Preparing for a Safe Post Quantum Computing Future: A Global Study

Sponsored by DigiCert

Independently conducted by Ponemon Institute LLC

Publication Date: October 2023

digicert

Ponemon INSTITUTE

Preparing for a Safe Post Quantum Computing Future:
A Global Study

Prepared by Ponemon Institute, October 2023

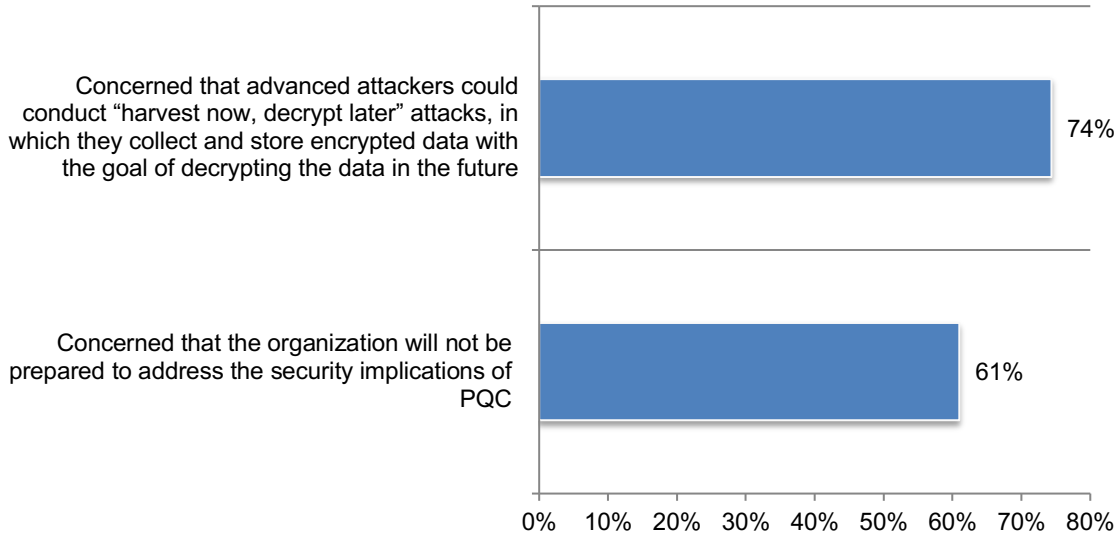
Part 1. Introduction

Sponsored by DigiCert, the purpose of this research is to understand how organizations are addressing the post quantum computing threat and preparing for a safe post quantum computing future. Ponemon Institute surveyed 1,426 IT and IT security practitioners in the United States (605), EMEA (428) and Asia-Pacific (393) who are knowledgeable about their organizations' approach to post quantum cryptography.

Quantum computing harnesses the laws of quantum mechanics to solve problems too complex for classical computers. With quantum computing, however, cracking encryption becomes much easier, which poses an enormous threat to data security.

That is why, as shown in Figure 1, 61 percent of respondents say they are very worried about not being prepared to address these security implications. Another threat of significance is that advanced attackers could conduct "harvest now, decrypt later" attacks, in which they collect and store encrypted data with the goal of decrypting the data in the future (74 percent of respondents). Despite these concerns, only 23 percent of respondents say they have a strategy for addressing the security implications of quantum computing.

Figure 1. There are serious concerns about the risks caused by post quantum computing (PQC)
On a scale from 1 = not concerned to 10 = very concerned, 7+ responses presented



The following findings illustrate the challenges organizations face as they prepare to have a safe post quantum computing future.

Security teams must juggle the pressure to keep ahead of cyberattacks targeting their organizations while preparing for a post quantum computing future. Only 50 percent of respondents say their organizations are very effective in mitigating risks, vulnerabilities and attacks across the enterprise. Reasons for the lack of effectiveness is that almost all respondents say cyberattacks are becoming more sophisticated, targeted and severe. According to the research, ransomware and credential theft are the top two cyberattacks experienced by organizations in this study.

The clock is racing to achieve PQC readiness. Forty-one percent of respondents say their organizations have less than five years to be ready. The biggest challenges are not having enough time, money and expertise to be successful. Currently, only 30 percent of respondents

say their organizations are allocating budget for PQC readiness. One possible reason for not having the necessary support is that almost half of respondents (49 percent) say their organization's leadership is only somewhat aware (26 percent) or not aware (23 percent) about the security implications of quantum computing. Forty-nine percent of respondents are also uncertain about the implications of PQC.

Resources are available to help organizations prepare for a safe post quantum computing future. In the last few years, industry groups such ANSI X9's Quantum Risk Study Group and NIST's post-quantum cryptography project have been initiated to help organizations prepare for PQC. Sixty percent of respondents say they are familiar with these groups. Of these respondents, 30 percent say they are most familiar with the ANSI X9's Quantum Risk Study Group and 28 percent are most familiar with NIST's industry group.

Many organizations are in the dark about the characteristics and locations of their cryptographic keys. Only slightly more than half of respondents (52 percent) say their organizations are currently taking an inventory of the types of cryptography keys used and their characteristics. Only 39 percent of respondents say they are prioritizing cryptographic assets and only 36 percent of respondents are determining if data and cryptographic assets are located on-premises or in the cloud.

Very few organizations have an overall centralized crypto-management strategy applied consistently across the enterprise. Sixty-one percent of respondents say their organizations only have a limited crypto-management strategy that is applied to certain applications or use cases (36 percent) or they do not have a centralized crypto-management strategy (25 percent).

Without an enterprise-wide cryptographic management strategy organizations are vulnerable to security threats, including those leveraging quantum computing methods. Only 29 percent of respondents say their organizations are very effective in the timely updating of their cryptographic algorithms, parameters, processes and technologies and only 26 percent are confident that their organization will have the necessary cryptographic techniques capable of protecting critical information from quantum threats.

While an accurate inventory of cryptographic keys is an important part of a cryptography management strategy, organizations are overwhelmed keeping up with their increasing use. Sixty-one percent of respondents say their organizations are deploying more cryptographic keys and digital certificates. As a result, 65 percent of respondents say this is increasing the operational burden on their teams and 58 percent of respondents say their organizations do not know exactly how many keys and certificates they have.

The misconfiguration of keys and certificates and the ability to adapt to cryptography changes prevents a cryptographic management program from being effective. Sixty-two percent of respondents say they are concerned about the ability to adapt to changes in cryptography such as algorithm deprecation and quantum computing. Another 62 percent are concerned about the misconfiguration of keys and certificates. Fifty-six percent are concerned about the increased workload and risk of outages caused by shorter SSL/TLS certificate lifespans.

To secure information assets and the IT infrastructure, organizations need to improve their ability to effectively deploy cryptographic solutions and methods. Most respondents say their organizations do not have a high ability to drive enterprise-wide best practices and policies, detect and respond to certificate/key misuse, remediate algorithm remediation or breach and prevent unplanned certificates.

Crypto Centers of Excellence (CCOEs) can support organizations' efforts to achieve a safe post quantum computing future. A CCOE can help improve operational cryptographic processes and increase an organization's trust environment. They do require advanced

technologies and expertise in cryptography to maintain secure operations and comply with applicable regulations. Most organizations in this research do plan on having a CCOE. However, currently only 28 percent of respondents say their organizations have a mature CCOE that provides crypto leadership, research, implementation strategy, ownership and best practices. Another 28 percent of respondents say they have a CCOE, but it is still immature.

Hiring and retaining qualified personnel is the most important strategic priority for digital security (55 percent of respondents). This is followed by achieving crypto-agility (51 percent of respondents), which is the ability to efficiently update cryptographic algorithms, parameters, processes and technologies to better respond to new protocols, standards and security threats, including those leveraging quantum computing methods.

Part 2. Key findings

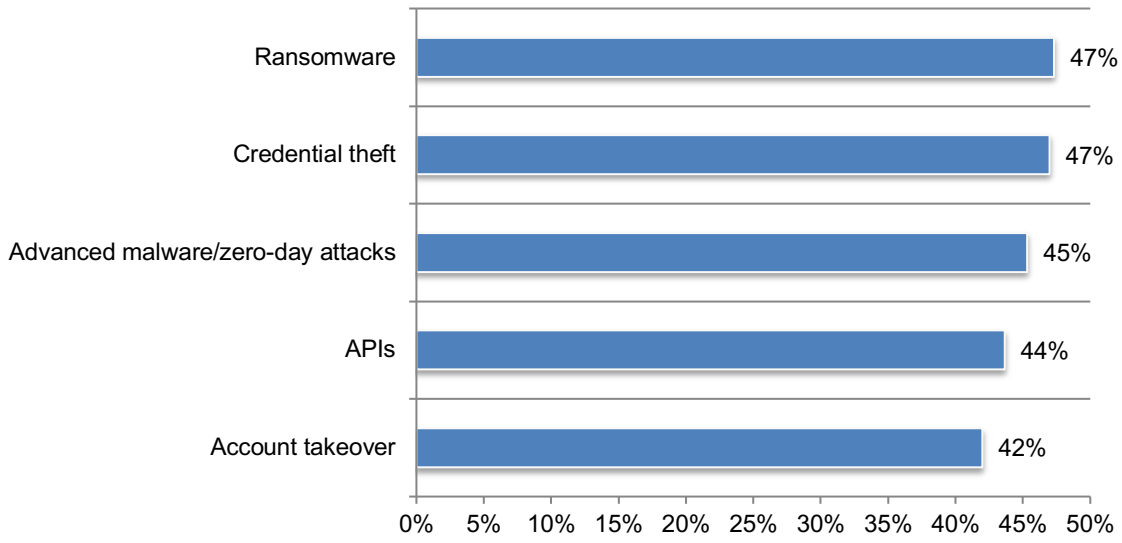
In this section, we provide an analysis of the global research. The complete findings are presented in the Appendix of this report. The report is organized according to the following topics.

- The shaky state of PQC readiness
- Challenges in cryptographic management
- Differences among the United States, EMEA and Asia-Pac organizations
- Best practices in achieving PQC readiness: an analysis of high performing organizations

The shaky state of PQC readiness

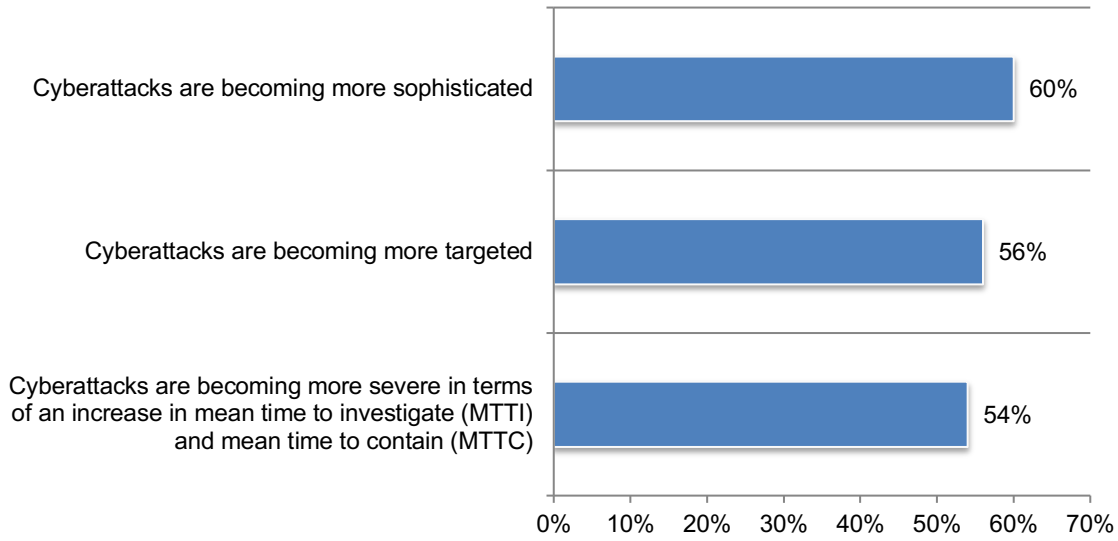
Preparation for PQC must move forward while at the same time dealing with the consequences of such cyberattacks as ransomware and credential theft. Fifty percent of respondents say their organizations are not very effective in mitigating risks, vulnerabilities and attacks across the enterprise. As a result, just in the past year 46 percent of respondents say their organizations had at least one cyberattack and 7 percent are unsure. Figure 2 presents the top five attacks. The top two, as shown, are ransomware and credential theft (both 47 percent of respondents).

Figure 2. Cyberattacks experienced
More than one response permitted



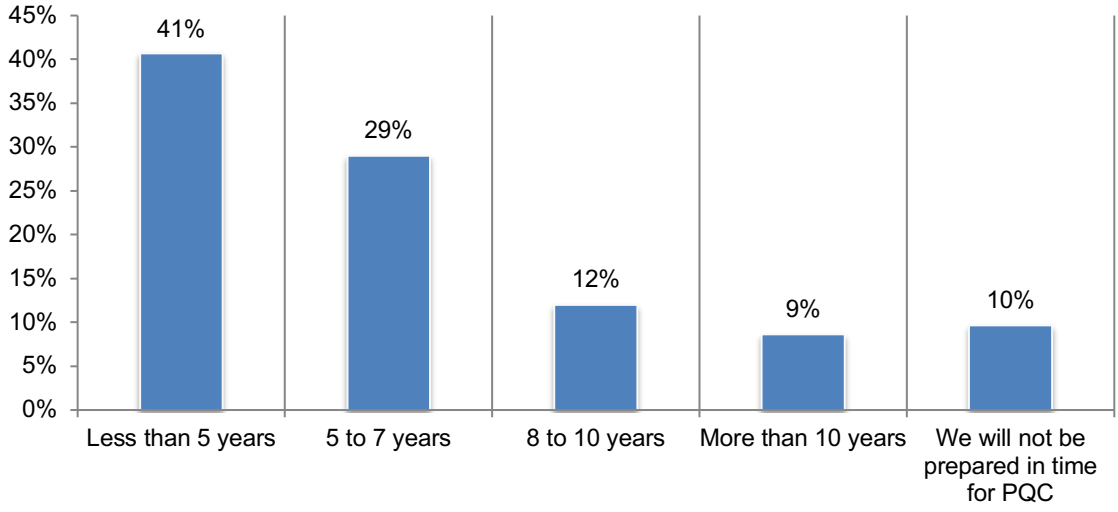
The severity and sophistication of cyberattacks affects organizations' security posture. According to Figure 3, 60 percent of respondents say cyberattacks are becoming more sophisticated, 56 percent say they are becoming more targeted and 54 percent say more severe in terms of an increase in mean time to investigate (MTTI) and mean time to contain (MTTC).

Figure 3. Cyberattacks are becoming more sophisticated, targeted and severe
Strongly agree and Agree responses combined



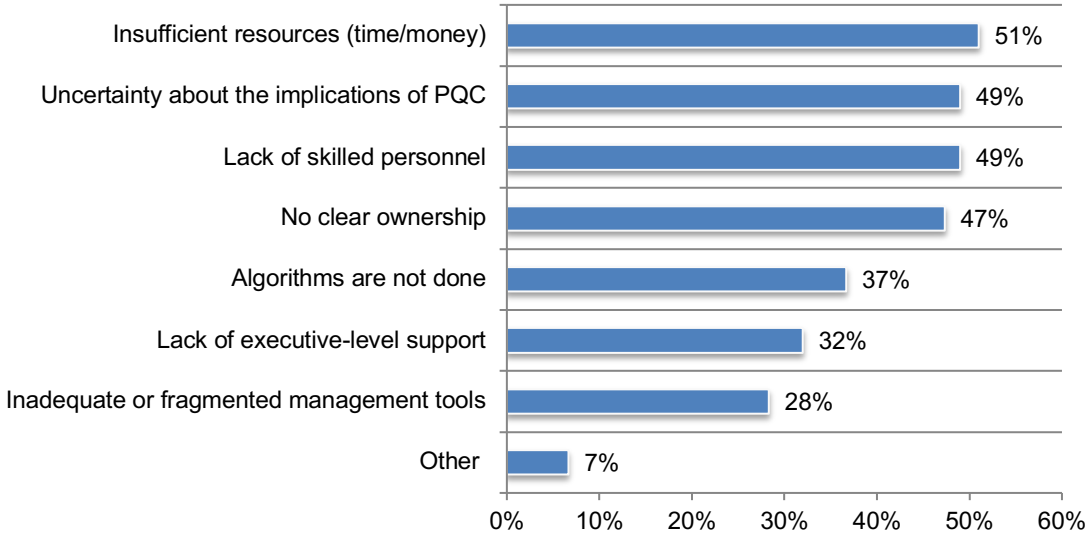
The clock is racing to prepare for PQC. Respondents were asked when their organizations need to be ready for PQC. As shown in Figure 4, 41 percent say they have less than 5 years. Only 21 percent of respondents believe they have from 8 to more than 10 years to prepare.

Figure 4. When do you believe your organization needs to be prepared for PQC?



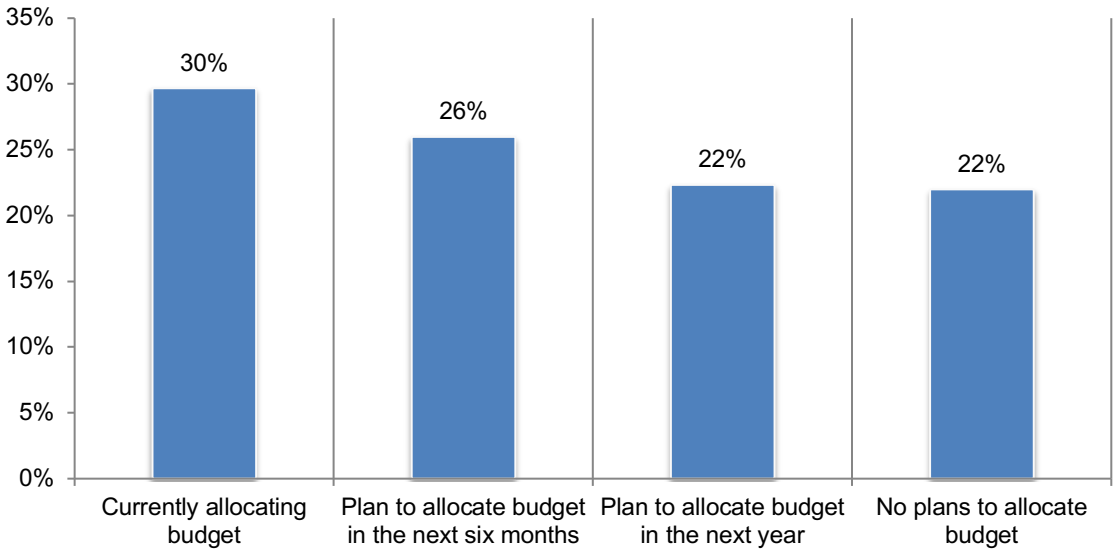
PQC readiness is hard to achieve because of a lack of time, money, skilled personnel and no clear ownership. According to Figure 5, insufficient allocation of resources is affecting the ability to prepare for a safe post quantum computing future (51 percent of respondents) followed by uncertainty about the implications of PQC (49 percent of respondents). Forty-seven percent of respondents say there is no clear ownership of what needs to be done and how to achieve PQC readiness.

Figure 5. What are the main challenges to preparing for PQC?
Three responses permitted



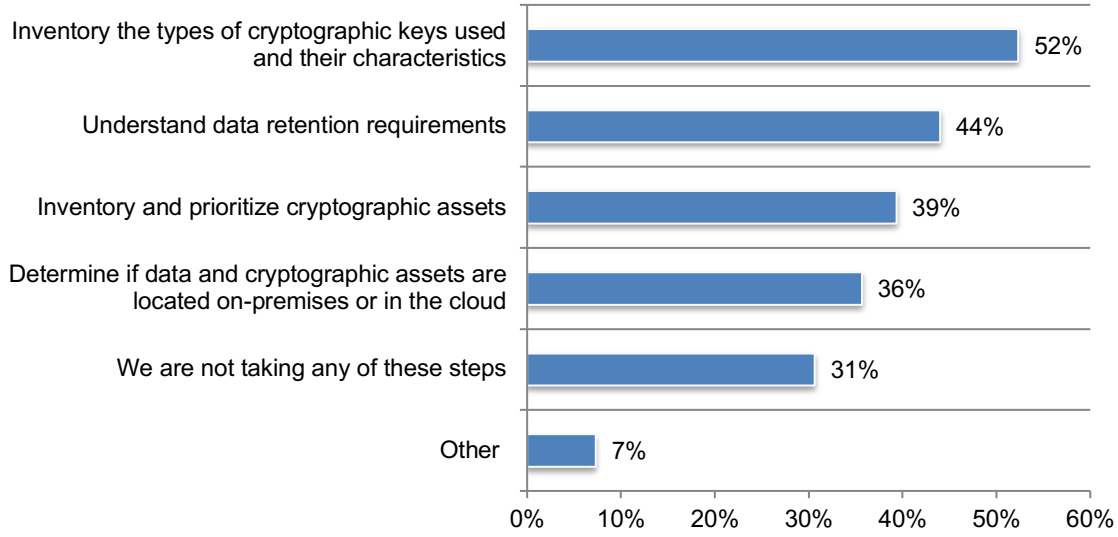
As discussed above, the lack of money hinders PQC readiness. As shown in Figure 6, only 30 percent of respondents say their organizations are allocating *any* budget to prepare for post quantum computing and 22 percent of respondents say their organizations have no plans to provide funding.

Figure 6. Is your organization allocating *any* budget to prepare for post quantum computing?



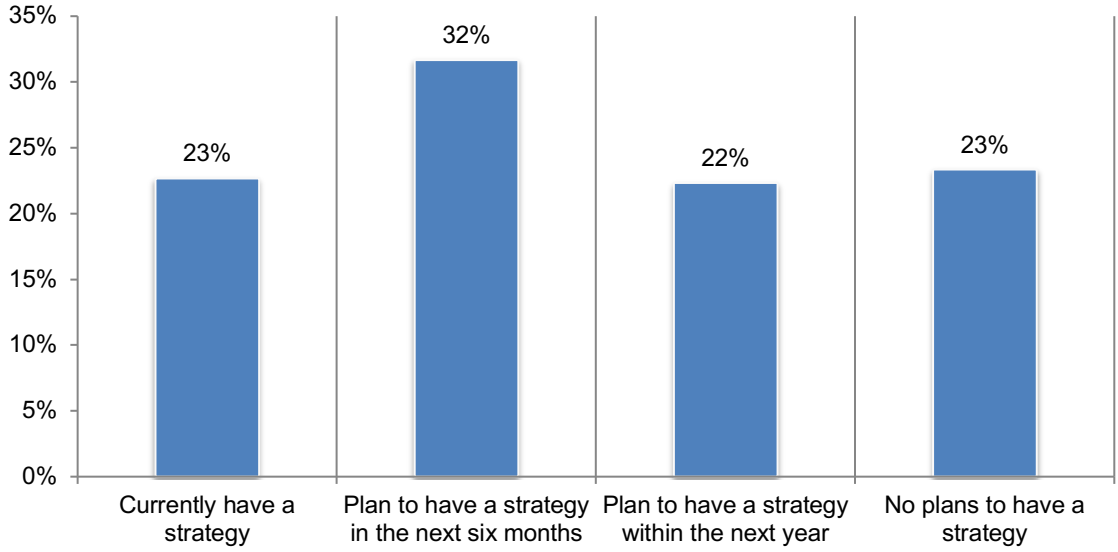
Many organizations are in the dark about the characteristics and locations of their cryptographic keys. Only slightly more than half of respondents (52 percent) say their organizations are taking an inventory of the types of cryptographic keys and their characteristics. This is followed by 44 percent of respondents say they are taking steps to understand data retention requirements. Only 39 percent of respondents are determining if data and cryptographic assets are located on-premises or in the cloud, as shown in Figure 7.

Figure 7. What steps is your organization taking to prepare for post quantum cryptography?
More than one response permitted



To be able to achieve PQC readiness in time organizations should have a strategy and timeline in place. However, as shown in Figure 8, only 23 percent of respondents say they have a strategy. Instead, 54 percent of respondents say they won't have a strategy for another six months (32 percent) or until next year (22 percent). Twenty-three percent of respondents say their organizations are flying blind with no plans to have a strategy.

Figure 8. Does your organization have a strategy for addressing the security implications of quantum computing?

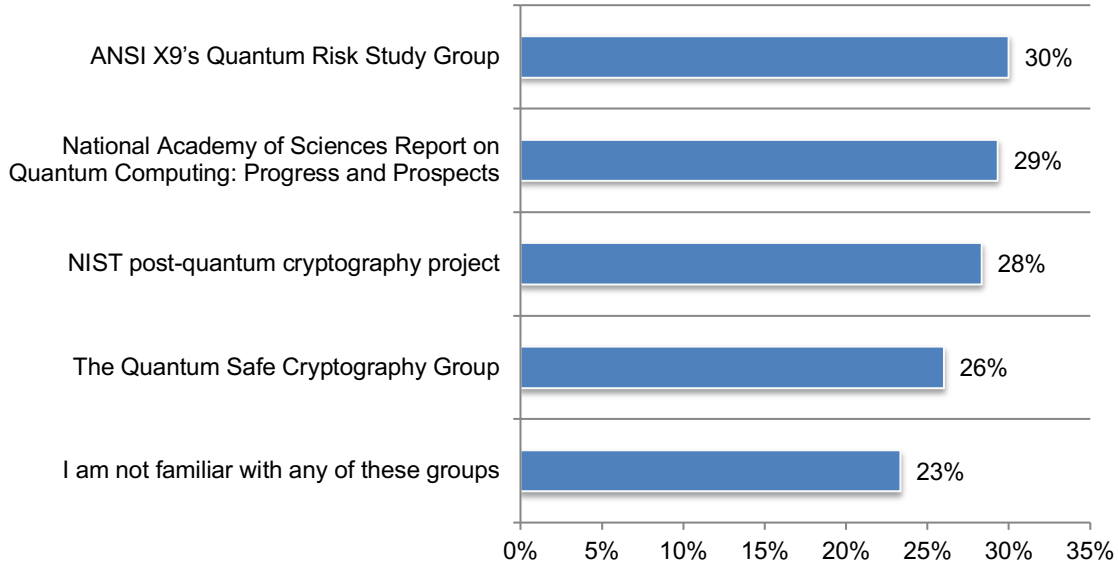


Resources are available to help organizations prepare for a safe post quantum computing future. Sixty percent of respondents are very knowledgeable or knowledgeable about the efforts being made by industry standards groups to prepare for the post-quantum future.

Figure 9 lists the industry standards groups. Respondents are most familiar with ANSI X9's Quantum risk Study Group. This Study Group was established in 2018 to review the state of quantum computing, determine the risks a cryptographically relevant quantum computer would pose to the financial industry and to try to determine a time-period for when it is most likely that such a quantum computer will exist.

Twenty-nine percent of respondents are knowledgeable about the efforts made by The National Academy of Sciences which issued a report "Quantum Computing: Progress and Prospects" and 28 percent of respondents are familiar with the NIST post-quantum cryptography project.

Figure 9. How knowledgeable is your organization about industry standards groups efforts to prepare for the post-quantum future?
More than one response permitted



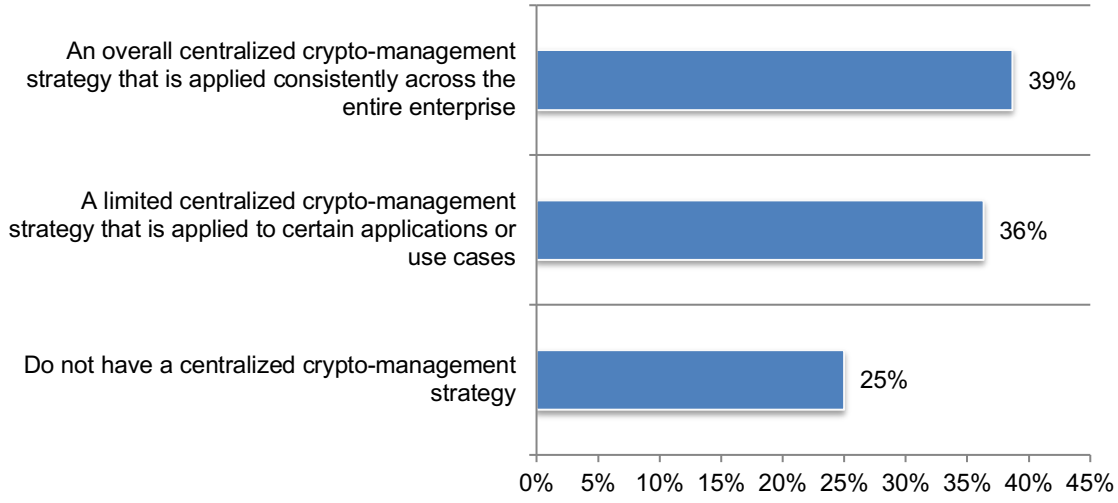
Challenges in cryptographic management

As defined in this research, cryptography is the art of keeping information secure by transforming it into a form that unintended recipients cannot understand. Cryptographic algorithms are used to digitally encode messages and data to ensure confidentiality, integrity, nonrepudiation and authentication in communications and transactions.

Very few organizations have a centralized crypto-management strategy applied consistently across the enterprise. Similar to many organizations not having a strategy for post quantum computing, 61 percent of respondents say their organizations have a limited crypto-management strategy applied to certain applications or use cases (36 percent) or they do not have a centralized strategy (25 percent), according to Figure 10.

It is recommended that such strategies should include inventorying cryptographic keys, understanding their characteristics, remediating weak crypto, adhering to best practices and providing ongoing monitoring to enforce policies that bring cryptography under controls and into compliance.

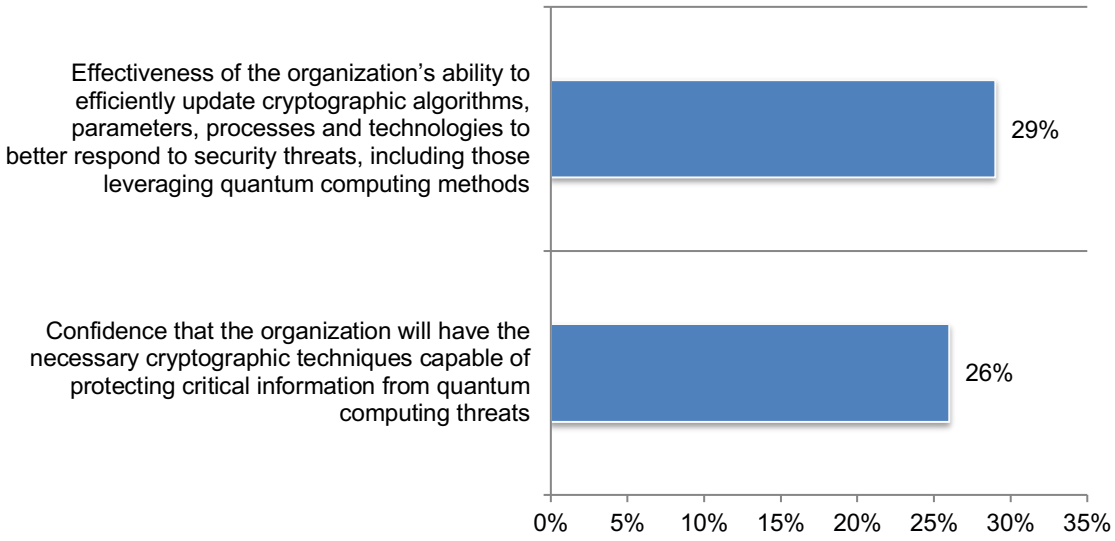
Figure 10. Does your organization have a centralized enterprise-wide strategy for managing cryptography?



Without an enterprise-wide cryptographic management strategy, few organizations are effective in updating cryptographic algorithms in a timely manner. Respondents were asked to rate their organizations' effectiveness in updating cryptographic algorithms, parameters, processes and technologies on a scale from 1 = not effective to 10= very effective. They were also asked to rate their confidence in having the necessary cryptographic techniques in place to protect critical information from quantum computing threats on a scale from 1 = not confident to 10 = very confident. Figure 11 shows the very effective and very confident respondents (7+ on the 10-point scale).

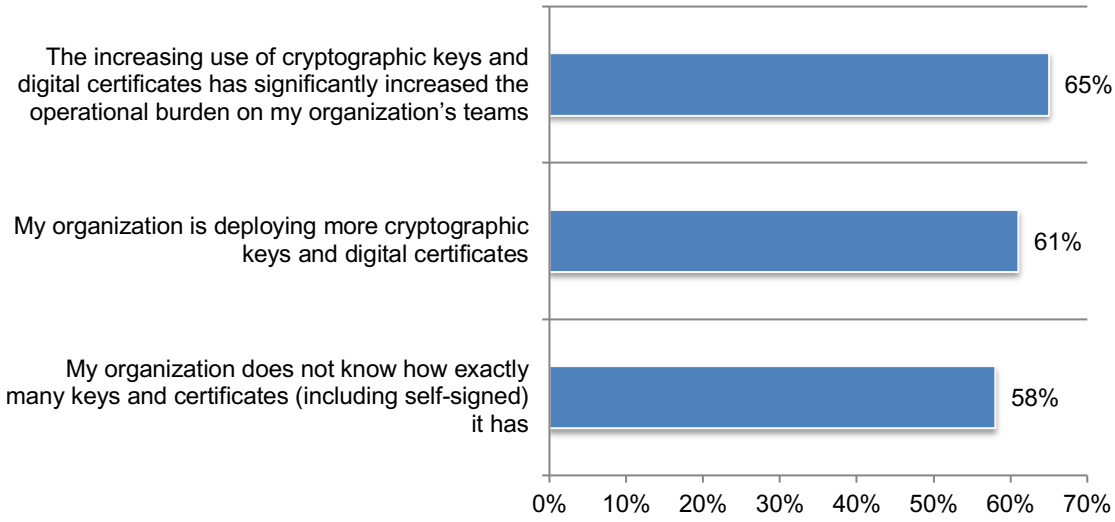
As shown, only 29 percent of respondents are very effective in the timely updating of their cryptographic algorithms, parameter, processes and technologies. Only 26 percent are confident that the organization will have the necessary cryptographic techniques capable of protecting critical information from quantum computing threats.

Figure 11. Effectiveness in updating cryptographic algorithms, parameters, processes and technologies and confidence in having the necessary cryptographic techniques to protect critical information from quantum computing threats
On a scale from 1 = not effective/no confidence to 10 = very effective/confident, 7+ responses presented



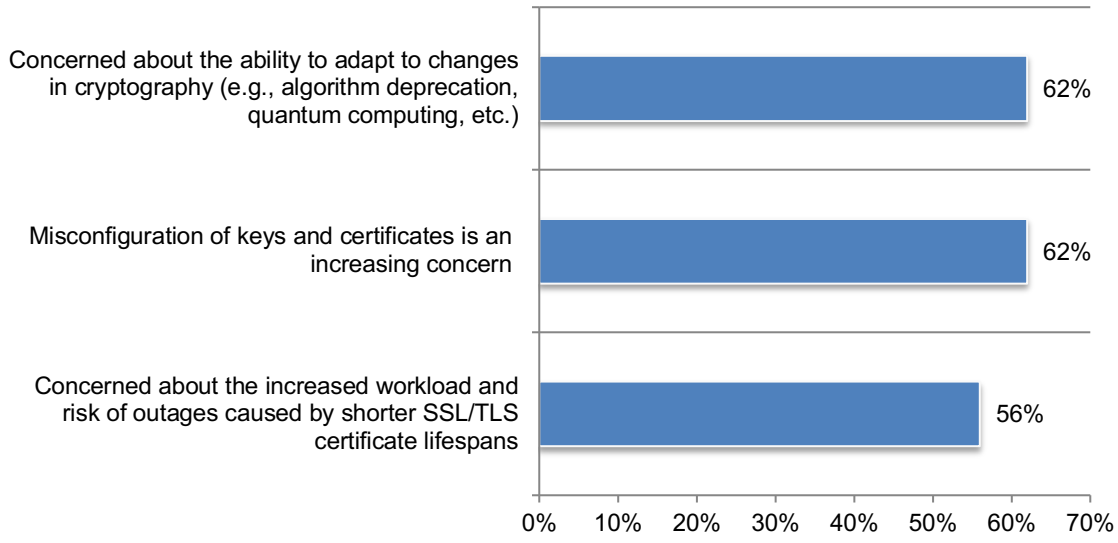
While an accurate inventory of cryptographic keys is an important part of a cryptography management strategy, organizations are overwhelmed keeping up with their increasing use. According to Figure 12, 61 percent of respondents say their organizations are deploying more cryptographic keys and digital certificates. As a result, 65 percent of respondents say this is increasing the operational burden on their teams and 58 percent of respondents say their organizations do not know the number of keys and certificates.

Figure 12. The deployment of more cryptographic keys and digital certificates is a burden and makes it difficult to know how many keys and certificates organizations have
Strongly agree and Agree responses combined



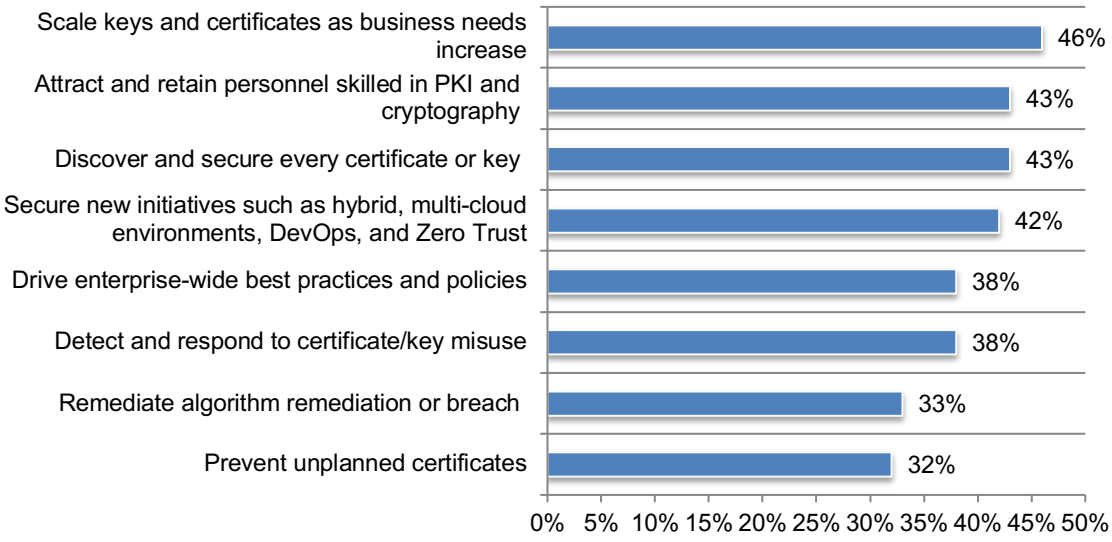
The misconfiguration of keys and certificates and the ability to adapt to cryptography changes prevents a cryptographic management program from being effective. There are significant challenges to a successful cryptographic management program. As shown in Figure 13, most respondents are concerned about the ability to adapt to changes in cryptography (62 percent), the misconfiguration of keys and certificates (62 percent) and the increased workload and risk of outages caused by shorter SSL/TLS certificate lifespans.

Figure 13. Organizations are concerned about shorter SSL/TLS certificate lifespans, misconfiguration of keys and certificates and the ability to adapt to changes in cryptography
Strongly agree and Agree responses combined



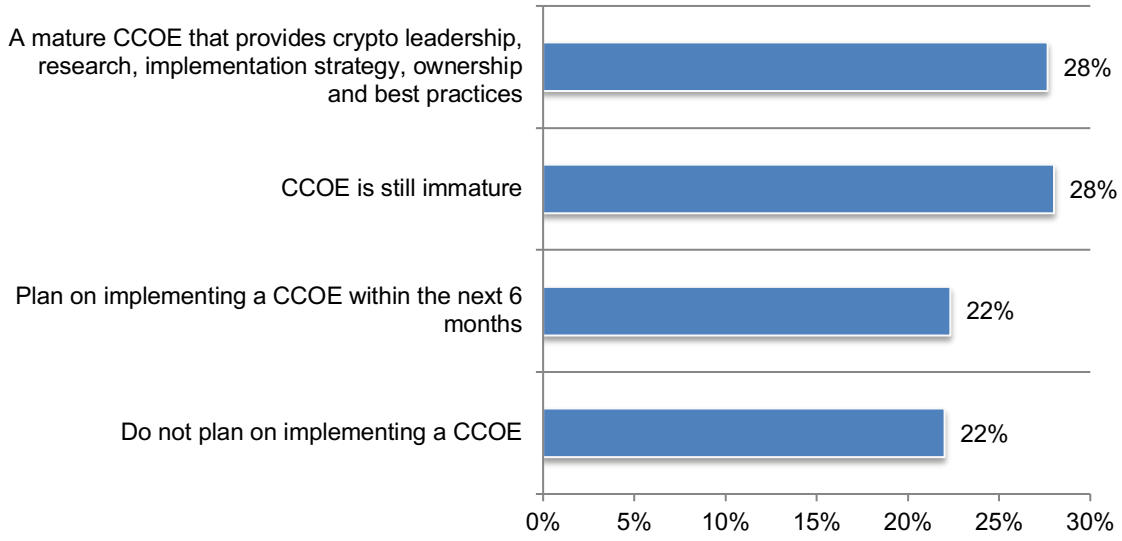
Critical information is at risk because of the inability to effectively deploy cryptographic solutions and methods. Respondents were asked to rate their ability to secure information assets and the IT infrastructure on a scale from 1 = low ability to 10 = high ability. Figure 14 presents the high ability responses (7+ on the 10-point scale). As shown, less than half of respondents rate their abilities as high. Only 46 percent of respondents have a high ability to scale keys and certificates as business needs increase and only 43 percent of respondents say their organizations have a high ability to attract and retain personnel skilled in PKI and cryptography or to discover and secure every certificate or key.

Figure 14. Ability to effectively deploy cryptographic solutions and methods to secure information assets and the IT infrastructure
On a scale from 1 = low ability to 10 = high ability, 7+ responses presented



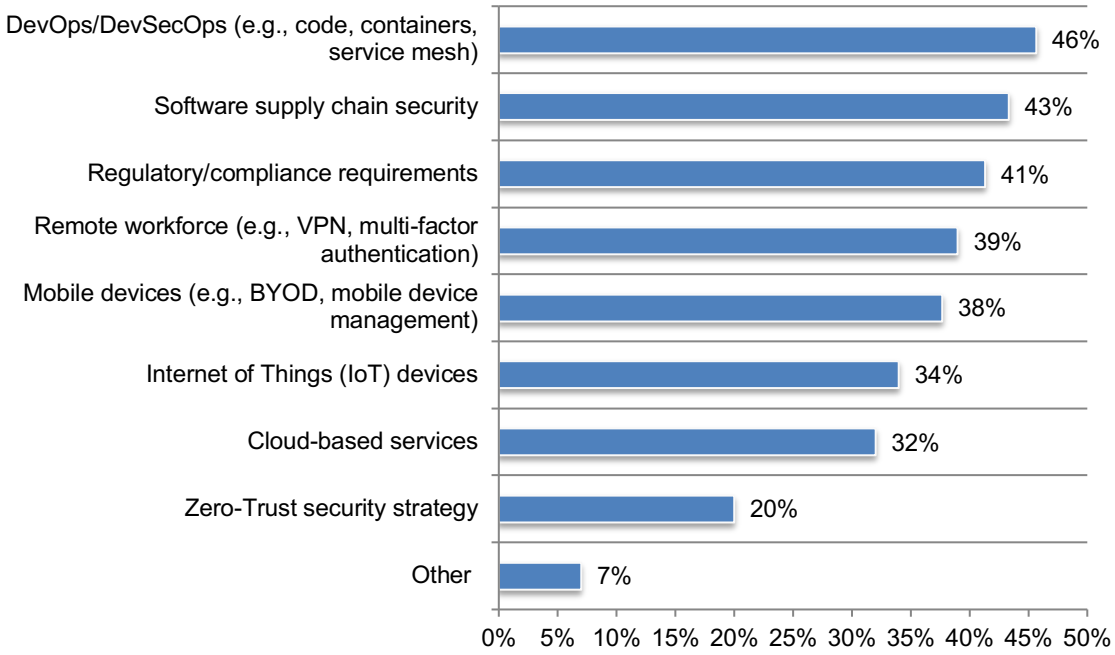
Crypto Centers of Excellence (CCOE) can support organizations' efforts to achieve a safe quantum computing future. A CCOE can help improve operational cryptographic processes and increase confidence in an organization's trust environment. CCOEs require advanced technologies and expertise in cryptography that is used to maintain secure operations and comply with applicable regulations. However, as shown, only 28 percent of respondents say their organizations have a mature CCOE and another 28 percent say they have a CCOE, but it is immature, as shown in Figure 15.

Figure 15. Has your organization implemented a Crypto Center of Excellence (CCOE)



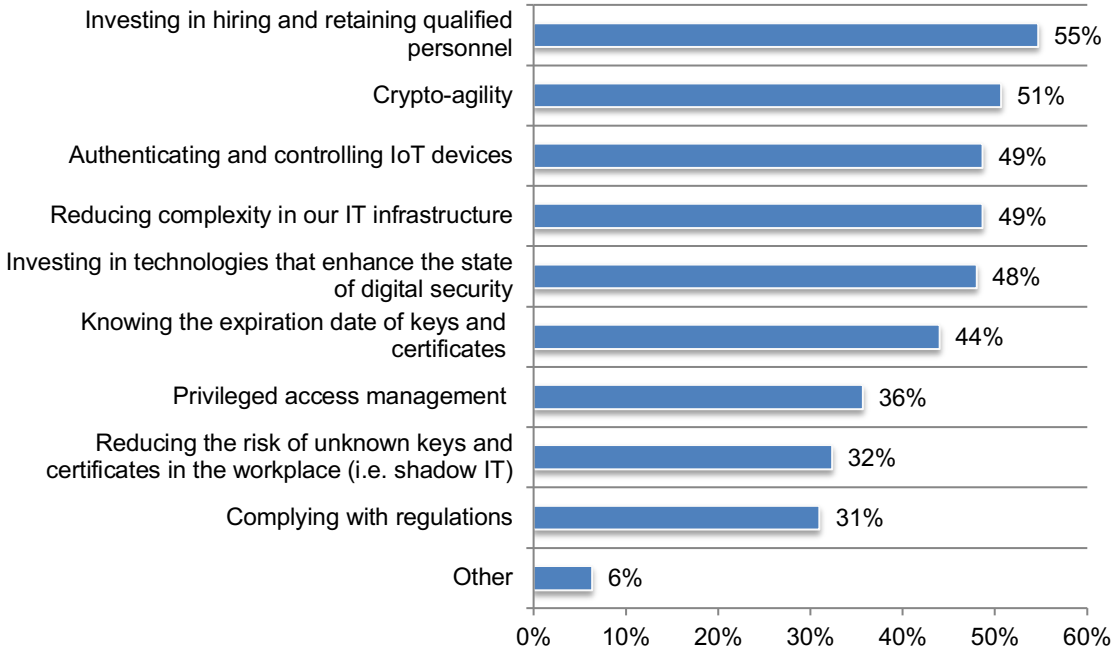
DevOps/DevSecOps is the primary driver for deploying PKI, keys, certificates and other secrets (46 percent of respondents). As shown in Figure 16, other primary drivers are the security of the software supply chain (43 percent of respondents) and regulatory/compliance requirements (41 percent of respondents).

Figure 16. What are the top three trends driving the deployment of PKI, keys, certificates and other secrets?
Top three responses presented



The need to have qualified personnel is a priority for digital security. As shown in Figure 17, investing in hiring and retaining qualified personnel is the most important strategic priority for digital security according to 55 percent of respondents. Fifty-one percent say crypto agility is a strategic priority. Crypto agility refers to the ability to efficiently update cryptographic algorithms, parameters, processes and technologies to better respond to new protocols, standards and security threats, including those leveraging quantum computing methods.

Figure 17. What are the most important strategic priorities for digital security?
More than one response permitted

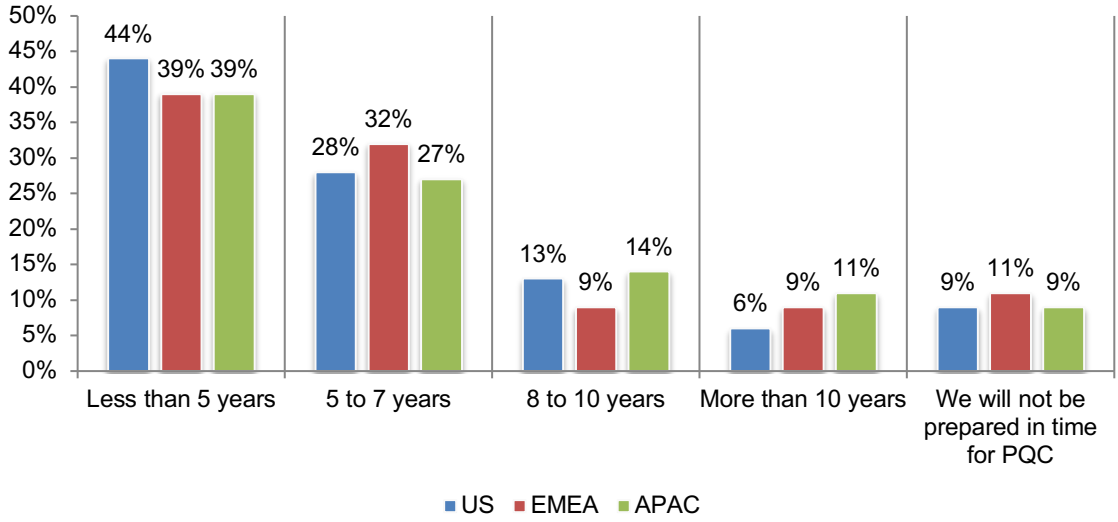


Differences among the United States, EMEA and Asia-Pac

In this section, we present a breakout of the global findings to determine if there any significant differences.

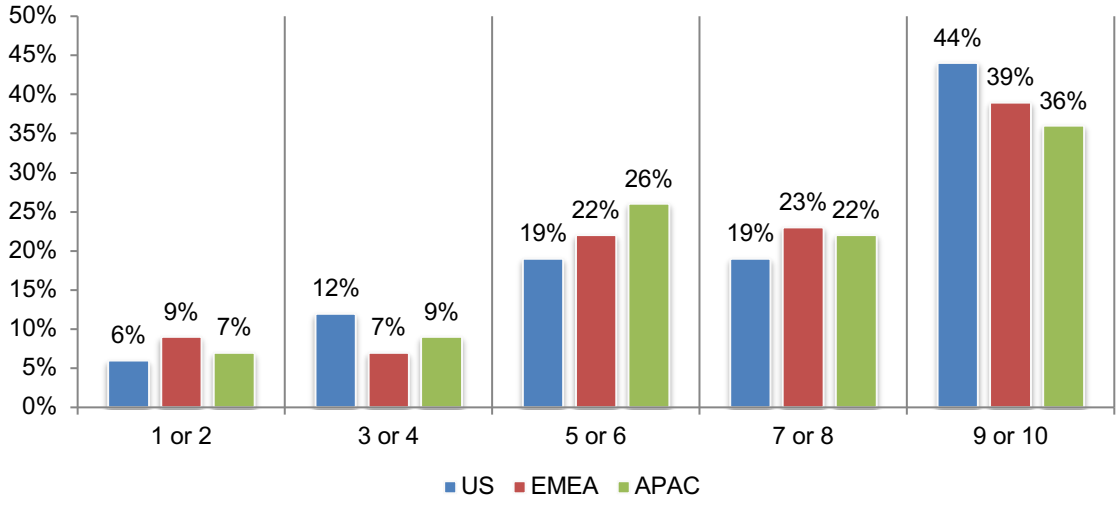
Respondents in the US are more likely to believe there is less time to prepare for PQC. Forty-four percent of US respondents say they need to be ready in less than five years vs. 39 percent of respondents in EMEA and Asia-Pac. Respondents in Asia-Pac also predict it will take 8 to more than 10 years to achieve readiness (25 percent vs.19 percent in the US), as shown in Figure 18.

Figure 18. When do you believe your organization needs to be prepared for PQC?



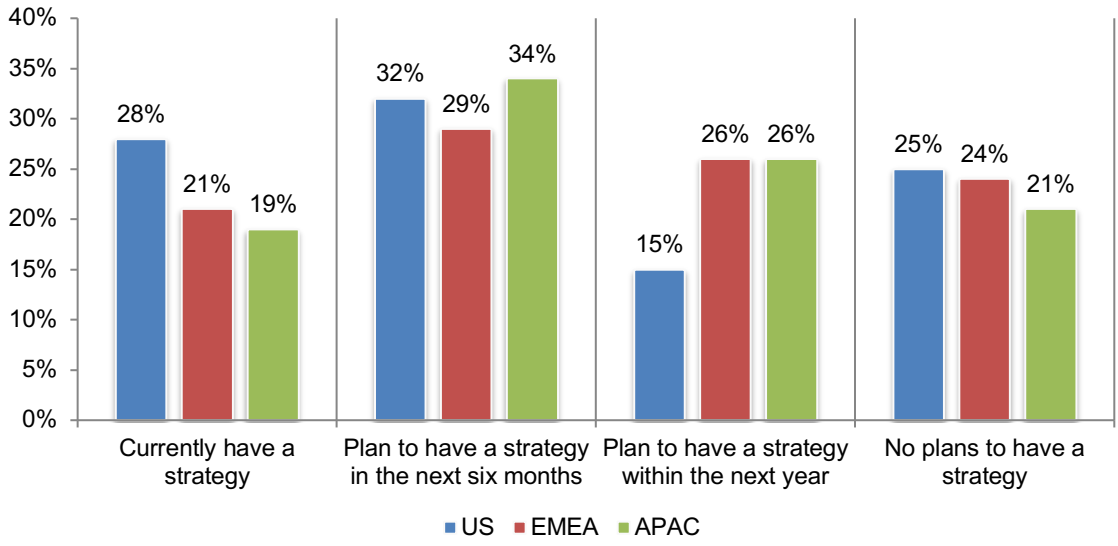
US respondents are also more concerned about the ability to mitigate risks created by PQC. Respondents were asked to rate their concerns about the security implications of PQC on a scale from 1 = not concerned to 10 = very concerned. Figure 19 presents the range of responses. As shown, 63 percent of US respondents are very concerned. In contrast, 58 percent of Asia Pacific respondents are very concerned (7+ responses on the 10-point scale).

Figure 19. How concerned are you that your organization will not be prepared to address the security implications of PQC?



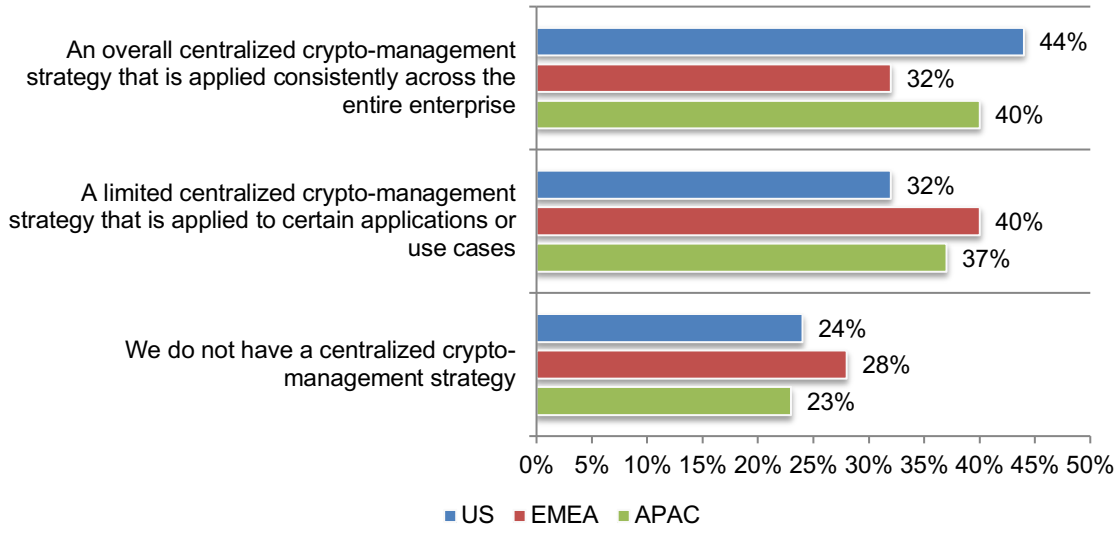
US respondents are more proactive in addressing the security implications of quantum computing by having a strategy currently or in the next six months. According to Figure 20, 60 percent of US respondents currently have a strategy (28 percent) or will have in the next six months (32 percent). Fifty-three percent of Asia-Pac and 50 percent of EMEA respondents say they have such a strategy

Figure 20. Does your organization have a strategy for addressing the security implications of quantum computing?



Organizations in EMEA are less likely to have an overall centralized crypto-management strategy. According to Figure 21, only 32 percent of respondents in EMEA say their organizations have a centralized enterprise-wide strategy for managing cryptography. US respondents are more likely to have such a strategy (44 percent).

Figure 21. Does your organization have a centralized enterprise-wide strategy for managing cryptography?



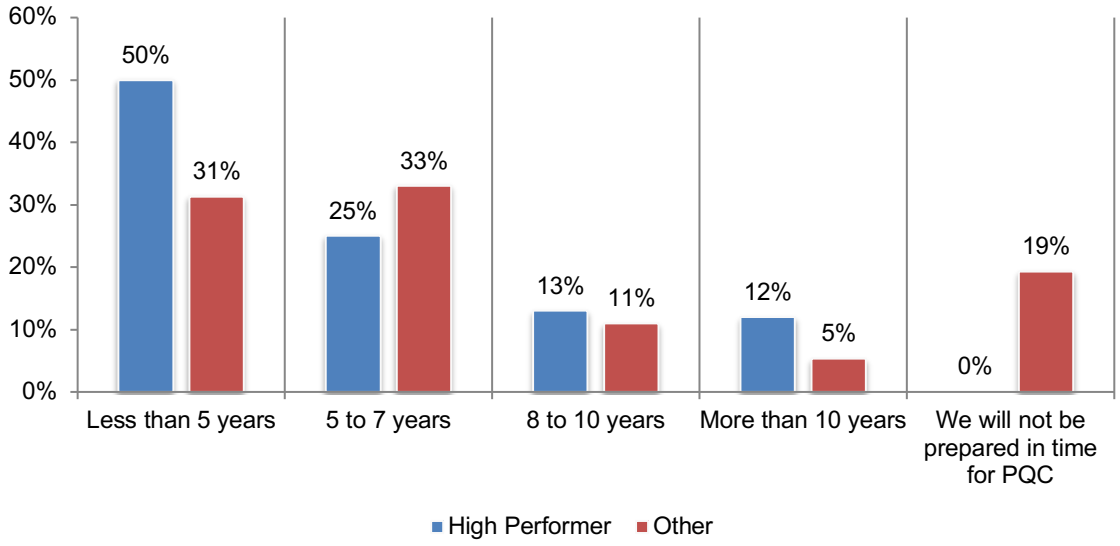
Best practices in achieving PQC readiness: An analysis of high performing organizations

Respondents were asked to rate their organizations' effectiveness in mitigating risks, vulnerabilities and attacks across the enterprise on a scale from 1 = not effective to 10 = highly effective. Fifty percent of respondents self-reported their organizations are effective or highly effective (7+ responses) in creating a strong cybersecurity posture. We refer to these organizations as "high performers".

In this section, we analyze what these organizations are doing differently to achieve a safe post quantum computing future. We refer to the other 50 percent of respondents (1 to 6 responses) as "other" in the figures below.

High performing organizations have more urgency to be ready for PQC. As shown in Figure 22, 50 percent of high performing respondents believe they have less than 5 years to prepare. In contrast, only 25 percent of respondents in the other group of respondents believe they have the same time-period to be prepared. Nineteen percent of respondents say their organizations will not be prepared in time.

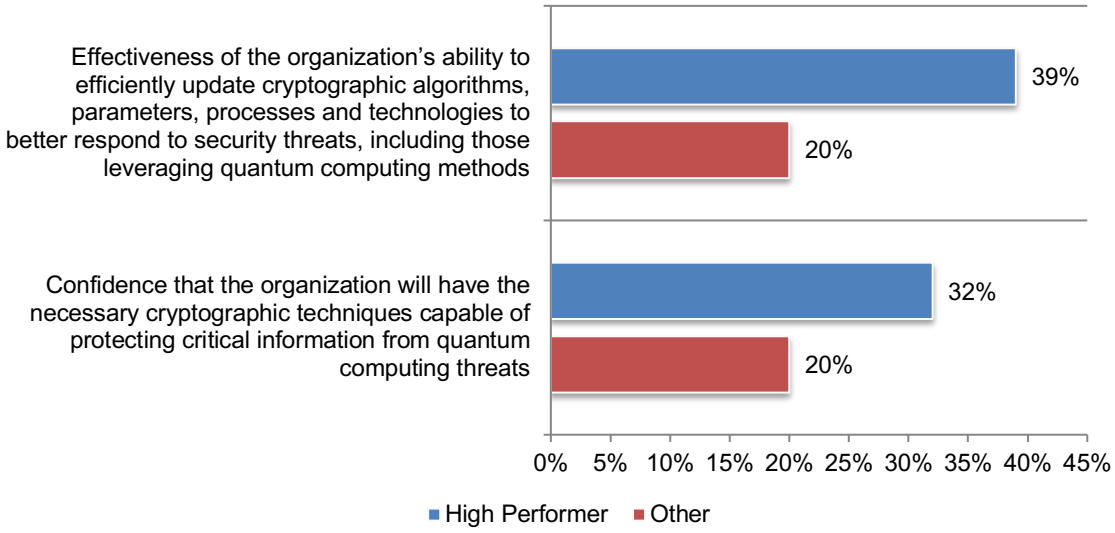
Figure 22. When do you believe your organization needs to be prepared for PQC?



High performing organizations are more positive about their ability to achieve a safe post quantum computing future. Respondents were asked to rate effectiveness and confidence in achieving PQ readiness based on specific criteria shown in Figure 23. Thirty-nine percent of high performers vs. 20 percent of other respondents rate their effectiveness to update efficiently cryptographic algorithms, parameters, processes and technologies to better respond to security threats, including those leveraging quantum computing methods.

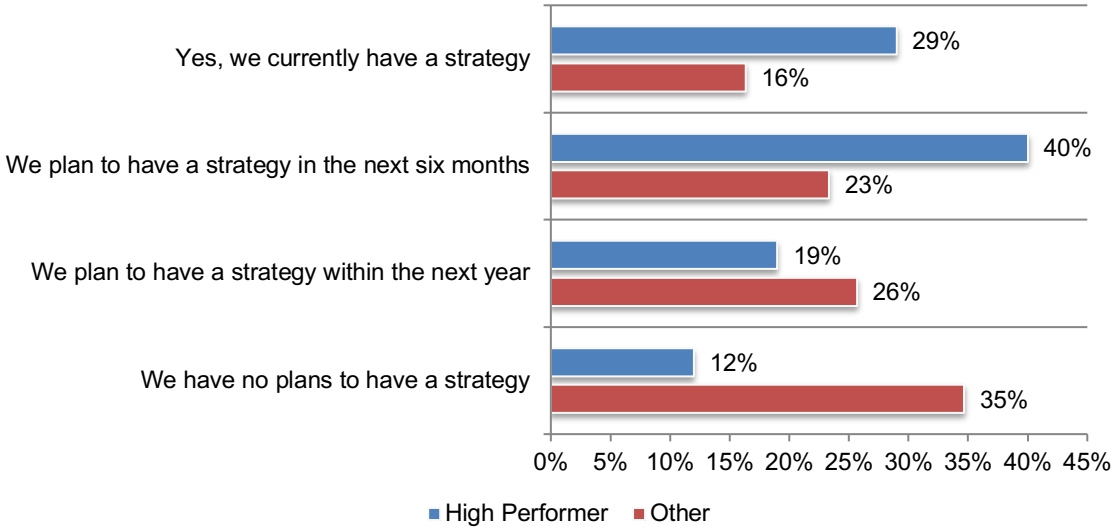
Thirty-two percent of high performing organizations vs. 20 percent of respondents in the other group are very confident that their organizations will have the necessary cryptographic techniques capable of protecting critical information from quantum computing threats.

Figure 23. Effectiveness in updating cryptographic algorithms, parameters, processes and technologies and confidence in having the necessary cryptographic techniques to protect critical information from quantum computing threats
On a scale from 1 = not effective/no confidence to 10 = very effective/confident, 7+ responses presented



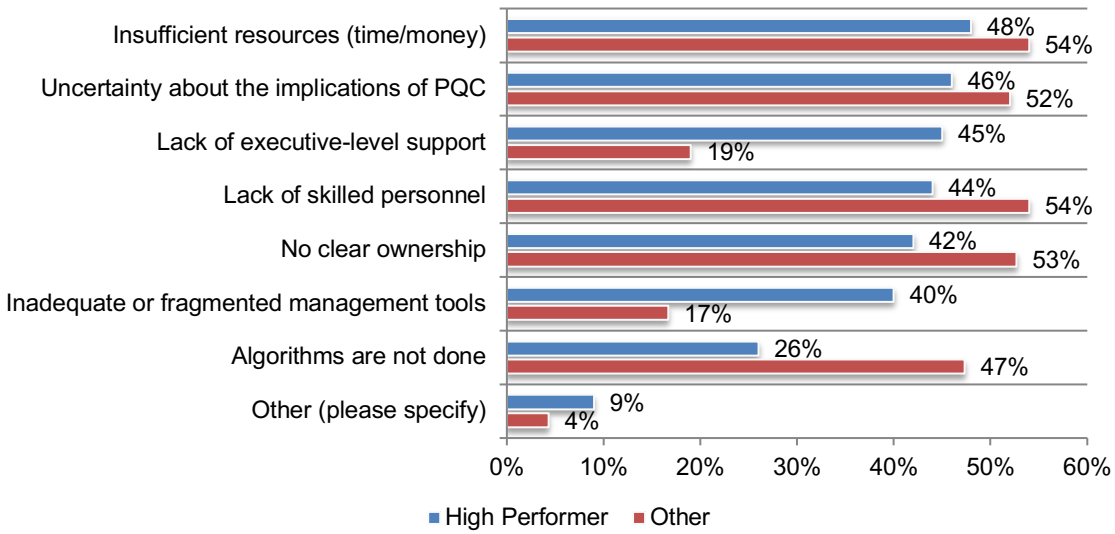
High performers are more likely to address the security implications of quantum computing with a strategy. Sixty-nine percent of respondents say their organizations currently have a strategy (29 percent) or within the next six months (40 percent). In contrast, 39 percent of respondents in organizations that are not high performers have a strategy today (16 percent) or within the next six months (23 percent).

Figure 24. Does your organization have a strategy for addressing the security implications of quantum computing?



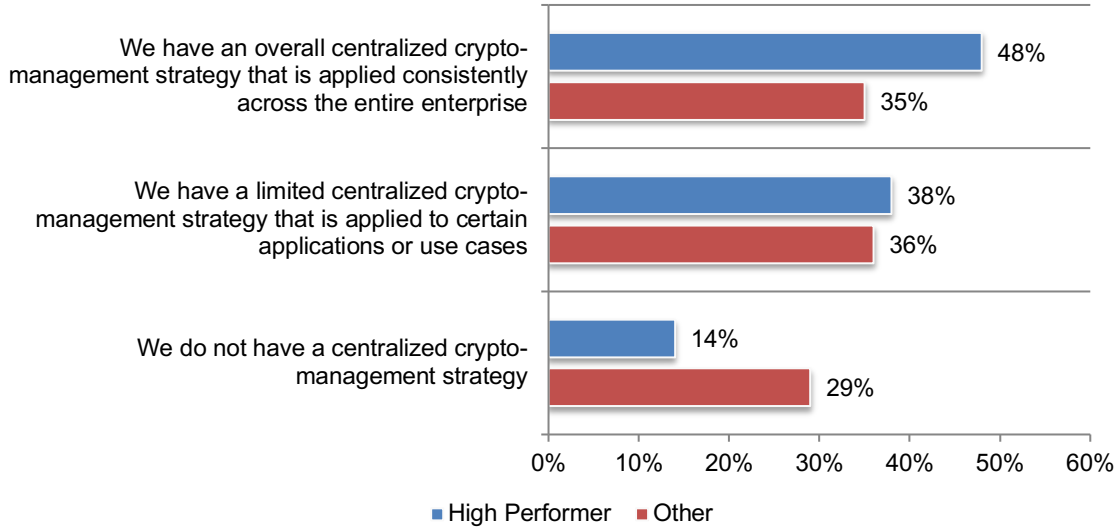
Organizations that are not high performers are most likely to struggle with having sufficient resources, lack of skilled personnel and no clear ownership. As shown in Figure 25, 54 percent of respondent vs 48 percent of high performers say that a main challenge is the lack of resources. A significant difference is that 47 percent of other respondents say that algorithms are not done vs. 26 percent of high performers.

Figure 25. What are the main challenges to preparing or PQC?
Three responses permitted



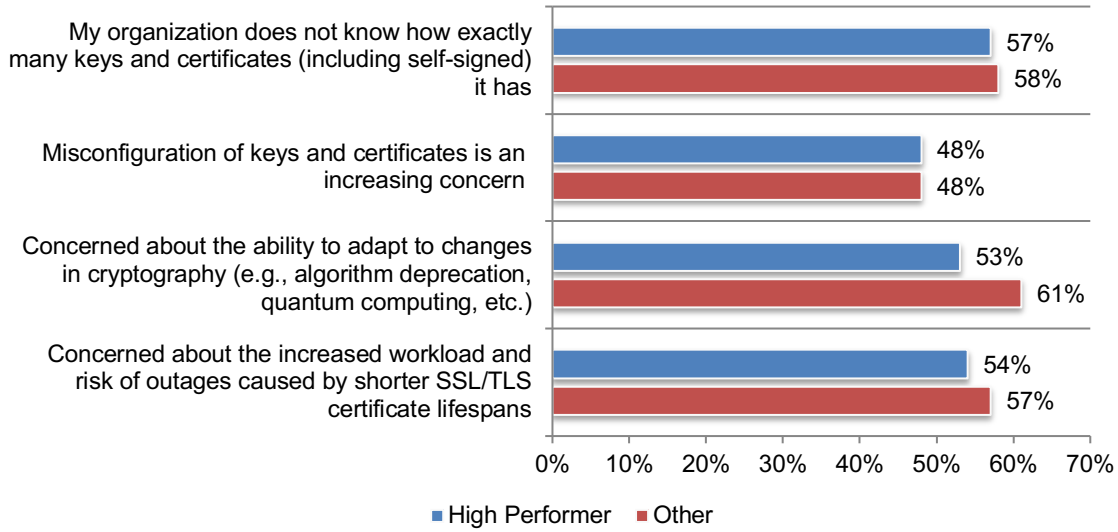
The positive attitude of high performers may be attributed to their organizations having an overall centralized crypto-management strategy applied consistently across the enterprise (48 percent of high performers vs. 35 percent of other respondents.

Figure 26. Does your organization have a centralized enterprise-wide strategy for managing cryptography?



Both groups are aware of the flaws in their cryptography management. As shown in Figure 27, 57 percent of high performers and 58 percent of other respondents say their organizations do not know how exactly many keys and certificates they know. Both 48 percent of respondents say misconfiguration of keys and certificates is an increasing concern.

Figure 27. Perceptions about cryptography management
Strongly agree and Agree responses combined



Conclusion

To be ready for post quantum computing, organizations need to have a strategy that incorporates the following steps.

- A successful strategy depends upon senior leadership's understanding of the threats to data security caused by post quantum computing and ensuring that the necessary resources are allocated to prepare for a safe post quantum computing future. According to the research, organizations are challenged by a lack resources, time and ownership.
- Visibility into the types of cryptography keys used and their characteristics is critical to securing data assets. Maintaining an accurate inventory of cryptographic keys is a challenge because of their increasing use. Only 39 percent of respondents say they are prioritizing cryptographic assets and only 36 percent say they know if cryptographic assets are located on-premises or in the cloud.
- Organizations should establish an overall centralized crypto-management strategy that is applied consistently across the enterprise with accountability and ownership.
- Cryptographic algorithms, parameters, processes and technologies should be updated in a timely manner. Organizations need to have the necessary cryptographic techniques capable of protecting critical information from quantum threats.
- Organizations need to improve their ability to adapt to cryptography changes. These changes include algorithm deprecation and quantum computing. A hindrance is the lack of qualified personnel to respond to new protocols, standards and security threats, including those leveraging quantum computing methods.

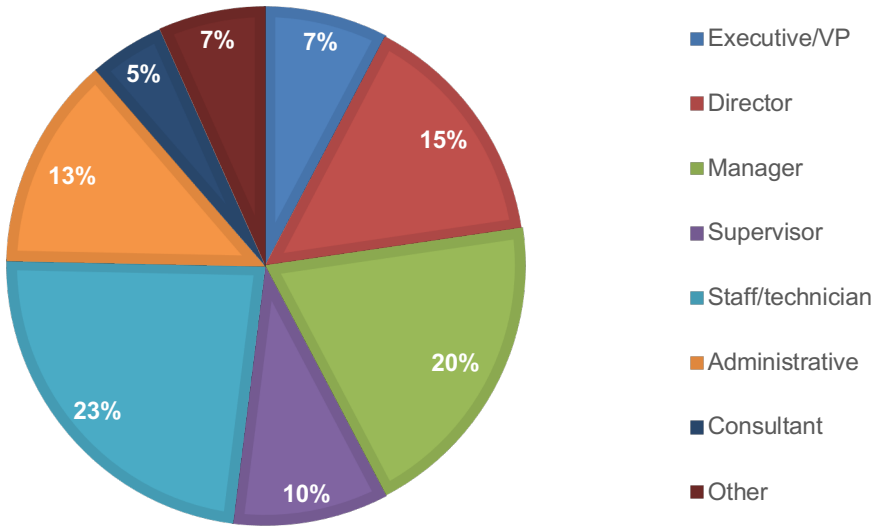
Part 3. Methodology

A sampling frame of 42,161 IT and IT security practitioners in the United States, EMEA and Asia-Pacific who are knowledgeable about their organizations' approach to post quantum cryptography were selected as participants to this survey. Table 1 shows 1,566 total returns. Reliability checks required the removal of 140 surveys. Our final sample consisted of 1,426 surveys or a 3.4 percent response rate.

Table 1. Sample response	US	EMEA	APAC	Global
Sampling frame	16,890	12,706	12,565	42,161
Total returns	663	471	432	1,566
Rejected or screened surveys	58	43	39	140
Final sample	605	428	393	1,426
Response rate	3.6%	3.4%	3.1%	3.4%

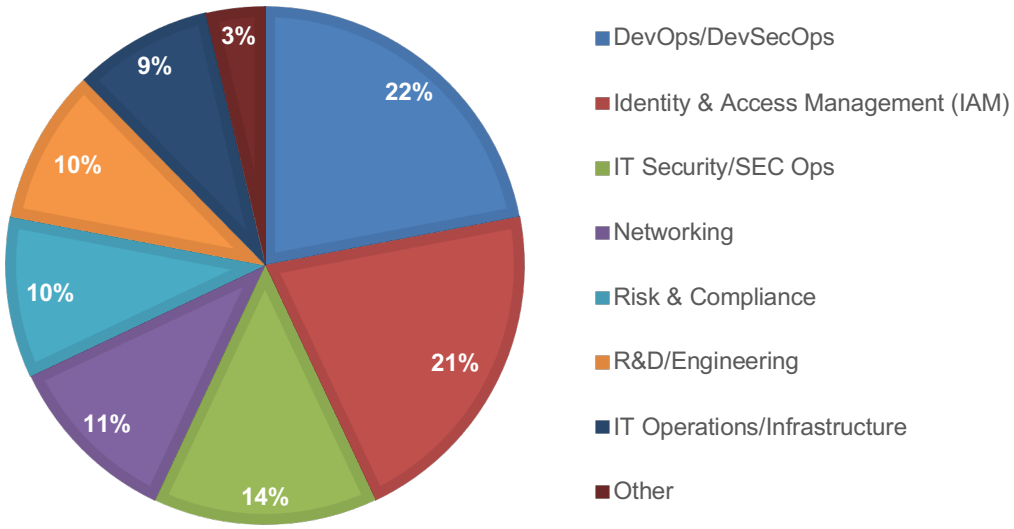
Pie chart 1 reports the respondent's organizational level within participating organizations. By design, more than half (52 percent) of respondents are at or above the supervisory levels.

Pie chart 1. Current position within the organization



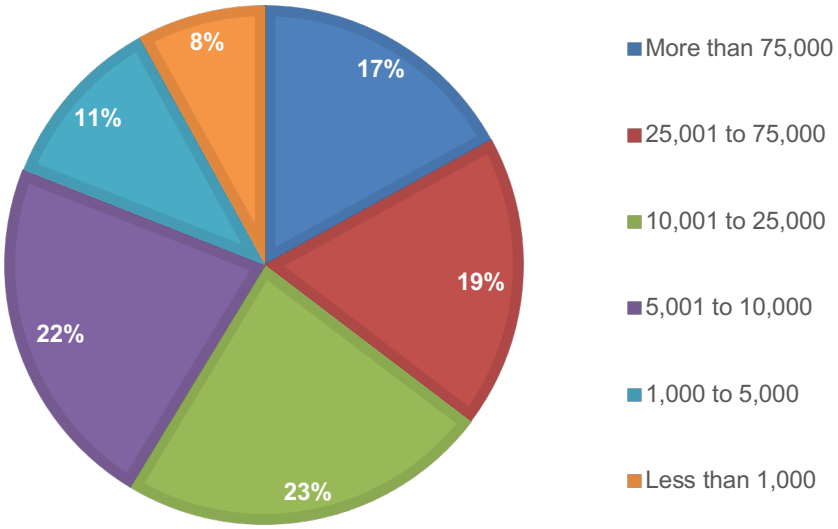
Pie chart 2 identifies the department or team the respondents are located in. Twenty-two percent of respondents are in DevOps/DevSecOps, this is followed by identity and access management (21 percent of respondents), IT security/SEC ops (14 percent of respondents), networking (11 percent of respondents), risk and compliance (10 percent of respondents) and R&D/engineering (10 percent of respondents).

Pie chart 2. What best describes your department or team?



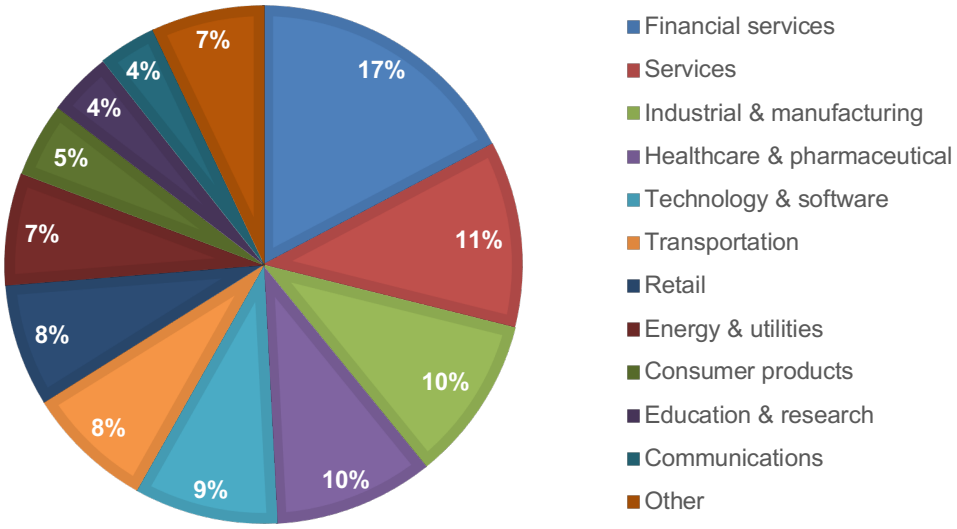
As shown in Pie chart 3, 59 percent of respondents are from organizations with a global headcount of more than 10,000 employees.

Pie chart 3. Global full-time headcount



Pie chart 4 reports the industry classification of respondents' organizations. This chart identifies financial services (17 percent) as the largest industry focus, which includes banking, investment management, insurance, brokerage, payments and credit cards. This is followed by services (11 percent of respondents), industrial and manufacturing (10 percent of respondents), healthcare and pharmaceuticals (10 percent of respondents), technology and software (9 percent of respondents), transportation and retail (each at 8 percent of respondents).

Pie chart 4. Primary industry classification



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 knowledgeable about their organizations' approach to post quantum cryptography. 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.

Part 5. Appendix with the consolidated global findings

The following tables provide the frequency or percentage frequency of responses to all survey questions contained in this study. All survey responses were captured in August 2023.

Survey response	Consolidated
Total sampling frame	42,161
Total survey returns	1,566
Survey rejects	140
Final sample	1,426
Sample weights	3.4%

S1. How knowledgeable are you about post quantum cryptography?	Consolidated
Very knowledgeable	40%
Knowledgeable	40%
Somewhat knowledgeable	20%
No knowledge (stop)	0%
Total	100%

S2. What best defines your familiarity with your organization's approach to post quantum cryptography?	Consolidated
Very familiar	41%
Familiar	30%
Somewhat familiar	29%
Not familiar (stop)	0%
Total	100%

S3. What best describes your role in the organization?	Consolidated
CISO	14%
CIO	13%
VP IT security	20%
Director/manager IT security	27%
Security architect	10%
PKI engineer	9%
Product manager	7%
None of the above (stop)	0%
Total	100%

Part 1. Background on security posture

Q1. How would you describe your organization's IT security posture in terms of its effectiveness at mitigating risks, vulnerabilities and attacks across the enterprise on a scale from 1 = not effective to 10 = very effective?	Consolidated
1 or 2	11%
3 or 4	17%
5 or 6	22%
7 or 8	32%
9 or 10	18%
Total	100%

Q2. Has your organization experienced one or more cyberattacks in the past 12 months?	Consolidated
Yes	46%
No	48%
Unsure	7%
Total	100%

Q3. If yes, what best describes the type of attacks experienced by your organization? Please select all that apply.	Consolidated
Advanced malware / zero-day attacks	45%
APIs	44%
Phishing / social engineering	40%
Denial of service	33%
Account takeover	42%
Credential theft	47%
Ransomware	47%
Web application attack	23%
Web-based attack	31%
Compromised / stolen devices	27%
Malicious insider	36%
Advanced malware	27%
Other (please specify)	8%
Total	451%

Q4. Please rate the following statements using the strongly agree to strongly disagree scale provided below each item.	
Q4a. In the past 12 months, cyberattacks experienced by my organization are becoming more targeted.	Consolidated
Strongly agree	24%
Agree	32%
Unsure	19%
Disagree	15%
Strongly Disagree	9%
Total	100%

Q4b. In the past 12 months, cyberattacks experienced by my organization are becoming more sophisticated.	Consolidated
Strongly agree	31%
Agree	29%
Unsure	20%
Disagree	14%
Strongly Disagree	6%
Total	100%

Q4c. In the past 12 months, cyberattacks experienced by my organization are becoming more severe in terms of an increase in mean time to investigate (MTTI) and mean time to contain (MTTC).	Consolidated
Strongly agree	26%
Agree	28%
Unsure	23%
Disagree	14%
Strongly Disagree	8%
Total	100%

Part 2. The state of post quantum computing (PQC) readiness

Q5. When do you believe your organization needs to be prepared for PQC?	Consolidated
Less than 5 years	41%
5 to 7 years	29%
8 to 10 years	12%
More than 10 years	9%
We will not be prepared in time for PQC	10%
Total	100%

Q6. How concerned are you that your organization will not be prepared to address the security implications of PQC on a scale from 1 = not concerned to 10 = very concerned.	Consolidated
1 or 2	7%
3 or 4	9%
5 or 6	22%
7 or 8	21%
9 or 10	40%
Total	100%

Q7. How concerned are you that advanced attackers could conduct “harvest now, decrypt later” attacks, in which they collect and store encrypted data with the goal of decrypting the data in the future on a scale of 1 = not concerned to 10 = very concerned.	Consolidated
1 or 2	2%
3 or 4	6%
5 or 6	18%
7 or 8	28%
9 or 10	46%
Total	100%

Q8. How effective is your organization’s ability to efficiently update cryptographic algorithms, parameters, processes and technologies to better respond to security threats, including those leveraging quantum computing methods on a scale from not effective to 1 = not effective to 10 = very effective.	Consolidated
1 or 2	16%
3 or 4	33%
5 or 6	22%
7 or 8	14%
9 or 10	15%
Total	100%

Q9. How confident are you that your organization will have the necessary cryptographic techniques capable of protecting critical information from quantum computing threats on a scale from not confident = 1 to 10 = very confident.	Consolidated
1 or 2	21%
3 or 4	29%
5 or 6	24%
7 or 8	13%
9 or 10	13%
Total	100%

Q10. Does your organization have a strategy for addressing the security implications of quantum computing?	Consolidated
Yes, we currently have a strategy	23%
We plan to have a strategy in the next six months	32%
We plan to have a strategy within the next year	22%
We have no plans to have a strategy	23%
Total	100%

Q11. How aware is your organization's leadership about the security implications of quantum computing?	Consolidated
Very aware	18%
Aware	33%
Somewhat aware	26%
Not aware	23%
Total	100%

Q12. How knowledgeable is your organization about the efforts being made by industry standards groups to prepare for the post-quantum future?	Consolidated
Very knowledgeable	26%
Knowledgeable	34%
Somewhat knowledgeable	31%
Not knowledgeable (please skip to Q14)	9%
Total	100%

Q13. If knowledgeable, are you familiar with the following organizations? Please select all that apply.	Consolidated
NIST post-quantum cryptography project	28%
National Academy of Sciences Report on Quantum Computing: Progress and Prospects	29%
ANSI X9's Quantum Risk Study Group	30%
The Quantum Safe Cryptography Group	26%
I am not familiar with any of these groups	23%
Total	137%

Q14. What are the main challenges to preparing for PQC? Please select the top three choices.	Consolidated
No clear ownership	47%
Algorithms are not done	37%
Lack of skilled personnel	49%
Insufficient resources (time/money)	51%
Inadequate or fragmented management tools	28%
Uncertainty about the implications of PQC	49%
Lack of executive-level support	32%
Other (please specify)	7%
Total	300%

Q15. What steps is your organization taking to prepare for post-quantum cryptography? Please check all that apply.	Consolidated
Inventory and prioritize cryptographic assets	39%
Understand data retention requirements	44%
Determine if data and cryptographic assets are located on-premises or in the cloud	36%
Inventory the types of cryptographic keys used and their characteristics	52%
Other (please specify)	7%
We are not taking any of these steps	31%
Total	209%

Q16. Has your organization implemented a Crypto Center of Excellence (CCOE)?	Consolidated
Yes, we have a mature CCOE that provides crypto leadership, research, implementation strategy, ownership and best practices	28%
Yes, but our CCOE is still immature	28%
No, but we plan on implementing a CCOE within the next 6 months	22%
No, we do not plan on implementing a CCOE	22%
Total	100%

Part 3. Cryptographic readiness capabilities

Q17. Does your organization have a centralized enterprise-wide strategy for managing cryptography?	Consolidated
We have an overall centralized crypto-management strategy that is applied consistently across the entire enterprise	39%
We have a limited centralized crypto-management strategy that is applied to certain applications or use cases	36%
We do not have a centralized crypto-management strategy	25%
Total	100%

Q18. In your opinion, what are the most important trends that are driving the deployment of PKI, keys, certificates, and other secrets? Please select three choices only.	Consolidated
Regulatory / compliance requirements	41%
Mobile devices (e.g., BYOD, mobile device management)	38%
Remote workforce (e.g., VPN, multi-factor authentication)	39%
Internet of Things (IoT) devices	34%
Software supply chain security	43%
DevOps / DevSecOps (e.g., code, containers, service mesh)	46%
Cloud-based services	32%
Zero-Trust security strategy	20%
Other (please specify)	7%
Total	300%

Q19. What are your most important strategic priorities for digital security within your organization? Please select four choices only.	Consolidated
Crypto-agility	51%
Privileged access management (PAM)	36%
Complying with regulations	31%
Reducing the risk of unknown keys and certificates in the workplace (i.e. shadow IT)	32%
Knowing the expiration date of keys and certificates	44%
Investing in technologies that enhance the state of digital security	48%
Investing in hiring and retaining qualified personnel	55%
Reducing complexity in our IT infrastructure	49%
Authenticating and controlling IoT devices	49%
Other (please specify)	6%
Total	400%

Please rate the following statements using the strongly agree to strongly disagree scale provided below each item.	
Q20. My organization is deploying more cryptographic keys and digital certificates.	Consolidated
Strongly agree	32%
Agree	29%
Unsure	20%
Disagree	14%
Strongly Disagree	6%
Total	100%

Q21. The increasing use of cryptographic keys and digital certificates has significantly increased the operational burden on my organization's teams.	Consolidated
Strongly agree	35%
Agree	30%
Unsure	17%
Disagree	12%
Strongly Disagree	6%
Total	100%

Q22. My organization does not know how exactly many keys and certificates (including self-signed) it has.	Consolidated
Strongly agree	28%
Agree	30%
Unsure	19%
Disagree	14%
Strongly Disagree	10%
Total	100%

Q23. My organization is concerned about the increased workload and risk of outages caused by shorter SSL/TLS certificate lifespans.	Consolidated
Strongly agree	24%
Agree	32%
Unsure	22%
Disagree	10%
Strongly Disagree	12%
Total	100%

Q24. Misconfiguration of keys and certificates is an increasing concern in my organization.	Total
Strongly agree	30%
Agree	32%
Unsure	17%
Disagree	12%
Strongly Disagree	8%
Total	100%

Q25. Our organization is concerned about the ability to adapt to changes in cryptography (e.g., algorithm deprecation, quantum computing, etc.)	Total
Strongly agree	30%
Agree	32%
Unsure	17%
Disagree	13%
Strongly Disagree	8%
Total	100%

Following are specific capabilities that relate to an organization's ability to effectively deploy cryptographic solutions and methods to secure information assets and the IT infrastructure. Using the following 10-point scale, please rate your organization's ability from 1 = low ability to 10 = high ability.

Q26a. Ability to discover and secure every certificate or key	Consolidated
1 or 2	18%
3 or 4	14%
5 or 6	24%
7 or 8	34%
9 or 10	9%
Total	100%

Q26b. Ability to prevent unplanned certificates	Consolidated
1 or 2	19%
3 or 4	18%
5 or 6	31%
7 or 8	19%
9 or 10	13%
Total	100%

Q26c. Ability to remediate algorithm remediation or breach	Consolidated
1 or 2	19%
3 or 4	25%
5 or 6	23%
7 or 8	20%
9 or 10	13%
Total	100%

Q26d. Ability to detect and respond to certificate/key misuse	Consolidated
1 or 2	23%
3 or 4	20%
5 or 6	20%
7 or 8	25%
9 or 10	13%
Total	100%

Q26e. Ability to scale keys and certificates as business needs increase	Consolidated
1 or 2	14%
3 or 4	18%
5 or 6	22%
7 or 8	30%
9 or 10	16%
Total	100%

Q26f. Ability to drive enterprise-wide best practices and policies	Consolidated
1 or 2	18%
3 or 4	18%
5 or 6	26%
7 or 8	26%
9 or 10	12%
Total	100%

Q26g. Ability to attract and retain personnel skilled in PKI and cryptography	Consolidated
1 or 2	21%
3 or 4	16%
5 or 6	20%
7 or 8	25%
9 or 10	18%
Total	100%

Q26h. Ability to secure new initiatives such as hybrid, multi-cloud environments, DevOps, and Zero Trust	Consolidated
1 or 2	17%
3 or 4	23%
5 or 6	18%
7 or 8	25%
9 or 10	17%
Total	100%

Part 4. Budget

Q27. What is the total IT security budget for 2023?	Consolidated
Less than $1 million	3%
$1 to $5 million	8%
$6 to $10 million	11%
$11 to $15 million	14%
$16 to $20 million	19%
$21 to $25 million	20%
$26 to $50 million	12%
$51 to $100 million	10%
More than $100 million	3%
Total	100%
Extrapolated value	$26.99

Q28. What percentage of the total IT security budget is allocated to cryptographic management?	Consolidated
1% to 10%	35%
11% to 25%	38%
More than 25%	27%
Total	100%

Q29. What percentage of the budget is allocated to managing and securing certificates?	Consolidated
1% to 10%	31%
11% to 25%	41%
More than 25%	27%
Total	100%

Q30. Is your organization allocating any budget to post quantum computing preparation?	Consolidated
Yes, we are currently allocating budget	30%
Yes, we plan to allocate budget in the next six months	26%
Yes, we plan to allocate budget in the next year	22%
No, we have no plans to allocate budget	22%
Total	100%

Part 5. Organization and respondents' demographics

D1. What best describes your position level within the organization?	Consolidated
Executive/VP	8%
Director	15%
Manager	20%
Supervisor	10%
Staff/technician	23%
Administrative	13%
Consultant	5%
Other (please specify)	7%
Total	100%

D2. What best describes your department or team?	Consolidated
IT Security/SEC Ops	14%
IT Operations/Infrastructure	9%
Identity & Access Management (IAM)	21%
R&D/Engineering	10%
Networking	11%
Risk & Compliance	10%
DevOps / DevSecOps	22%
Other (please specify)	4%
Total	100%

D3. What range best describes the full-time headcount of your global organization?	Consolidated
Less than 1,000	8%
1,000 to 5,000	11%
5,001 to 10,000	22%
10,001 to 25,000	23%
25,001 to 75,000	18%
More than 75,000	17%
Total	100%
Extrapolated value	29,745

D4. What best describes your organization's primary industry classification?	Consolidated
Agriculture & food services	1%
Communications	4%
Consumer products	5%
Education & research	4%
Energy & utilities	7%
Financial services	17%
Healthcare & pharmaceutical	10%
Industrial & manufacturing	10%
Retail	8%
Services	12%
Technology & software	9%
Transportation	8%
Other (please specify)	6%
Total	100%

For more information about this study, please contact Ponemon Institute by sending an email to research@ponemon.org or call at 1.800.887.3118.

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.