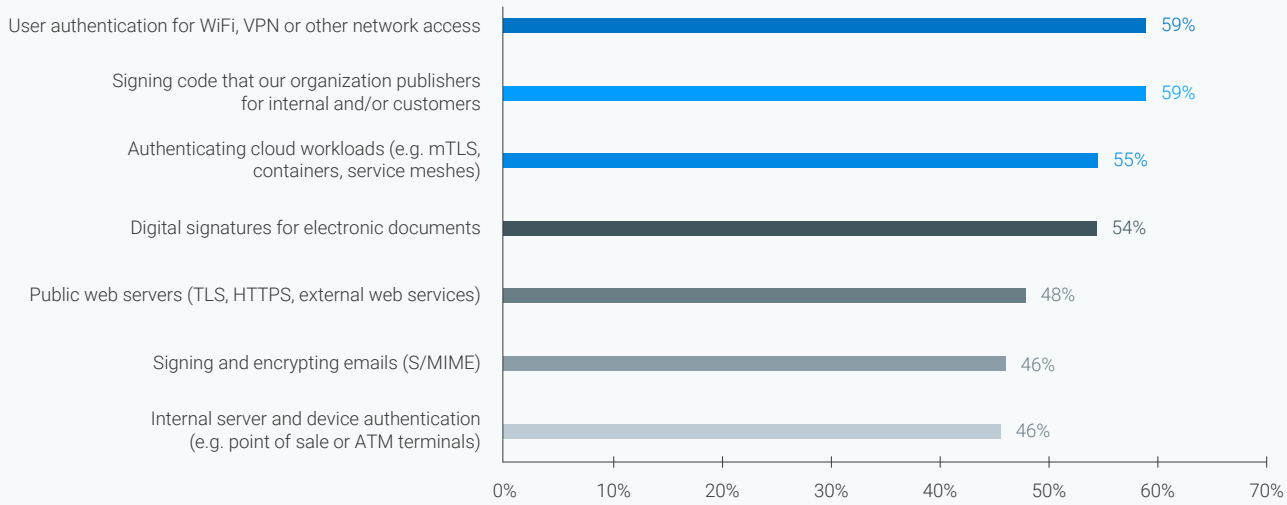


Digital certificate security

Digital certificates are also known as a public key certificate and used to cryptographically verify the ownership of a public key. Digital certificates are for sharing public keys to be used for encryption and authentication.

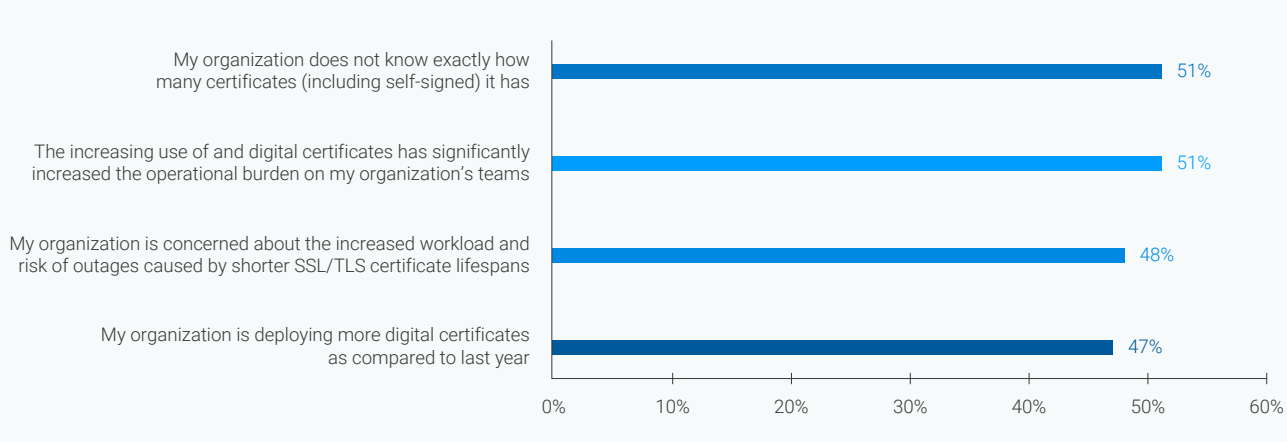
Figure 8 presents various use cases for digital certificates. *The most important use case for digital certificates is user authentication for WiFi, VPN or other network access (59 percent of respondents). Another important use is signing code that our organization publishes for internal and/or customers (59 percent or respondents). Authenticating cloud workloads (55 percent of respondents) indicates progress in modernizing digital certificate security. Another important use case is digital signatures for electronic documents (54 percent of respondents).*

Figure 8. How does your organization use digital certificates?
More than one response permitted



The increasing use of digital certificates is a significant burden for IT security. As shown in Figure 9, *47 percent of respondents say their organizations are deploying more digital certificates as compared to last year. Fifty-one percent of respondents say the increasing use of digital certificates has increased the operational burden on their staff.*

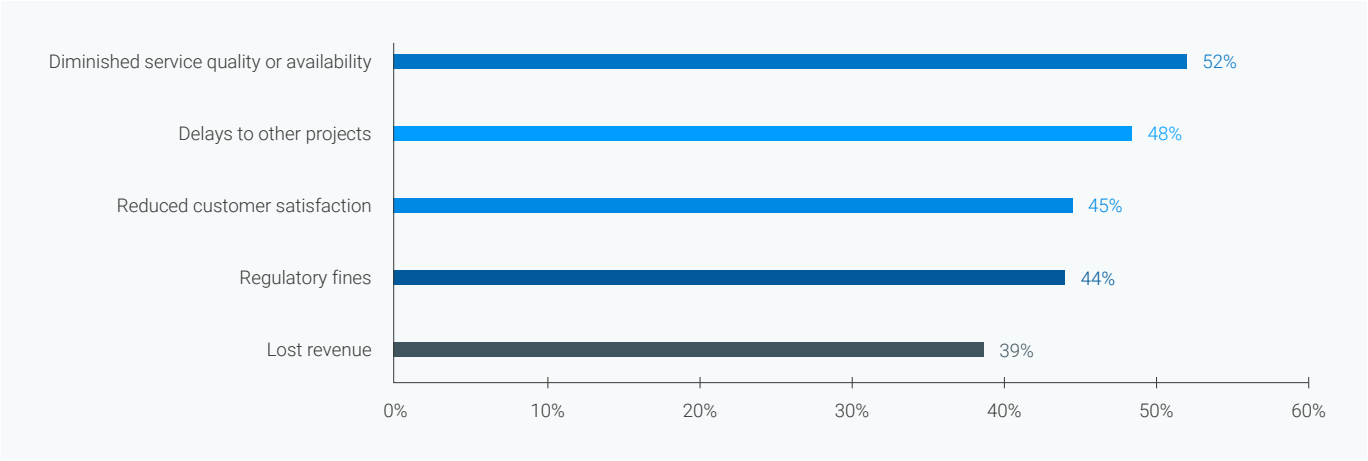
Figure 9. The increased deployment of digital certificates impacts an organization's security.
Strongly agree and Agree responses combined



Sixty-two percent of respondents say their organizations experienced one or more outages or security incidents due to an issue with digital certificates. These respondents were asked to rank the severity of these incidents from 1 = not severe to 10 = very severe. *Fifty-six percent of respondents say the incidents were severe or very severe.*

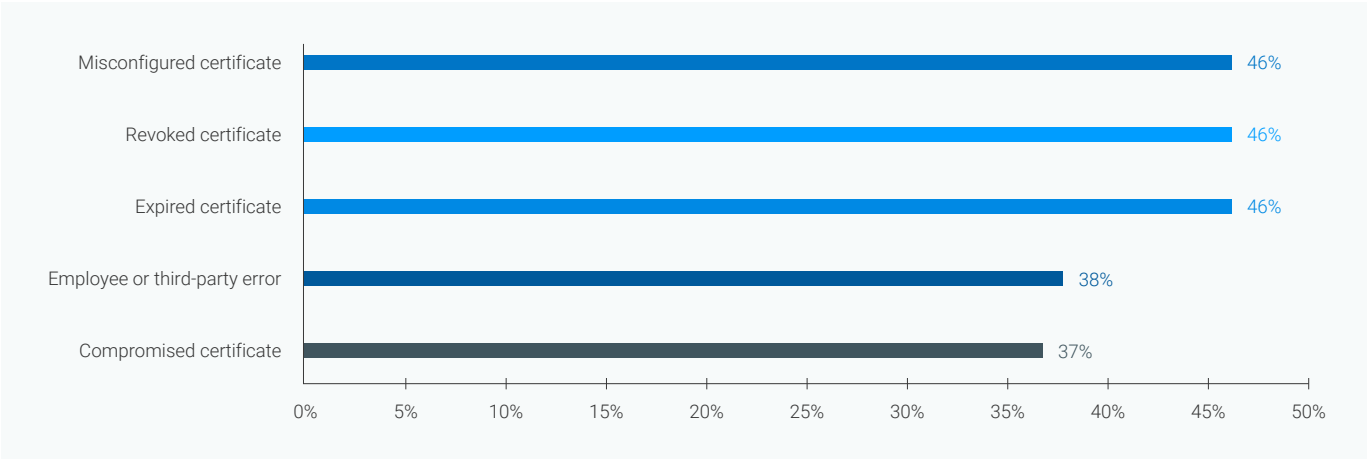
According to Figure 10, *the most significant consequences were diminished service quality or availability (52 percent of respondents), delays to other projects (48 percent of respondents) and reduced customer satisfaction (45 percent of respondents).*

Figure 10. How did the outages or security incidents affect your organization?
More than one response permitted



Outages or security incidents due to an issue with digital certificates were mostly caused by expired certificates, revoked certificates and misconfigured certificates (all 46 percent of respondents), as shown in Figure 11. Respondents were asked to rank the risk associated with misconfiguration of certificates from 1 = low risk to 10 = high risk. *Fifty-seven percent of respondents say the risk is a high risk.*

Figure 11. What was the cause of security incidents due to an issue with digital certificates?

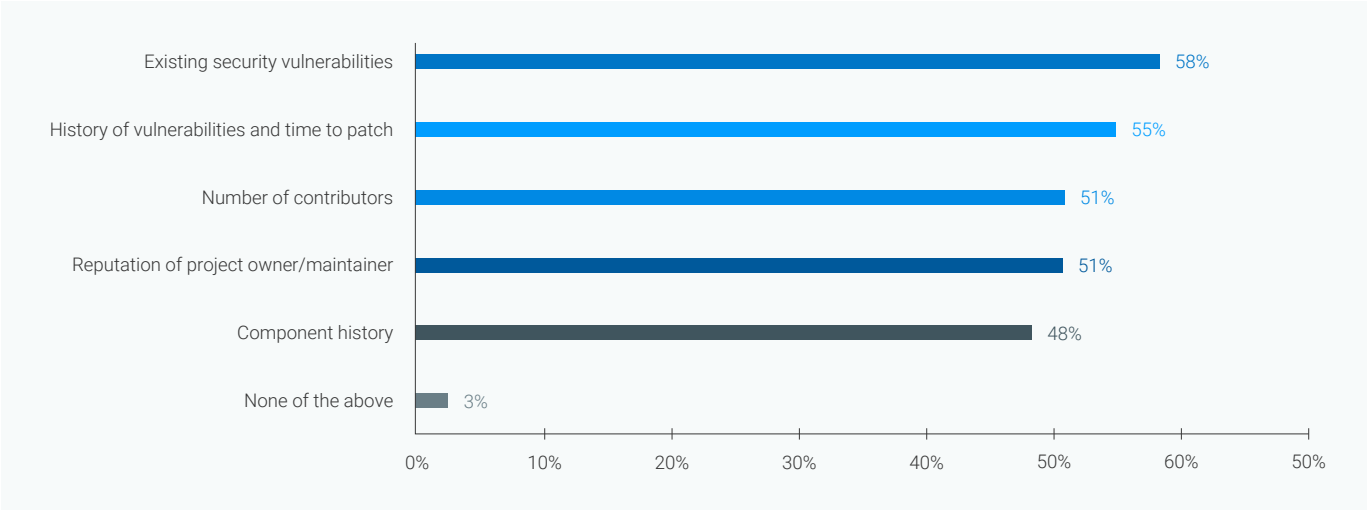


Code signing operations

Code signing is the process of digitally signing executables and scripts to confirm that the software has not been altered or corrupted since it was signed. The process employs the use of a cryptographic hash to validate authenticity and integrity.

Sixty percent of development teams in this study use open source software. Of these respondents, 58 percent of respondents say their organizations evaluate the security of open source components based on existing security vulnerabilities. Fifty-five percent of respondents say the history of vulnerabilities and time to patch are used to evaluate the security of open source components, as shown in Figure 12.

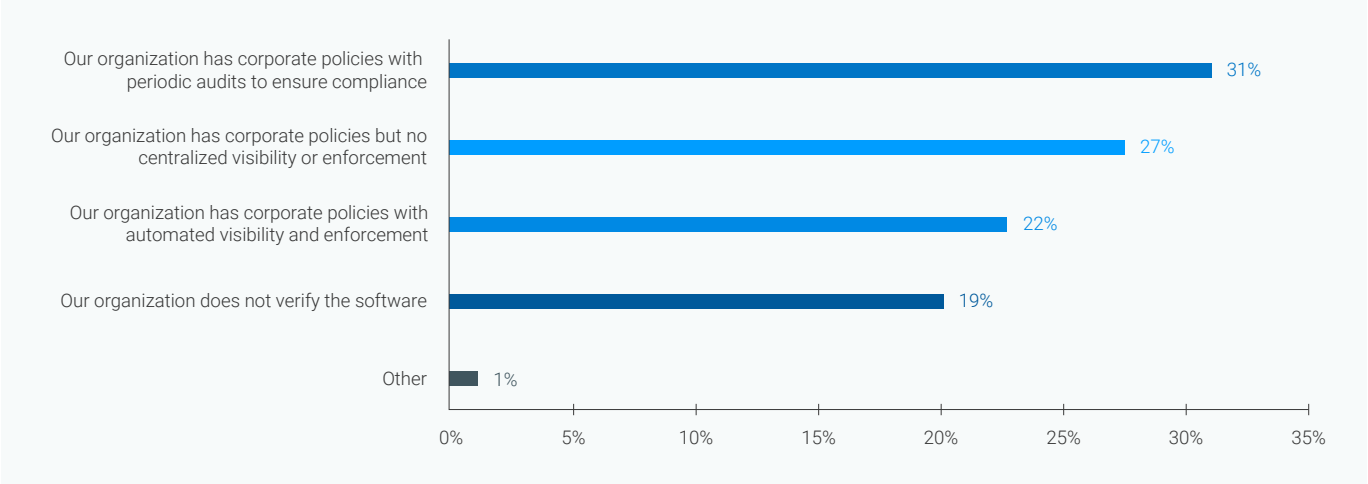
Figure 12. What factors are used to evaluate the security of open source components?
More than one response permitted



Fifty-seven percent of respondents say their organizations are concerned or extremely concerned that their organizations publish software that has been compromised by software supply chain attack keys.

As shown in Figure 13, to verify the software it publishes, *organizations are mainly using corporate policies with periodic audits to ensure compliance (31 percent of respondents) or corporate policies but with no centralized visibility or enforcement (27 percent of respondents).*

Figure 13. How does your organization verify software it publishes?



As shown in Figure 14, *the two most important features in code-signing solutions are policy and workflow enforcement (44 percent of respondents) and auditing and reporting (40 percent of respondents).*

Figure 14. When choosing a code-signing solution what are the most important features?
Two responses permitted

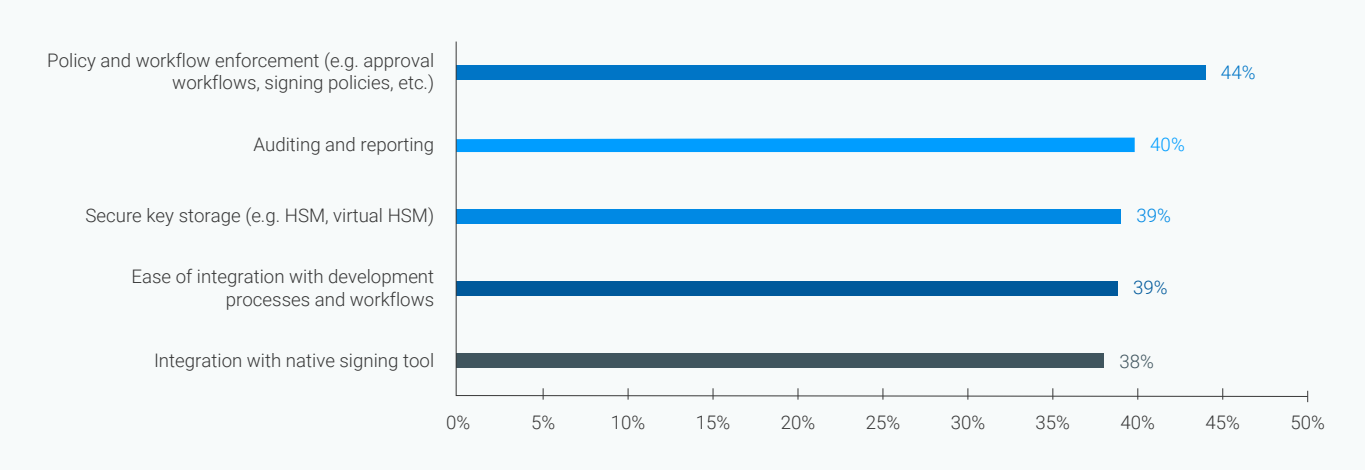
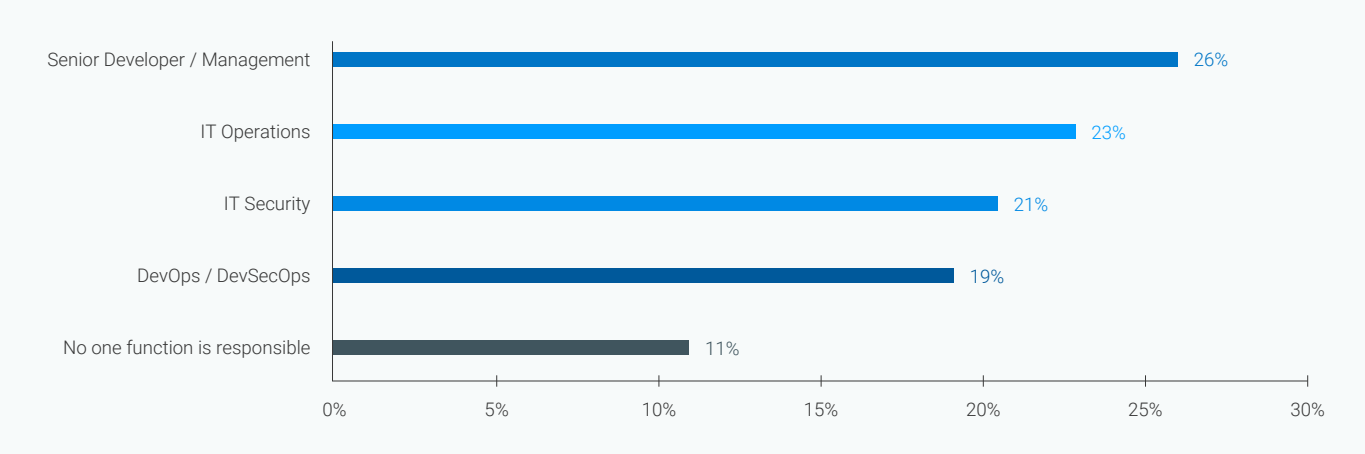


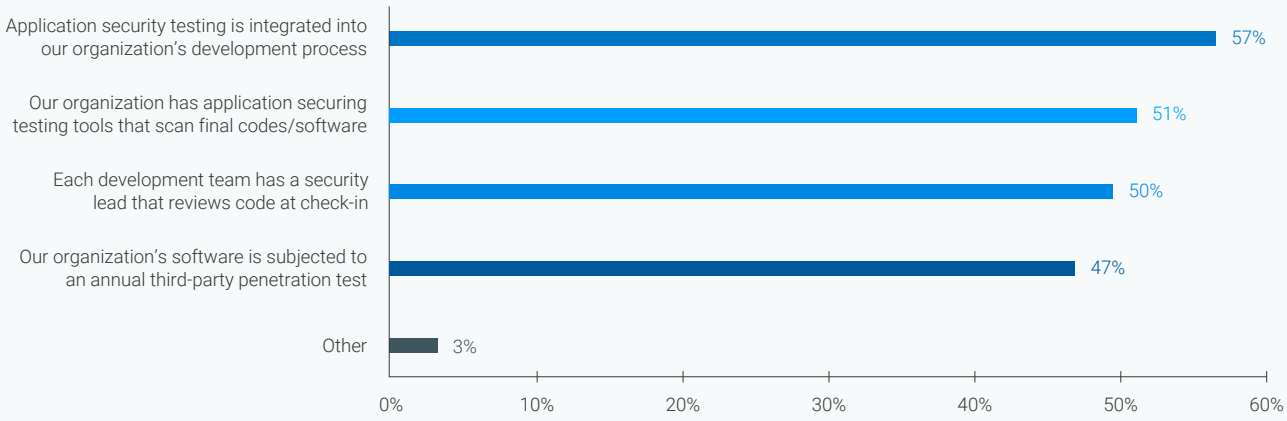
Figure 15 lists the various roles responsible for monitoring and enforcing enterprise code signing. As shown, *senior developers/ managers are most responsible according to 26 percent of respondents followed by IT operations according to 23 percent of respondents.*

Figure 15. Who is most responsible for monitoring and enforcing enterprise code signing?
Only one choice permitted



Fifty-five percent of respondents say their organizations scan for and manage potential threats and vulnerabilities in the software it publishes. *As shown in Figure 16, application security testing is integrated into organizations' development process, according to 57 percent of respondents. Other methods for scanning and managing potential threats are application securing testing tools that scan final code/software (51 percent of respondents) and each development team has a security lead that reviews code at check-in (50 percent of respondents).*

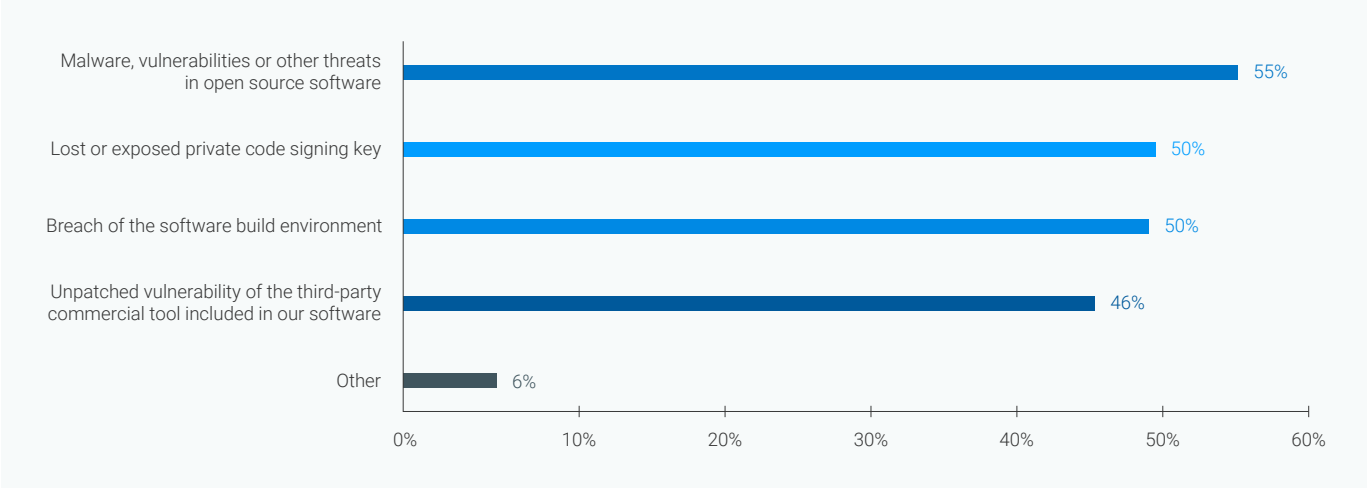
Figure 16. How does your organization scan for and manage potential threats and vulnerabilities in the software it publishes?
More than one response permitted



Securing the software supply chain

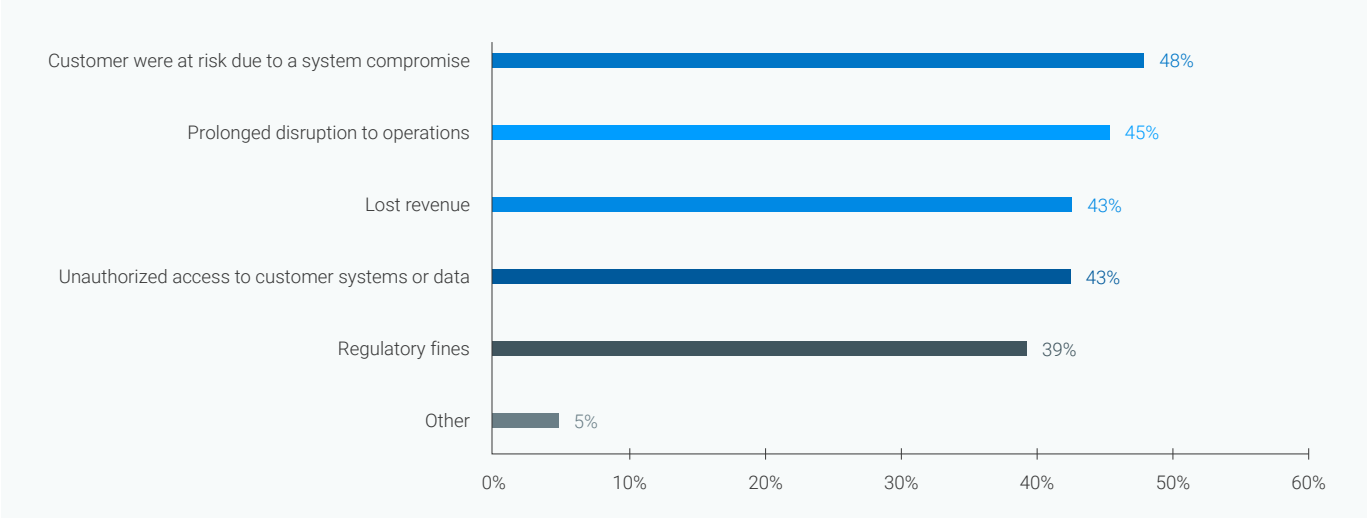
Forty-eight percent of respondents say their organizations have been impacted by one or more software supply chain attacks or exploits in the past year. *Of these respondents, 65 percent say they had one (36 percent) or between two and three (29 percent). According to Figure 17, most supply chain attacks are caused by malware, vulnerabilities or other threats in open source software, according to 55 percent of respondents followed by lost or exposed private code signing key, according to 50 percent of respondents.*

Figure 17. What was the nature of the supply chain attack?
More than one response permitted



According to Figure 18, *the primary impacts to the software supply chain were making customers at risk due to a system compromise (48 percent of respondents) and prolonged disruption to operations (45 percent of respondents).*

Figure 18. What was the impact to the software supply chain?
More than one response permitted

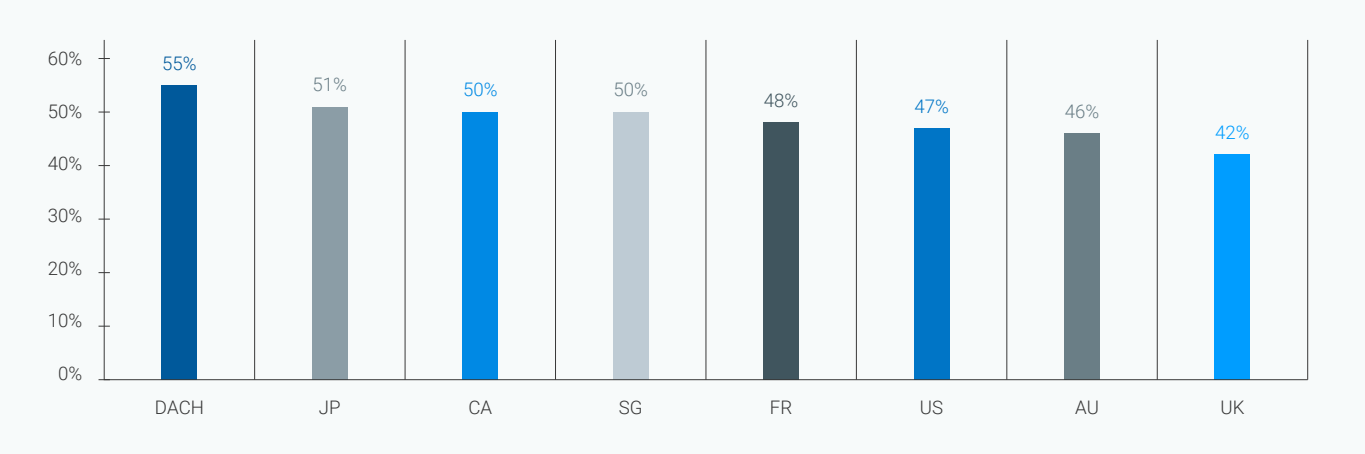


Country and regional differences

In this section, we provide interesting differences in the responses from the United States (507 respondents), the United Kingdom (295 respondents), Canada (272 respondents), DACH (Germany and Switzerland 363 respondents), France (361 respondents), Australia (237 respondents), Japan (252 respondents) and Singapore (259 respondents).

DACH leads other countries in conducting inventories to identify every certificate within their organizations (55 percent of respondents). *According to Figure 19, the biggest laggards are the US (47 percent of respondents), Australia (46 percent of respondents) and the United Kingdom (42 percent of respondents).*

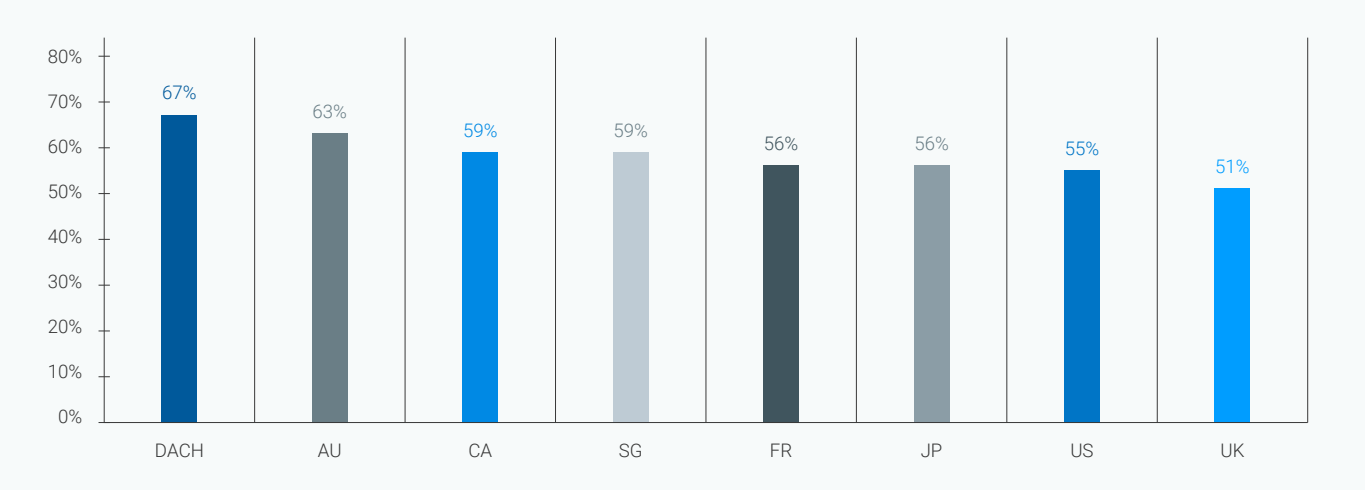
Figure 19. Has your organization taken an inventory to identify every certificate within the organization?
Yes responses presented



Respondents in DACH are most likely to believe it is highly critical to monitor and manage their organization's public and internal certificates, according to 67 percent of respondents. Respondents were asked to rate how critical it is to monitor and manage their organization's public and internal certificates on a scale from 1 = not critical to 10 = highly critical.

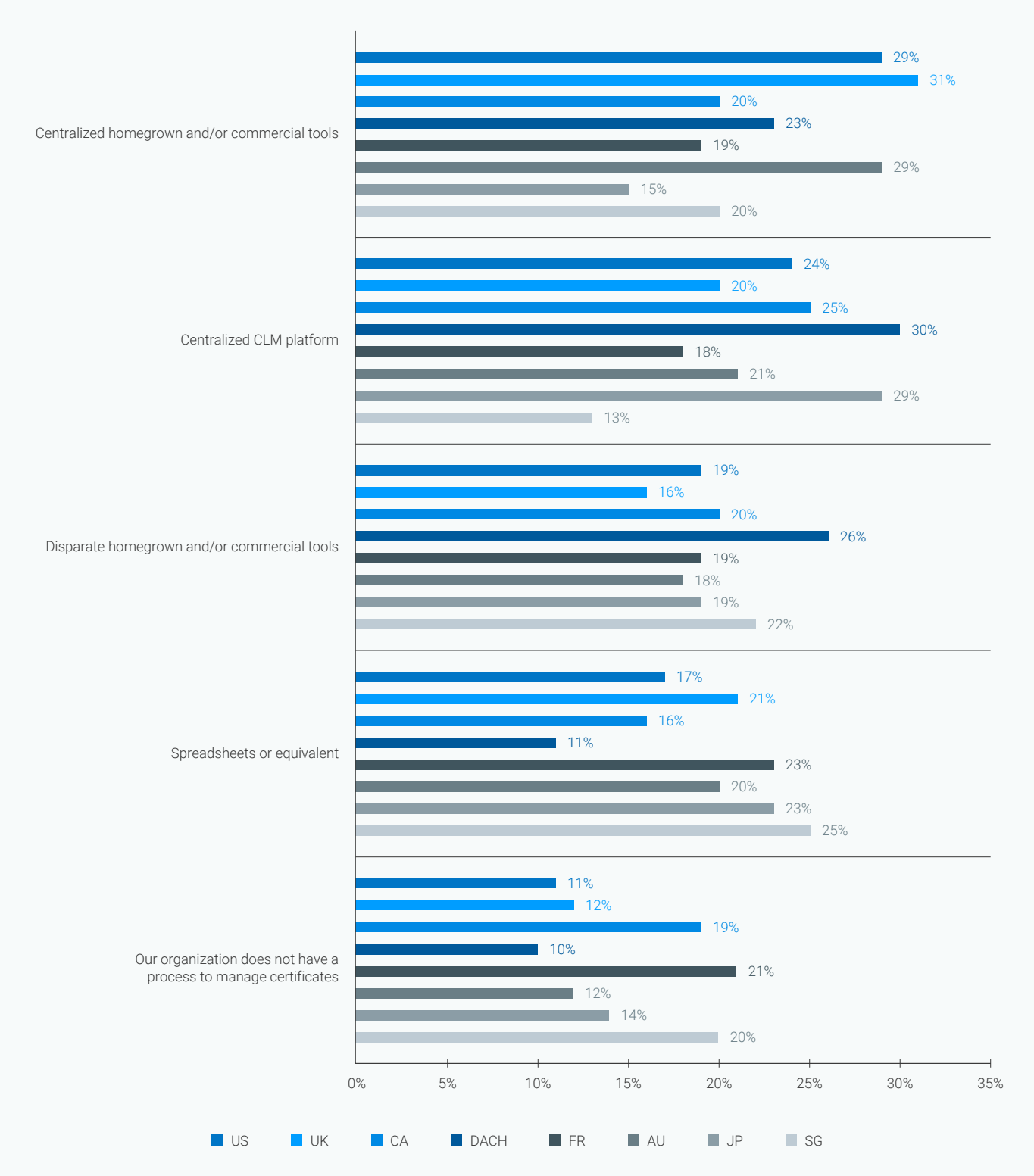
Figure 20 presents the very and highly critical responses (7+ responses). *Australia follows with 63 percent of respondents. Significant differences exist between DACH and US and the UK (55 percent and 51 percent of respondents, respectively).*

Figure 20. How critical is the monitoring and managing of your organization's public and internal certificates.
On a scale from 1 = not critical to 10 = highly critical, 7+ responses presented



The UK (31 percent of respondents), Australia (29 percent of respondents) and the US (29 percent of respondents) are most likely to manage their certificates using a centralized homegrown and/or commercial tool, as shown in Figure 21. The US is most likely to use a centralized CLM platform (30 percent of respondents) and disparate homegrown and/or commercial tools (26 percent of respondents). France (23 percent of respondents), Japan (23 percent of respondents) and Singapore (25 percent of respondents) are most likely to use spreadsheets or equivalent.

Figure 21. How does your organization manage its certificates?



Ownership of the CLM strategy is critical to ensuring its success. However, as shown in Figure 22, *the US (63 percent of respondents), UK (59 percent of respondents) and Canada (61 percent of respondents) say there is no clear ownership for their CLM strategy. A main challenge for Australian respondents is insufficient budget (49 percent of respondents).*

Figure 22. What are the two main challenges involved in setting a CLM strategy in your organization?
Two responses permitted

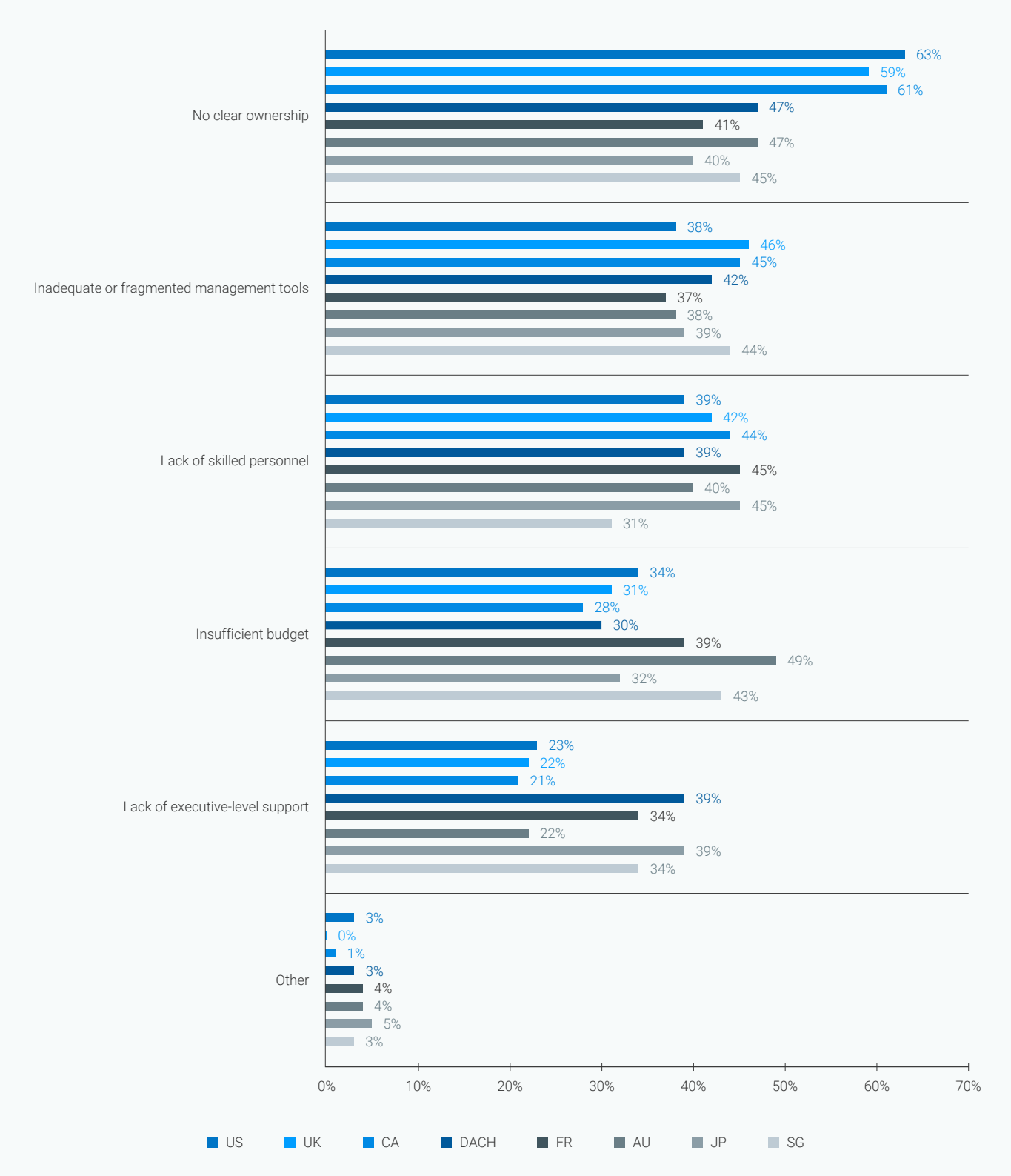
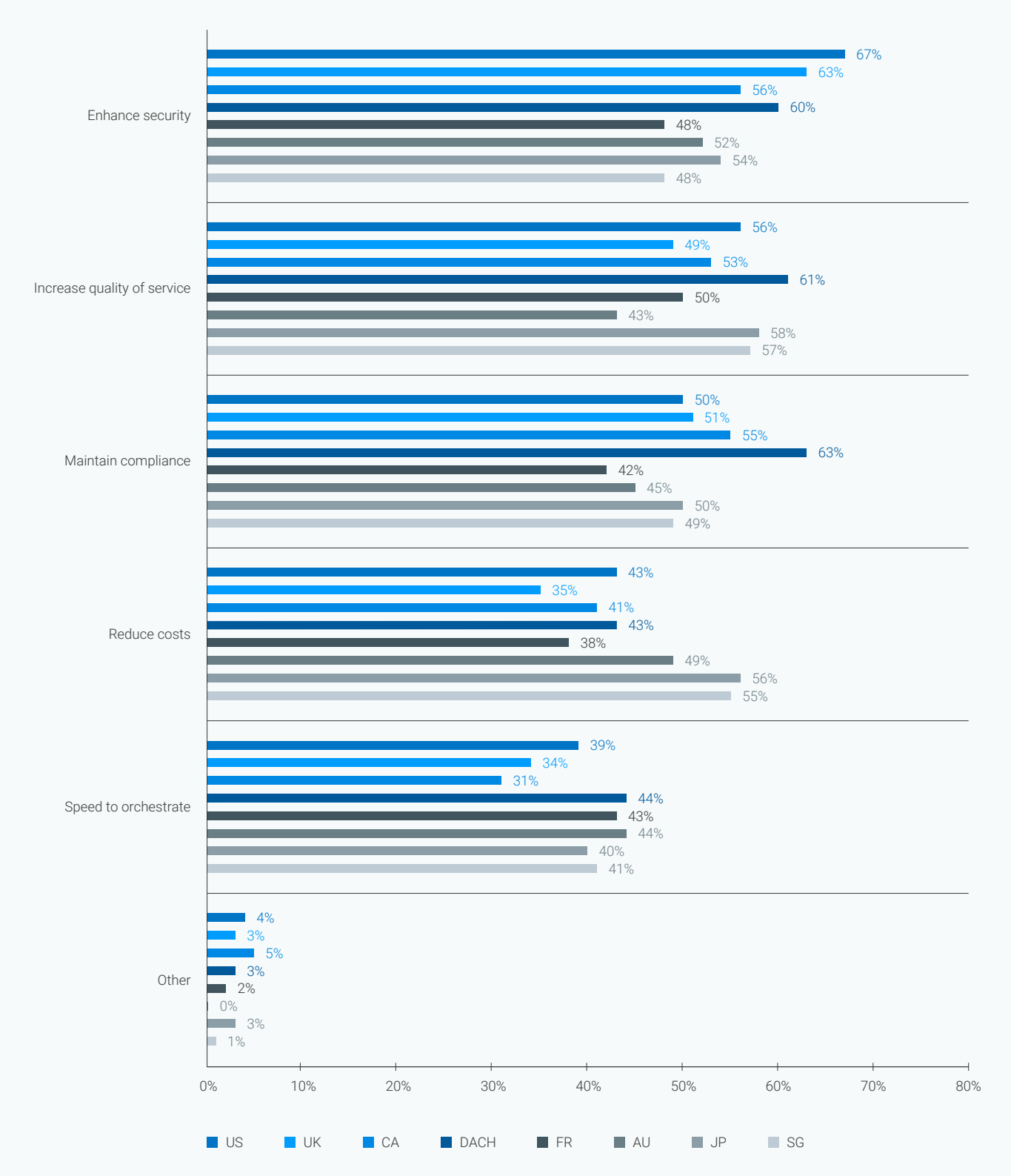


Figure 23 lists the benefits of CLM automation. *The US (67 percent of respondents), the UK (63 percent of respondents) and DACH (60 percent of respondents) say it enhances security. DACH is most likely to say it increases quality of service (61 percent of respondents) and maintains compliance (63 percent of respondents).*

Figure 23. What are the benefits of automating CLM?
More than one response permitted



DACH (57 percent of respondents), the US and Australia (both 51 percent of respondents) are most likely to have a formal access control and approval process for signing software. The UK (45 percent of respondents), France (45 percent of respondents) and Japan (43 percent of respondents) are least likely to have this process in place, as shown in Figure 24.

Figure 24. Does your organization have a formal access control and approval process for signing software?
Yes responses presented

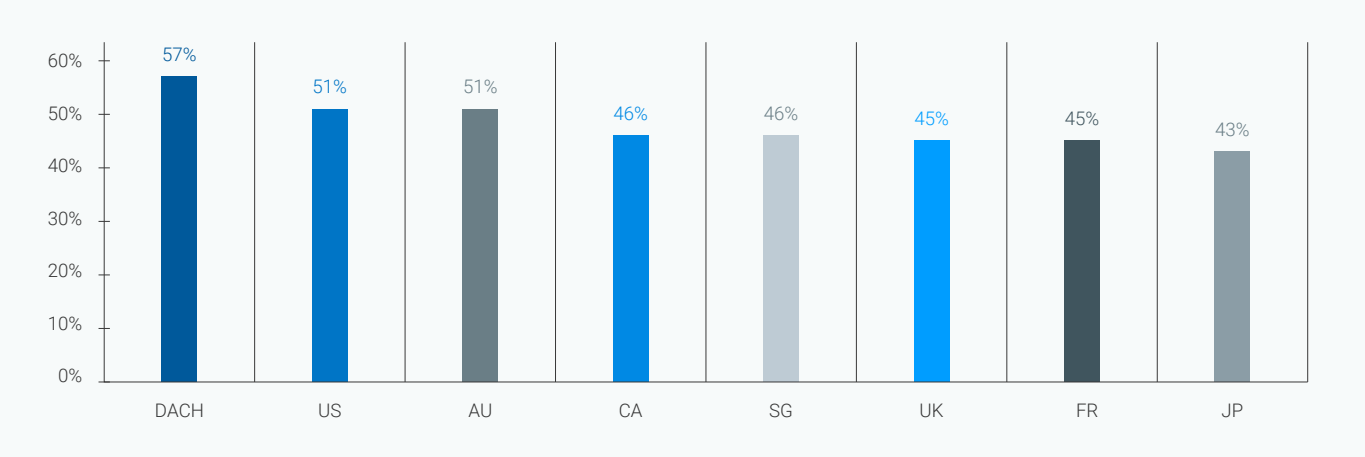
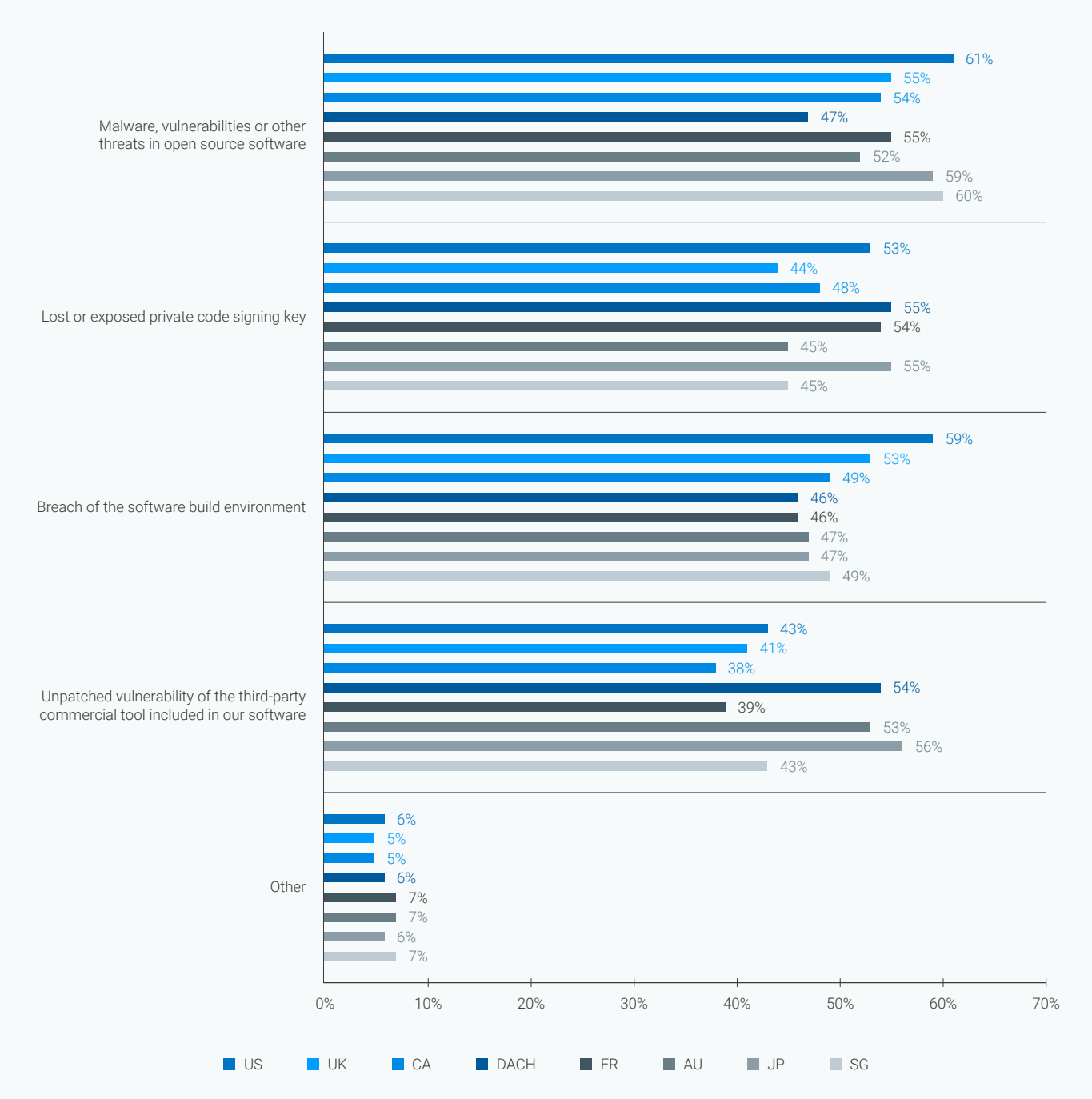


Figure 25 lists the causes of software supply chain attacks experienced by organizations. *Malware, vulnerabilities or other threats in open source software were the top causes for the US (61 percent of respondents), Singapore (60 percent of respondents) and Japan (59 percent of respondents).*

A lost or exposed private code signing key was most often experienced by Japan (55 percent of respondents), DACH (55 percent of respondents) and France (54 percent of respondents). The US (59 percent of respondents) and the UK (53 percent of respondents) were most often to experience a breach of the software build environment. Japan (56 percent of respondents), DACH (54 percent of respondents) and Australia (53 percent of respondents) had a software supply chain attack due to an unpatched vulnerability of the third-party commercial tool included in their software.

Figure 25. What was the nature of the software supply chain attack?
More than one response permitted



Part 3. Methodology

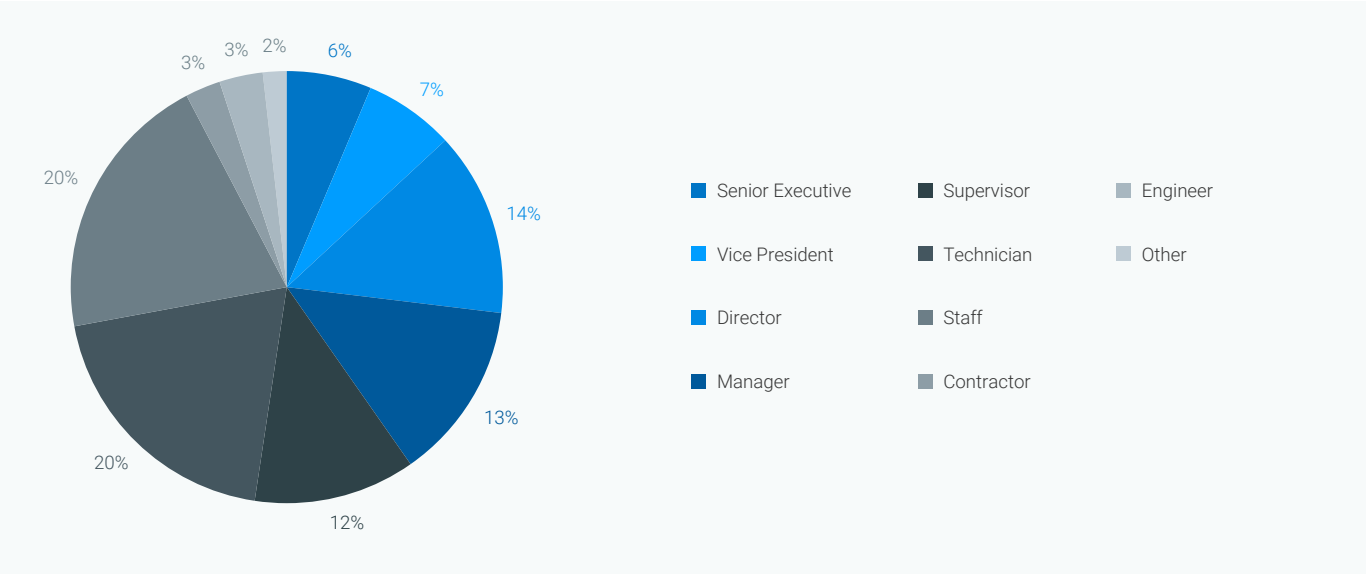
A sampling frame of 78,003 IT and IT security practitioners in the United States, the United Kingdom, Canada, Germany and Switzerland, France, Australia, Japan and Singapore and who are familiar with their organization's PKI and involved in certificate lifecycle management were selected as participants to this survey. Table 1 shows 2,945 total returns. Screening and reliability checks required the removal of 389 surveys. Our final sample consisted of 2,546 surveys or a 3.3 percent response rate.

Table 1. Sample response

Sample response	Freq	Pct %
Sampling frame	78,003	100.0%
Total returns	2,945	3.8%
Rejected or screened surveys	389	0.5%
Final sample	2,546	3.3%

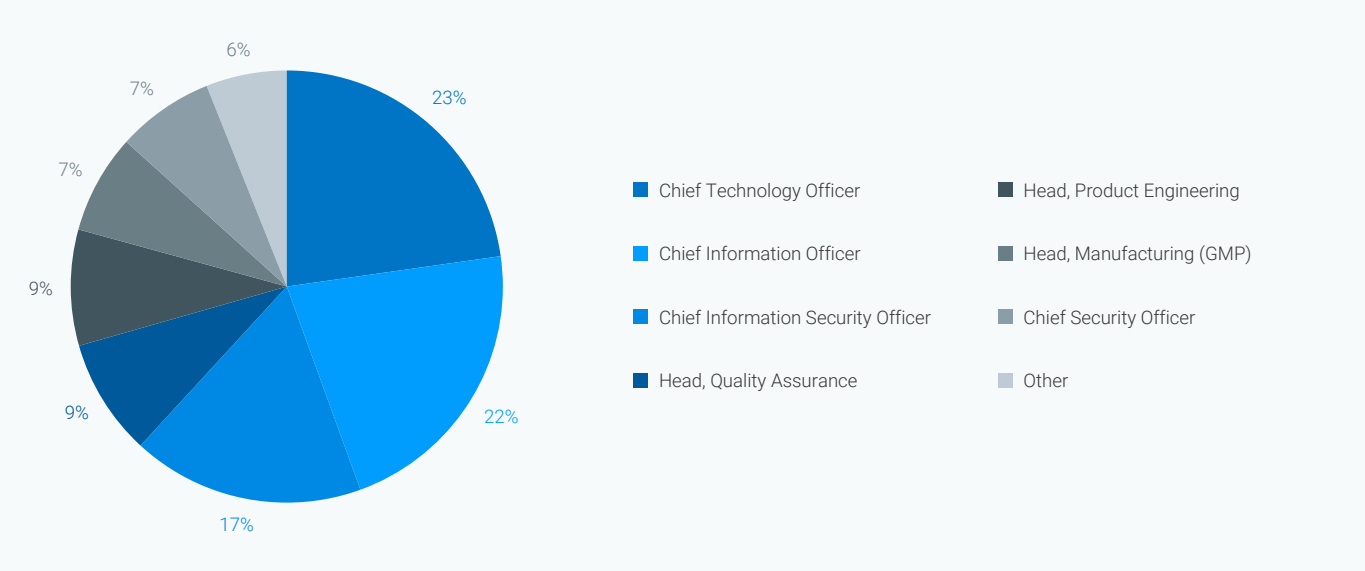
Pie chart 1 reports the respondent's organizational level within participating organizations. Fifty-two percent of respondents are at or above the supervisory levels. The largest categories at 20 percent of respondents are technician and staff.

Pie chart 1. Current position within the organization



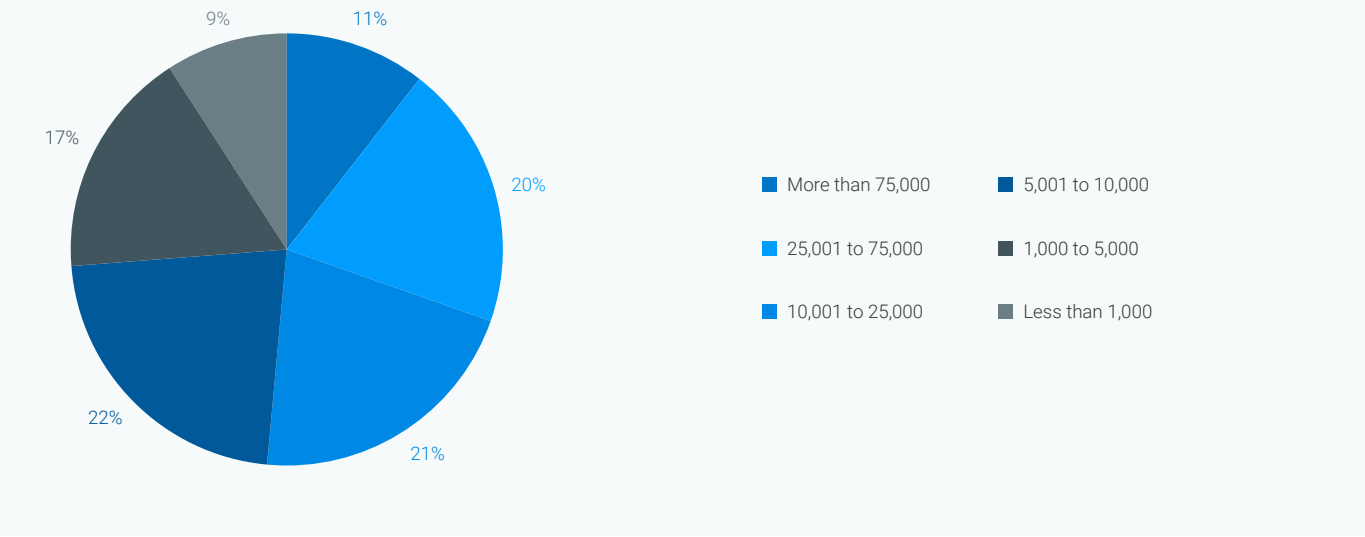
As shown in Pie chart 2, 23 percent of respondents report to the chief technology officer, 22 percent of respondents report to the chief information officer, 17 percent of respondents report to the chief information security officer, 9 percent of respondents report to the head of quality assurance and 9 percent of respondents report to the head of product engineering.

Pie chart 2. Direct reporting channel



Pie chart 3 shows the percentage distribution of companies according to global headcount, which is a surrogate for organizational size. As can be seen, 52 percent of the sample includes larger-sized companies with more than 10,000 full-time equivalent employees.

Pie chart 3. Headcount (size) for participating organizations companies



Part 4. 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 individuals, 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 cybersecurity and IT security practitioners. We also acknowledge that the results may be biased by external events such as media coverage. Finally, 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, there is always the possibility that a subject did not provide accurate responses.

Appendix: Detailed Survey Results

The following tables provide the frequency or percentage frequency of responses to survey questions. All survey responses were captured in June 2024.

Credential and lifecycle management, PKI and software supply chain security in banking and insurance	
Survey response	**Total**
Total sampling frame	78,003
Total returns	2,945
Rejected surveys	389
Final sample	2,546
Response rate	3.3%

Part 1. Screening Questions

S1. What best defines your familiarity with your organization's PKI? Please select one choice only.	Consolidated
Very familiar	28%
Familiar	36%
Somewhat familiar	37%
Not familiar (stop)	0%
Our organization does not have a PKI (stop)	0%
Total	**100%**

S2. How involved are you in certificate lifecycle management in your organization?	Consolidated
Very involved	34%
Involved	33%
Somewhat involved	34%
Not involved (stop)	0%
Total	**100%**

S3. What best describes your organization's financial services industry sectors?	Consolidated
Banking	48%
Insurance	52%
None of the above (stop)	0%
Total	**100%**

S4. What best describes your role/title in your organization?	Consolidated
Chief Information Officer (CIO)	10%
Chief Information Security Officer (CISO)	9%
Chief Technology Officer (CTO)	8%
VP of Information Security	8%
Security Risk Management	10%
DevSecOps Leader	8%
IT Architect	4%
IT Director	8%
IT Manager	9%
PKI Architect	5%
SOC Manager	7%
Security Products Testing	4%
Software Engineering	7%
Other (please specify)	6%
None of the above (stop)	0%
Total	**100%**

Part 2. Certificate lifecycle management and PKI strategies

Q1. Has your organization taken an inventory to identify every certificate within the organization?	Consolidated
Yes	49%
No	51%
Total	**100%**

Q2. How does your organization use digital certificates? Please select all that apply.	Consolidated
Public web servers (TLS, HTTPS, external web services)	48%
Signing and encrypting emails (S/MIME)	46%
User authentication for WiFi, VPN or other network access	59%
Internal server and device authentication (e.g. point of sale or ATM terminals)	46%
Authenticating cloud workloads (e.g. mTLS, containers, service meshes)	55%
Signing code that our organization publishes for internal and/or customers	59%
Digital signatures for electronic documents	54%
Total	**366%**

Q3. Using the following 10-point scale, please rate how critical is the monitoring and managing of your organization's public and internal certificates using a single platform from 1 = not critical to 10 = highly critical.	Consolidated
1 or 2	9%
3 or 4	12%
5 or 6	21%
7 or 8	31%
9 or 10	27%
Total	**100%**

Q4. How does your organization manage its certificates? Please select one choice only.	Consolidated
Spreadsheets or equivalent	19%
Disparate homegrown and/or commercial tools	20%
Centralized homegrown and/or commercial tools	23%
Centralized CLM platform	23%
Our organization does not have a process to manage certificates	15%
Total	**100%**

Q5. What best describes the maturity of your organization's CLM? Please select one choice only.	Consolidated
Initial – No standardized processes or policies, manual management tasks and mostly reactive posture regarding certificate-related risks like outages	18%
Repeatable – Basic documentation of certificate management procedures; starting to introduce tools to automate certificate issuance; some centralization of process	20%
Defined – Comprehensive documentation of certificate policies and procedures; broad adoption of tools to automate certificate lifecycle; regular audits to ensure compliance	24%
Managed – Enterprise-wide visibility of all public and internal certificate types; centralized enforcement of policies across entire technical and administrative domains; real-time monitoring and alerting for certificate expirations and issuance errors	20%
Optimized – Fully deployed lifecycle management and automation across all certificate types and environments; proven agility to quickly respond to new requirements and security issues; collaboration with industry peers for long term planning	18%
Total	**100%**

Q6. What are the two main challenges involved in setting a CLM strategy in your organization? Please select two choices only.	Consolidated
No clear ownership	50%
Lack of skilled personnel	41%
Insufficient budget	36%
Inadequate or fragmented management tools	41%
Lack of executive-level support	29%
Other (please specify)	3%
Total	**200%**

Q7. What are the two most important features when choosing a CLM solution? Please select two choices only.	Consolidated
Continuous discovery of public and internal certificates	36%
Lifecycle automation using standard and proprietary interfaces	36%
Approval and other workflow	32%
Detailed auditing and reporting	31%
Extensibility (e.g. integrations, APIs, protocols)	31%
Support for multiple CAs (e.g. CA-agnostic)	33%
Other (please specify)	1%
Total	**200%**

Q8. What are the benefits of automating certificate lifecycle management? Please select all that apply.	Consolidated
Enhance security	56%
Maintain compliance	51%
Increase quality of service	53%
Reduce costs	45%
Speed to orchestrate	40%
Other (please specify)	3%
Total	**247%**

Q9. In your opinion, what are the three most important trends that are driving the deployment of PKI, certificates and other secrets? Please select three choices only.	Consolidated
Regulatory or industry compliance requirements	55%
BYOD (e.g. mobile device management)	43%
Remote workforce (e.g., VPN, multi-factor authentication)	41%
Internet of Things (IoT) devices	40%
DevOps / DevSecOps (e.g., code, containers, service mesh)	39%
Cloud-based services	41%
Zero-Trust security strategies	39%
Other (please specify)	2%
Total	**300%**

Q10. What are your three strategic priorities for cryptography within your organization? Please select three choices only.	Consolidated
Preparing for crypto-agility (e.g. post-quantum cryptography (PQC), short-lived certificates, CA distrust)	65%
Supporting cloud transformation and/or DevOps initiatives	60%
Modernizing PKI and certificate lifecycle management with common private and public policy and governance	62%
Reducing complexity and operational costs of our PKI infrastructure	57%
Preventing unexpected outages caused by expired certificates	56%
Total	**300%**

Q11a. My organization is deploying more digital certificates as compared to last year.	Consolidated
Strongly agree	23%
Agree	24%
Unsure	19%
Disagree	20%
Strongly disagree	14%
Total	**100%**

Q11b. The increasing use of and digital certificates has significantly increased the operational burden on my organization's teams.	Consolidated
Strongly agree	25%
Agree	26%
Unsure	17%
Disagree	17%
Strongly disagree	15%
Total	**100%**

Q11c. My organization does not know exactly how many digital certificates (including self-signed) it has.	Consolidated
Strongly agree	24%
Agree	27%
Unsure	19%
Disagree	16%
Strongly disagree	14%
Total	**100%**

Q11d. My organization is concerned about the increased workload and risk of outages caused by shorter SSL/TLS certificate lifespans.	Consolidated
Strongly agree	24%
Agree	24%
Unsure	23%
Disagree	16%
Strongly disagree	13%
Total	**100%**

Q12. Using the following 10-point scale, rank the risk associated with misconfiguration of certificates from 1 = low risk to 10 = high risk.	Consolidated
1 or 2	10%
3 or 4	12%
5 or 6	21%
7 or 8	29%
9 or 10	28%
Total	**100%**

Q13. Using the following 10-point scale, rank the risk associated with the inability to adapt to changes in cryptography (e.g. algorithm deprecation, quantum computing, etc.) certificates from 1 = low risk to 10 = high risk.	Consolidated
1 or 2	10%
3 or 4	13%
5 or 6	21%
7 or 8	30%
9 or 10	26%
Total	**100%**

Q14. Which of the following PKI technologies does your organization have? Please select all that apply.	Consolidated
Internal private PKI	42%
Private CA service provided by a cloud provider	44%
Public CA service	42%
Built-in certificate issuers	27%
Self-signed certificates (e.g. Open SSL, CFSSL)	33%
Managed PKI service (e.g. SaaS PKI or PKI as a service)	29%
Other (please specify)	1%
Total	**219%**

Q15. What are the most important features when choosing a PKI solution?	Consolidated
Flexible deployment options (e.g. on-premises, SaaS, hybrid.)	43%
Ease of installation and configuration	41%
Single vendor for public CA and private CA certificates	46%
Support for protocols (e.g. EST, CMP, ACME)	34%
Scalability and performance	46%
Other (please specify)	3%
Total	**212%**

Q16a. In the past year, has your organization experienced one or more outages or security incidents due to an issue with digital certificates?	Consolidated
Yes	62%
No (please skip to Q17a)	29%
Unsure (please skip to Q17a)	9%
Total	**100%**

Q16b. If yes, what was the cause? Please select all that apply.	Consolidated
Expired certificate	46%
Revoked certificate	46%
Compromised certificate	37%
Misconfigured certificate	46%
Employee or third-party error	38%
Other (please specify)	213%

Q16c. How severe were the outages or security incidents from 1 = not severe to 10 = very severe.	Consolidated
1 or 2	10%
3 or 4	12%
5 or 6	22%
7 or 8	28%
9 or 10	28%
Total	**100%**

Q16d. How did the outages or security incidents affect your organization? Please select all that apply.	Consolidated
Lost revenue	39%
Diminished service quality or availability	52%
Reduced customer satisfaction	45%
Regulatory fines	44%
Delays to other projects	48%
Total	**228%**

Part 3. Code signing operations

Q17a. Do your development teams use open source software?	Consolidated
Yes	60%
No (please skip to Q18)	40%
Total	**100%**

Q17b. If yes, what factors are used to evaluate the security of open source components? Please select all that apply.	Consolidated
Existing security vulnerabilities	58%
History of vulnerabilities and time to patch	55%
Reputation of project owner/maintainer	51%
Number of contributors	51%
Component history	48%
None of the above	3%
Total	**266%**

Q18. Are you involved in how your organization signs the software it publishes (code-signing)?	Consolidated
Yes	55%
No (please skip to Q28)	45%
Total	**100%**

Q19. Using the following 10-point scale, how concerned are you that your organization publishes software that has been compromised by software supply chain attack keys from 1 = not concerned to 10 = extremely concerned?	Consolidated
1 or 2	9%
3 or 4	12%
5 or 6	22%
7 or 8	29%
9 or 10	28%
Total	**100%**

Q20. Where are code signing keys stored in your organization? Please select all that apply.	Consolidated
Centralized key storage service (e.g. cloud HSM or vault)	54%
Build servers	49%
Developer workstations	52%
Source code repository	48%
Other (please specify)	6%
Total	**208%**

Q21. Does your organization have a formal access control and approval process for signing software?	Consolidated
Yes	48%
No	52%
Total	**100%**

Q22. How does your organization use code signing throughout your development process? Please select all that apply.	Consolidated
We sign final software executables that we make available for customers	46%
We sign software and scripts that we run on our own systems	32%
Our developers sign software source code commits	34%
Total	**112%**

Q23. What types of groups sign/publish code within the organization?	Consolidated
DevOps and application development teams	35%
Platform teams on cloud orchestration	36%
IT operations on scripts	26%
Other (please specify)	3%
Total	**100%**

Q24. Who is most responsible for monitoring and enforcing enterprise code signing? Please select only one response.	Consolidated
Senior Developer / Management	26%
DevOps / DevSecOps	19%
IT Operations	23%
IT Security	21%
No one function is responsible	11%
Total	**100%**

Q25. When choosing a code-signing solution, what are the most important features? Please select two responses only.	Consolidated
Integration with native signing tool	38%
Policy and workflow enforcement (e.g. approval workflows, signing policies, etc.)	44%
Secure key storage (e.g. HSM, virtual HSM)	39%
Ease of integration with development processes and workflows	39%
Auditing and reporting	40%
Total	**200%**

Q26. How does your organization verify\y software it publishes? Please select one choice only.	Consolidated
Our organization does not verify the software	19%
Our organization has corporate policies but no centralized visibility or enforcement	27%
Our organization has corporate policies with periodic audits to ensure compliance	31%
Our organization has corporate policies with automated visibility and enforcement	22%
Other (please specify)	1%
Total	**100%**

Q27a. Does your organization scan for and manage potential threats and vulnerabilities in the software it publishes?	Consolidated
Yes	55%
No (please skip to Q28)	45%
Total	**100%**

Q27b. If yes, how does your organization scan for and manage potential threats and vulnerabilities in the software it publishes? Please check all that apply.	Consolidated
Each development team has a security lead that reviews code at check-in	50%
Our organization has application securing testing tools that scan final code/software	51%
Application security testing is integrated into our organization's development process	57%
Our organization's software is subjected to an annual third-party penetration test	47%
Other (please specify)	3%
Total	**207%**

Part 4. Securing the software supply chain

Q28. How much responsibility do you have for setting and/or implementing your organization's software supply chain security strategy? This includes addressing risks associated with open source/third party dependencies, source code, development pipelines and general compliance efforts.	Consolidated
I have complete responsibility for the strategy	47%
I share responsibility with others	49%
I have no responsibility (please skip to Part 5)	4%
Total	**100%**

Q29. Has your organization been impacted by one or more software supply chain attacks or exploits in the past year?	Consolidated
Yes	48%
No (please skip to Q33)	47%
Unsure (please skip to Q33)	5%
Total	**100%**

Q30. If yes, how many supply chain attacks or exploits occurred in the past year?	Consolidated
One	36%
2 to 3	29%
4 to 5	21%
More than 5	14%
Total	**100%**

Q31. If yes, what was the nature of the attack(s)? Please select all that apply.	Consolidated
Malware, vulnerabilities or other threats in open source software	55%
Breach of the software build environment	50%
Lost or exposed private code signing key	50%
Unpatched vulnerability of the third-party commercial tool included in our software	46%
Other (please specify)	6%
Total	**207%**

Q32. If yes, what was the impact to the software supply chain? Please select all that apply.	Consolidated
Prolonged disruption to operations	45%
Customers were at risk due to a system compromise	48%
Unauthorized access to customer systems or data	43%
Lost revenue	43%
Regulatory fines	39%
Other (please specify)	5%
Total	**223%**

Q33. Does your organization produce or generate Software Bill of Materials (SBOM)?	Consolidated
Yes	41%
No (please skip to Part 5)	59%
Total	**100%**

Q34. Using the following 10-point scale, rank how critical are SBOMs to reducing risk in the software supply chain from 1 = not critical to 10 = highly critical.	Consolidated
1 or 2	9%
3 or 4	12%
5 or 6	21%
7 or 8	28%
9 or 10	30%
Total	**100%**

Part 5. Organization and respondents' demographics

D1. What organizational level best describes your current position?	Consolidated
Senior Executive	6%
Vice President	7%
Director	14%
Manager	13%
Supervisor	12%
Technician	20%
Staff	20%
Contractor	3%
Engineer	3%
Other	2%
Total	**100%**

D2. Check the Primary Person you or your IT security leader reports to within the organization.	Consolidated
Head, Manufacturing (GMP)	7%
Head, Product Engineering	9%
Head, Quality Assurance	9%
Chief Information Officer	22%
Chief Technology Officer	23%
Chief Information Security Officer	17%
Chief Security Officer	7%
Other (please specify)	6%
Total	**100%**

D3. What range best describes the full-time headcount of your global organization?	Consolidated
Less than 1,000	9%
1,000 to 5,000	17%
5,001 to 10,000	22%
10,001 to 25,000	21%
25,001 to 75,000	20%
More than 75,000	11%
Total	**100%**

D4. In which country/region is your organization located?	Consolidated
United States	20%
United Kingdom	12%
Canada	11%
Germany & Switzerland (DACH)	14%
France	14%
Australia	9%
Japan	10%
Singapore	10%
Total	**100%**

Ponemon Institute

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 company identifiable information in our business research). Furthermore, we have strict quality standards to ensure that subjects are not asked extraneous, irrelevant or improper questions.