KEYFACTOR

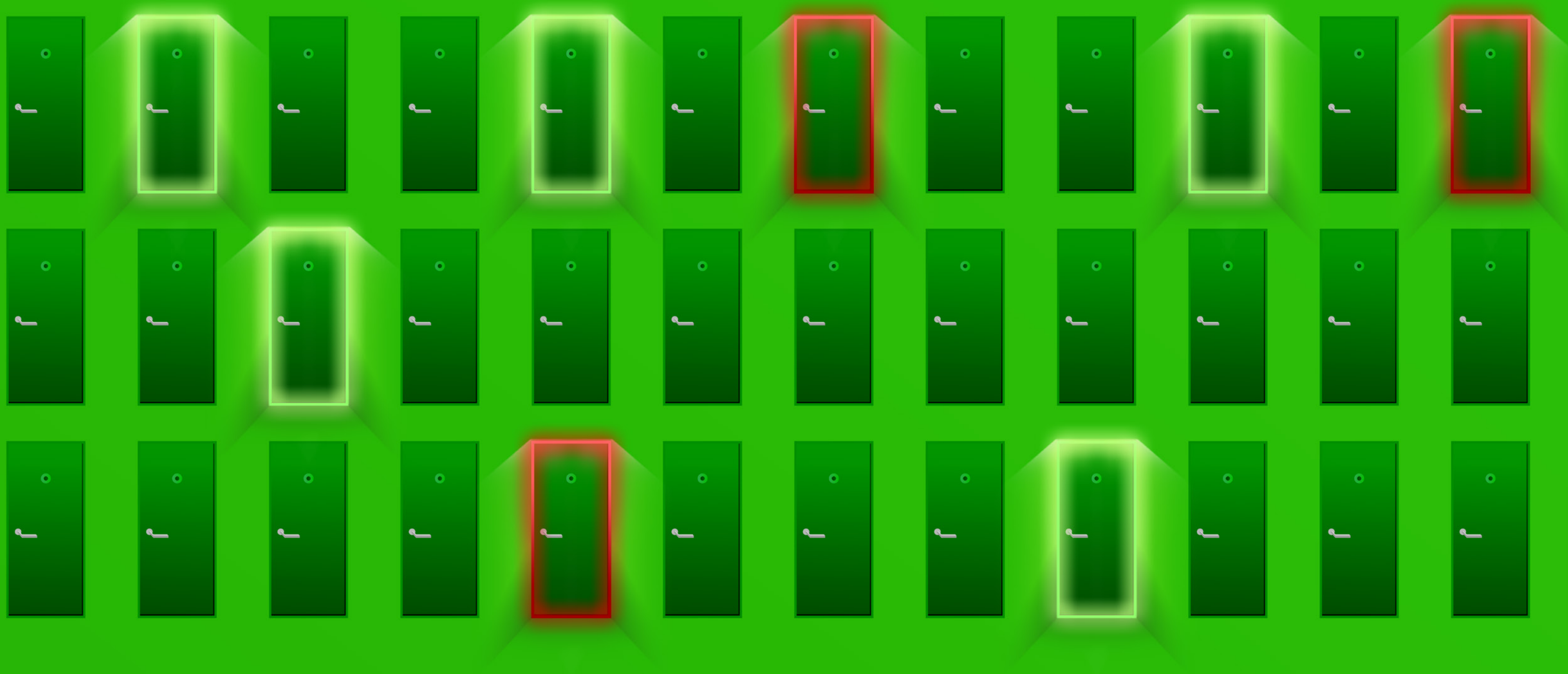
NORTH AMERICAN EDITION

The Impact of Unsecured Digital Identities

SPONSORED BY KEYFACTOR

Independently conducted by Ponemon Institute LLC

Publication Date: February 2020



Ponemon INSTITUTE

Table of Contents

Introduction

The Impact of Unsecured Digital Identities, sponsored by Keyfactor, reveals what happens when PKI and cryptography practices are not at their best. The report is based on survey responses from 603 IT and information security professionals across North America. We conclude from the findings that current approaches to managing and protecting cryptographic keys and digital certificates – known as digital identities – are putting organizations at significant risk.

In this year's report, we introduce the Critical Trust Index™ – a range of metrics that measure enterprises' ability to manage the rapid growth of keys and digital certificates required to secure critical data and connections across their business. Using a ten-point scale, IT and information security professionals responded to sixteen questions, indicating their ability from low (0) to high (10).

FOLLOWING IS A HIGH-LEVEL SUMMARY OF THE FINDINGS:

DISRUPTIVE OUTAGES ARE ON THE RISE.

Most organizations (73 percent) represented in this research continue to experience unplanned downtime and outages due to mismanaged digital certificates. Over half of respondents (55 percent) say their organizations have experienced four or more certificate-related outages in the past two years alone.

55%

of respondents say their organization experienced four or more certificate-related outages in the past two years.

Respondents estimate that their organizations have approximately

88,750

cryptographic keys and digital certificates in use today.

UNSECURED DIGITAL IDENTITIES UNDERMINE TRUST.

An estimated average of 88,750 keys and certificates are used by organizations today to secure data and authenticate systems. However, 74 percent of respondents believe their organizations do not know exactly how many keys and certificates (including self-signed) they have, much less where to find them or when they expire. Furthermore, 76 percent of respondents say that failure to secure keys and certificates undermines the trust their organization relies upon to operate.

FAILED AUDITS AND CA COMPROMISE CONSIDERED THE MOST SERIOUS THREATS.

According to the findings, failed audits due to insufficient key management practices and compromised or rogue certificate authorities (CA) are the most frequent and most serious problems faced by organizations when it comes to managing PKI and cryptography.

The average organization experienced

5.8

audit failures due to insufficient key management practices in the past two years.

2/3

of respondents are adding additional layers of encryption technologies.

MORE ENCRYPTION IS INCREASING OPERATIONAL COMPLEXITY AND COSTS.

Two-thirds of organizations are adding additional layers of encryption technologies to comply with industry regulations and IT policies. As a result, managing a growing number of cryptographic keys and digital certificates has increased operational costs and reduced the overall efficiency of business processes.

PKI LACKS RESOURCES AND CLEAR OWNERSHIP.

Only 38 percent of respondents say their organizations have enough IT security staff members dedicated to their PKI deployment. More than half of respondents (53 percent) say they are unable to hire and retained qualified IT security personnel. Responsibility for the PKI budget is also dispersed throughout the organization, with IT operations (21 percent) and lines of business (19 percent) cited most often as owners of the PKI budget.

Only

38%

of respondents say they their organizations have enough IT security staff dedicated to PKI.

48%

of respondents say authenticating and controlling IoT devices is a top strategic priority for digital security within their enterprise.

STRATEGIC PRIORITIES FOCUS ON THE IoT AND CERTIFICATE EXPIRATION.

According to respondents, the following are the top four strategic priorities for digital security in their enterprise: authenticating and controlling IoT devices, knowing the expiration date of certificates, reducing complexity in their IT infrastructure, and reducing the risk of unknown certificates in the workplace (i.e. shadow IT).

Key Findings

In this section, we analyze the key findings of the research. The complete detailed findings are available in the Appendix of this report. We have organized the findings according to these topics:

- Consequences of insufficient key & certificate management practices
- Risks & challenges in securing digital identities
- The state of PKI deployment

CONSEQUENCES OF INSUFFICIENT KEY AND CERTIFICATE MANAGEMENT PRACTICES

Failed audits and CA compromise are the most serious and frequent threats. Respondents were asked to rate the seriousness of cybersecurity threats caused by key or certificate management problems in their organization on a scale of 1 = least serious to 5 = most serious. As shown in Figure 1, the most serious threats are failed audits or compliance due to undocumented or unenforced key management policies or insufficient key management practices and CA compromise or rogue CAs that enable attackers to conduct man-in-the-middle and phishing attacks.

FIGURE 1.

How serious is the problem of cybersecurity threats caused by key or certificate management problems?

On a scale from 1 = least serious problem to 5 = most serious problem

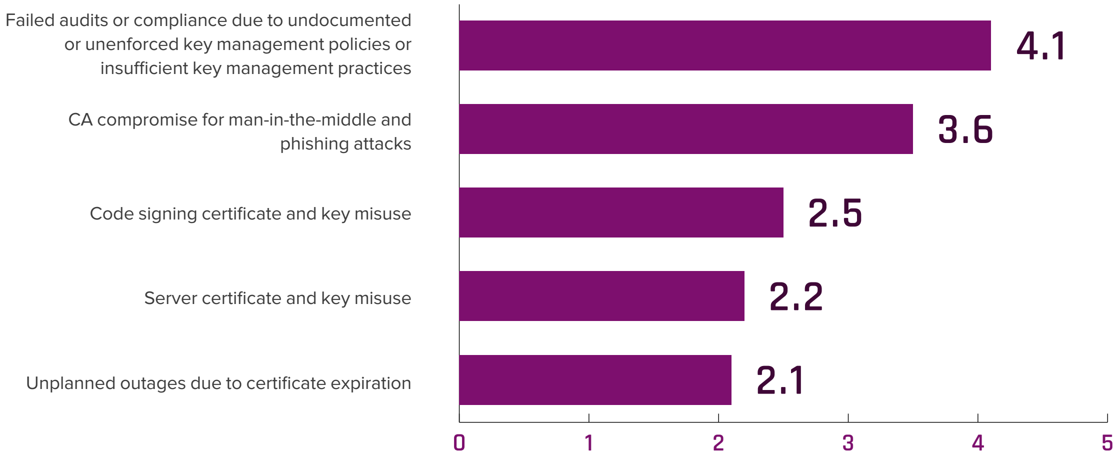
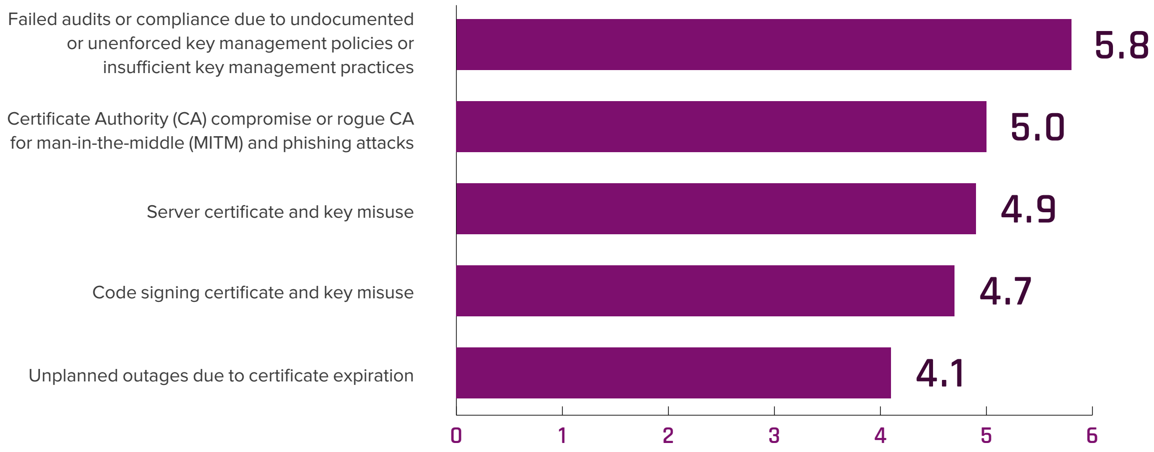


Figure 2 represents the average frequency of failed certificate management practices over the past 24 months. Organizations experienced an average of 5.8 failed audits or compliance followed by incidents involving CA compromise or rogue CAs. The least frequent incidents are unplanned outages due to certificate expiration, though the frequency of these events is still concerning.

FIGURE 2.

How many times has this occurred in your organization in the past 24 months?

Extrapolated values presented

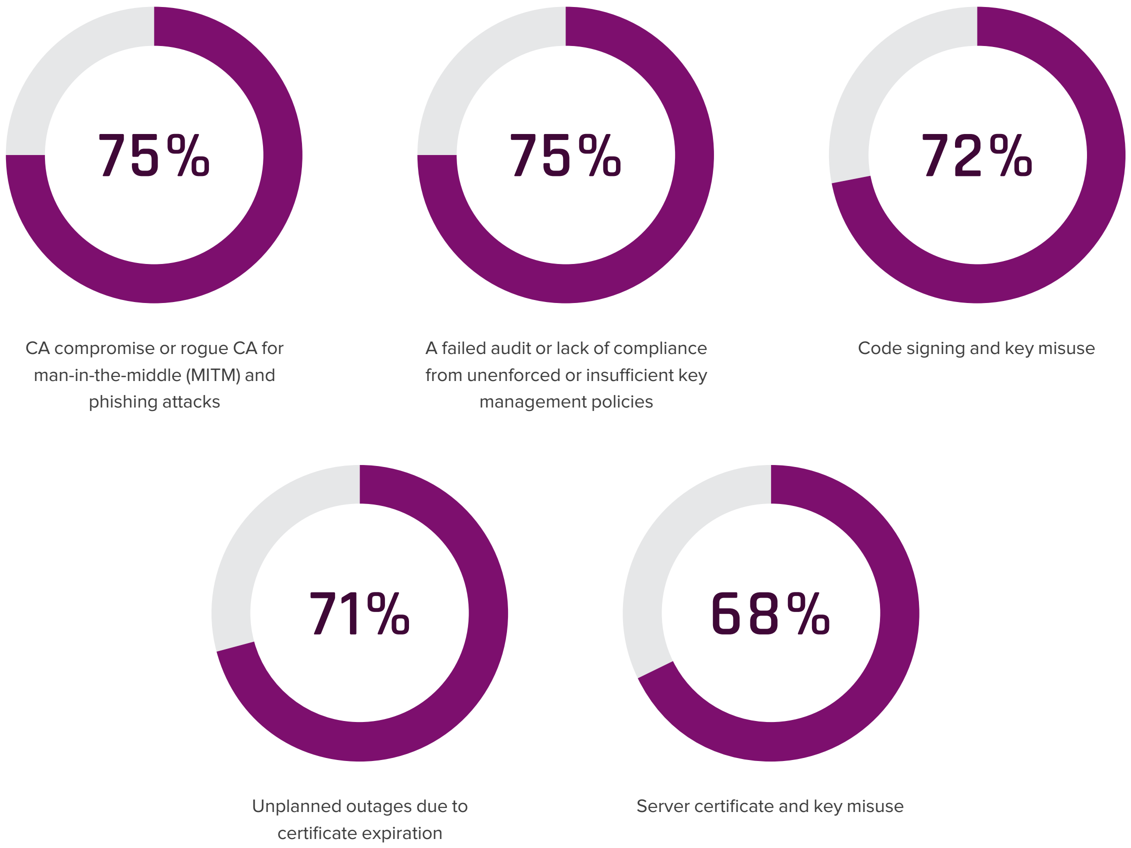


Failed audits and CA compromises also have the biggest financial impact. Respondents were asked to rate the financial impact of the consequences of failed certificate management practices on a scale of 1 = no impact to 10 = very serious impact. Figure 3 presents the serious and very serious impact (7+ responses). Seventy-five percent of respondents rate the financial impact of CA compromise or rogue CA for man-in-the-middle and phishing attacks a serious or very serious problem.

FIGURE 3.

How serious is the financial impact?

Serious and very serious responses combined

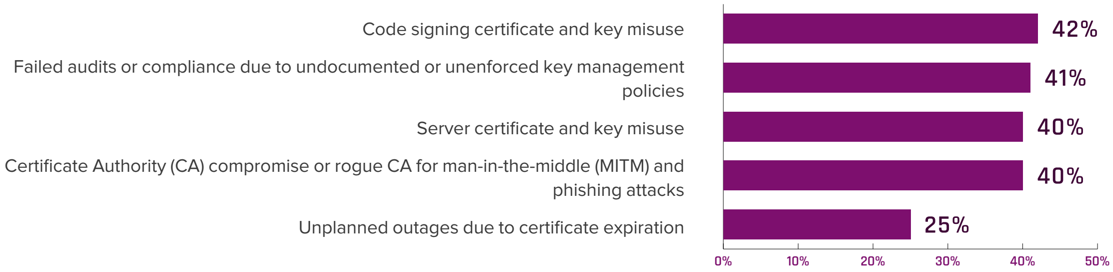


Code signing certificate and key misuse is most likely to occur in the next two years. The trust and integrity of software hinges entirely on the protection of code signing keys, but keeping them secure in fast-paced and dispersed development environments is challenging. Recent attacks involving misused keys such as those seen at ASUS or Netgear underscore the importance of protecting these critical assets. As seen in Figure 4, these incidents were rated the most likely to occur in the next 24 months.

FIGURE 4.

What is the likelihood that this issue will occur in your organization over the next 24 months?

Extrapolated values presented



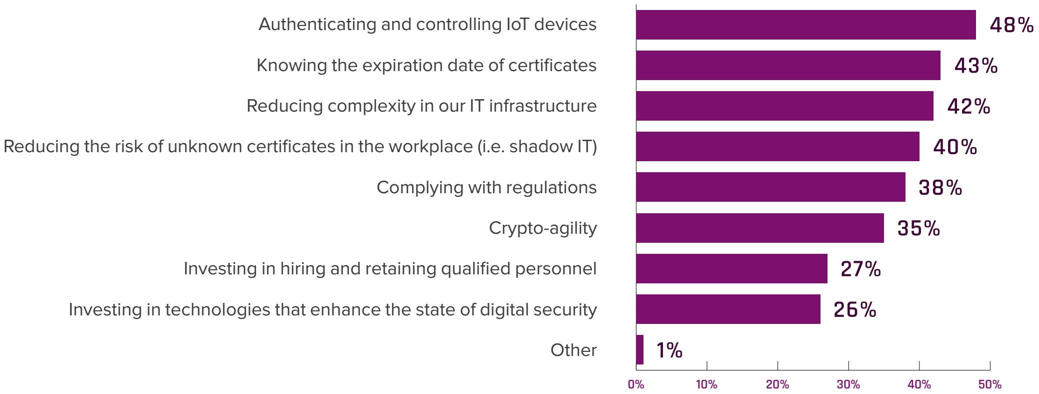
RISKS & CHALLENGES IN SECURING DIGITAL IDENTITIES

Securing IoT devices and staying ahead of certificate expiration are top strategic priorities. Emerging connected devices present a significant challenge for enterprises, as attackers seek to exploit weak credentials to steal data, disrupt services or distribute malware. When asked to rank their top three strategic priorities for digital security, 48 percent of respondents prioritized authenticating and controlling IoT devices, while another 43 percent say knowing the expiration date of certificates is critical.

FIGURE 5.

What are your strategic priorities for digital security within your organization?

Three responses permitted



The growing number of digital certificates and keys is increasing operational costs. As shown in Figure 6, two-thirds of respondents say their organization is adding additional layers of encryption technologies to comply with industry regulations and IT policies, while 60 percent say they are adding additional layers of encryption to secure IoT devices.

As the emergence of new IoT devices and industry mandates drive the need for robust encryption and device identity, the number of keys and digital certificates in most organizations has reached tens or even hundreds of thousands. Meanwhile, a trend toward shorter certificate validity has multiplied the management workload for IT and security teams by two to three-fold over the last decade. Not surprisingly, 58 percent of respondents say management of keys and digital certificates is increasing operational costs, while another 64 percent say it is reducing the general efficiency of business processes.

Only 47 percent of respondents are concerned about the impact that quantum computing will have on their key and certificate management practices, but we expect this number will rise as recent advances in quantum technology bring us closer to the potential breaking point of the keys and algorithms we rely upon today. This is especially true for IoT devices with lifespans of 10 years or more.

FIGURE 6.

Perceptions about the state of certificate management

Strongly agree and agree responses combined

66%

Adding additional layers of encryption technologies to comply with regulations and policies

64%

The management of cryptographic keys and digital certificates is reducing the general efficiency of business processes

63%

The increased use of encryption to comply with IT policies, audits, and regulations is increasing operational costs as a result of having to maintain a growing number of keys and digital certificates

60%

Adding additional layers of encryption technologies to secure IoT devices

58%

The management of cryptographic keys and digital certificates is increasing operational costs

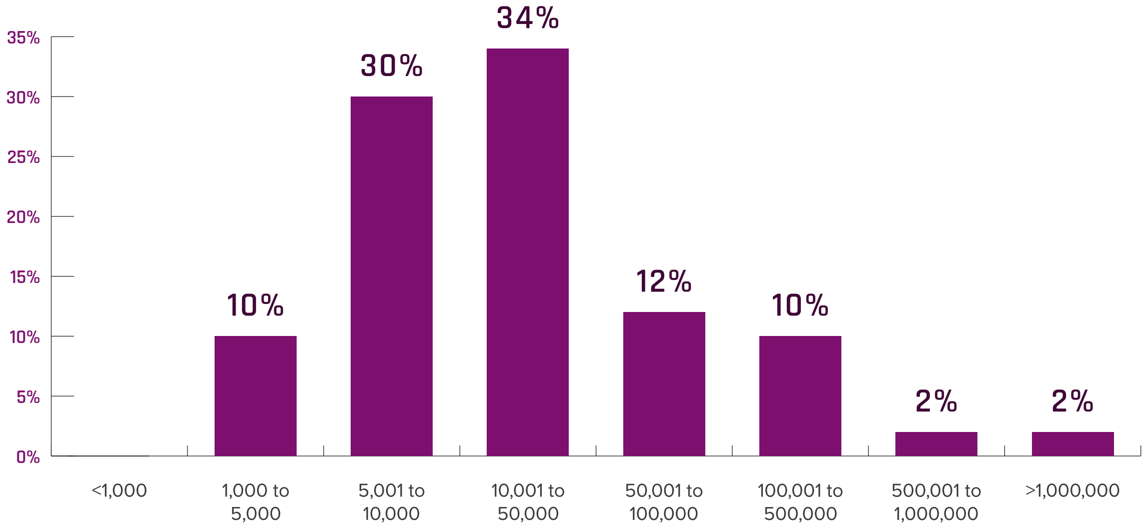
47%

Concerned that the rise of Quantum Computing will require my organization to significantly change its approaches to digital certificate and key management

Many respondents estimate their organizations have more than 10,000 keys and digital certificates in use. Respondents were asked to estimate the number of keys and certificates currently in use across their organization. As shown in Figure 7, 60 percent of respondents estimate their organizations have more than ten thousand keys and certificates in use (i.e. 10,001+). The extrapolated average number of keys and certificates used to secure data and authenticate systems is 88,750 across all respondents.

FIGURE 7.

The estimated number of keys and certificates used to secure data and authenticate systems

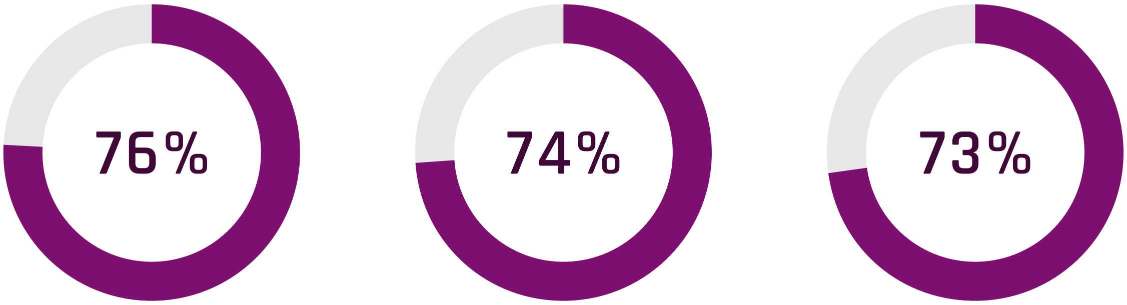


Unknown and unsecured digital identities undermine trust and disrupt operations. Figure 8 highlights the risks and challenges involved in managing digital identities at scale. 76 percent of respondents say failing to secure keys and certificates undermines the trust their organization relies upon to operate. Most respondents (74 percent) admit they do not knowing exactly how many keys and certificates (including self-signed) their organization has, much less how to protect them or where to find them when they expire. As a result, 73 percent of respondents continue to experience unanticipated downtime or outages due to unknown, expired, or misconfigured certificates.

FIGURE 8.

The risks and challenges in managing digital certificates

Strongly agree and agree responses combined



Failing to secure keys and certificates undermines the trust my organization relies upon to operate

My organization does not know how exactly many keys and certificates (including self-signed) it has

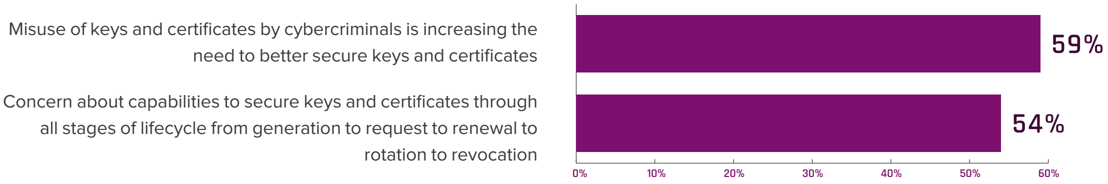
In my organization, digital certificates have caused and still cause unanticipated downtime or outages

Most organizations are concerned about their ability to secure keys and certificates. Attackers increasingly target unprotected or poorly managed keys and certificates to circumvent security controls, hide in encrypted traffic, or deploy malware. According to Figure 9, 59 percent of respondents say the misuse of keys and certificates by cybercriminals is increasing the need to better secure these critical assets. Yet, more than half (54 percent) of respondents are concerned about their ability to secure keys and certificates throughout all stages of their lifecycle – from generation to revocation.

FIGURE 9.

Security concerns in managing keys and certificates

Strongly agree and agree responses combined

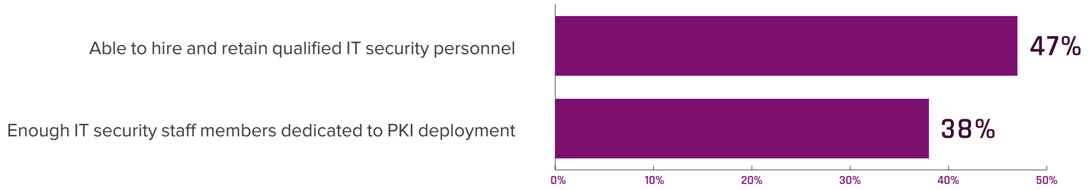


Insufficient IT security skills and resources leave PKI shorthanded. Deploying and running an effective PKI involves many moving parts beyond software – including infrastructure, policies, and trained personnel. However, most organizations lack specialized knowledge and depth in personnel required to support the ongoing operation of their PKI. According to Figure 10, only 38 percent of respondents say their organizations have sufficient IT security staff members dedicated to their PKI deployment. This problem is further complicated by the fact that only 47 percent of respondents say their organizations are able to hire and retain qualified IT security personnel.

FIGURE 10.

Challenges in staffing IT security

Yes responses presented

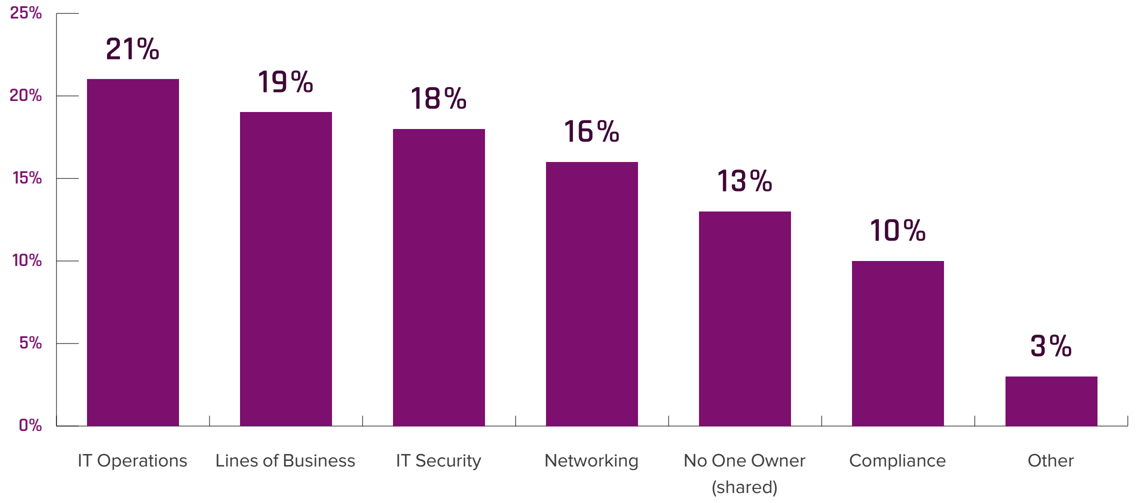


No one function emerges as the clear owner of the PKI budget. Public key infrastructure (PKI) is often a core technology used by multiple teams across the business – network engineers, developers, operations and security teams. Lack of clear ownership tends to place conflicting pressure on those involved when something goes wrong – such as a PKI-related outage or security breach.

Organizations represented in the study spend an average of $19.5 million on IT security annually, with an average of 16 percent (approximately $3 million) dedicated to the PKI budget. As seen in Figure 11, despite the increasingly important role that PKI plays in protecting sensitive data and applications, responsibility for the PKI budget is often dispersed throughout the organization, without clear lines of accountability.

FIGURE 11.

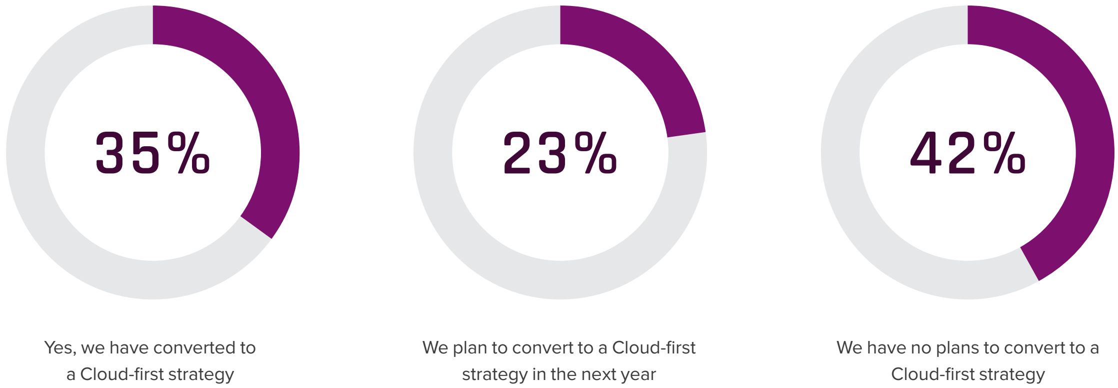
Who owns the PKI budget?



Cloud-first strategies are changing PKI deployment. As seen in Figure 12, more than half (58 percent) of organizations within this study have converted or plan to convert to a cloud-first strategy. Of these organizations, about two-thirds (67 percent) have included PKI in their cloud-first strategy.

FIGURE 12.

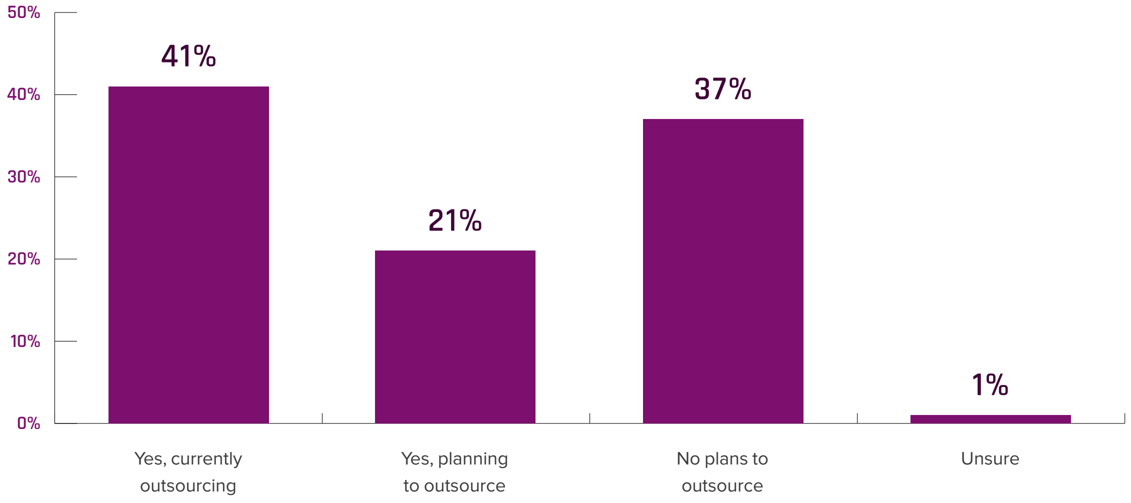
Have you or will you be converting to a Cloud-first strategy?



Most organizations have or plan to outsource their PKI deployment. Deploying and running a PKI in-house requires significant investment of resources – both human and capital. According to Figure 13, 62 percent of respondents say their organizations are currently outsourcing (41 percent) or planning to outsource (21 percent) all of part of their PKI deployment. Managed PKI or PKI as-a-Service solutions provide all the benefits of PKI, without the cost and complexity of running it in-house.

FIGURE 13.

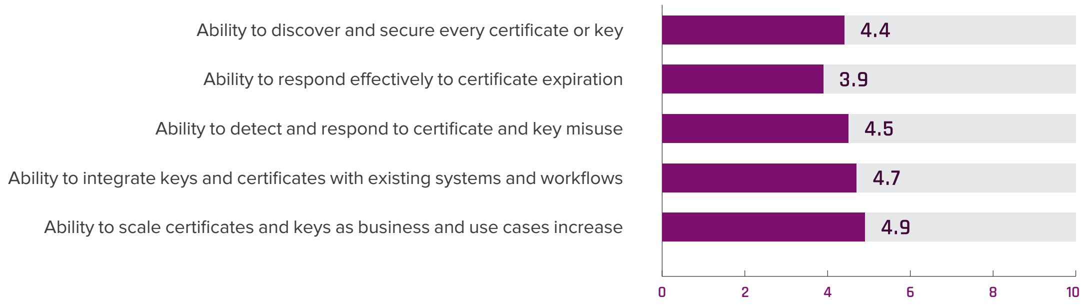
Would your organization consider outsourcing all or part of its PKI deployment?



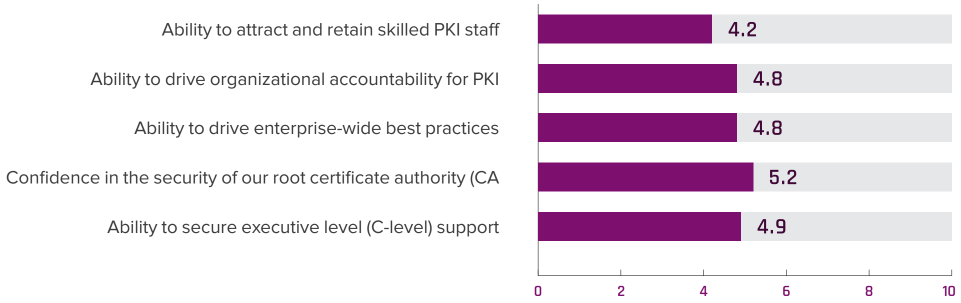
The Critical Trust Index™

The Critical Trust Index™ is designed to measure three core competencies that enterprises need to effectively secure and manage their digital identities – key and certificate management, PKI operations, and business agility and growth. Based on 16 survey questions related to the three core competencies, respondents indicated their organization's ability on a ten-point scale from very low (0) to very high (10). The findings in this section are organized by the three core competencies.

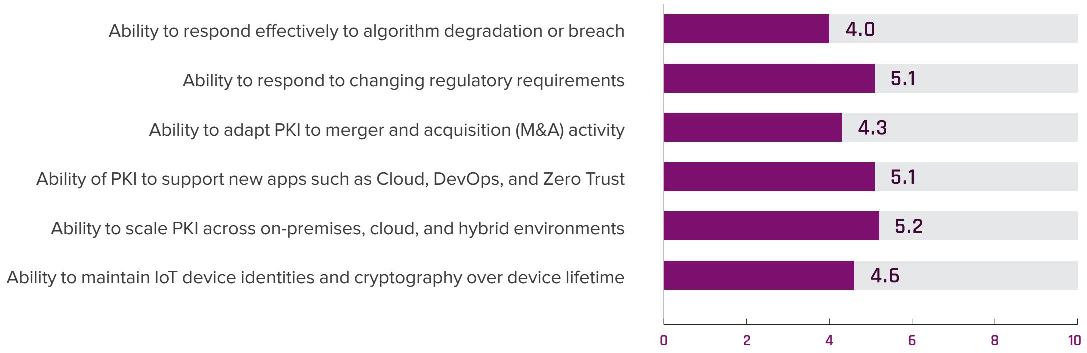
KEY & CERTIFICATE MANAGEMENT



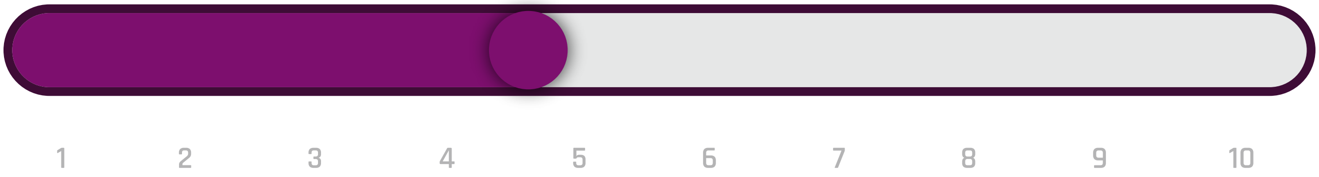
PKI OPERATIONS



BUSINESS AGILITY & GROWTH



OVERALL SCORE



4.7/10

Based on the collective responses to all 16 questions, the average respondent scored a **4.7 out of 10** on the Critical Trust Index™. It's clear that a significant gap exists between the rapid growth of connectivity driven by digital transformation and the ability of enterprises to manage the growing number of keys and digital certificates required to secure those connections and protect sensitive data.

How does your organization compare?

We invite you to calculate your score on the Critical Trust Index™ and get your personalized recommendations at benchmark.keyfactor.com.

CALCULATE YOUR SCORE

Methods

The sampling frame is composed of 16,825 IT and information security practitioners across North America. All respondents are familiar with their companies' strategy for the protection of digital identities. As shown in Table 1, 668 respondents completed the survey. Screening removed 65 surveys.

TABLE 1.

Sample Response

	FREQUENCY	PERCENT %
TOTAL SAMPLING FRAME	16,825	100.0%
TOTAL RETURNS	668	4.0%
REJECTED OR SCREENED SURVEYS	65	.4%
FINAL SAMPLE	603	3.6%

Figure 14 reports the current position or organizational level of the respondents. More than half of respondents (61 percent) reported their current position as supervisory or above and 30 percent of respondents are at the staff/technician level.

FIGURE 14.

Distribution of respondents according to position level

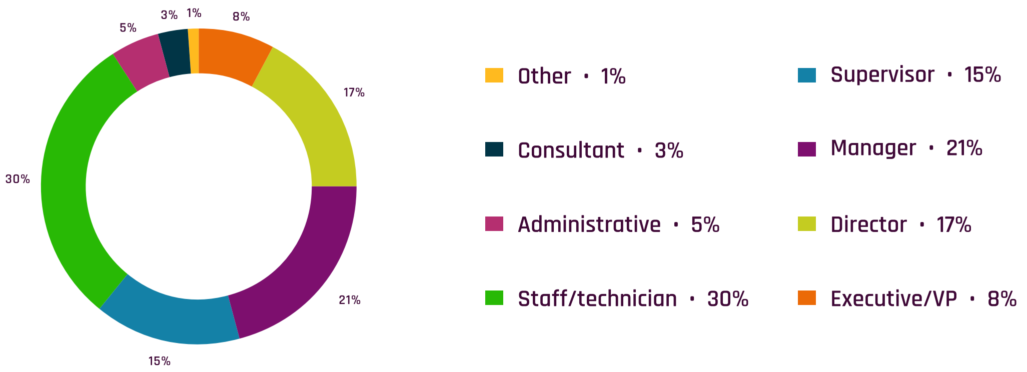
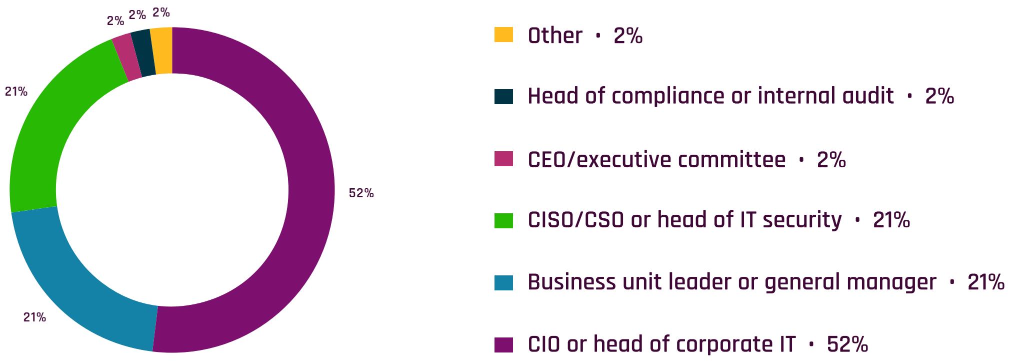


Figure 15 identifies the primary person to whom the respondent or their IT security leader reports. Fifty-two percent of respondents identified the CIO or head of corporate IT as the person to whom they report. Another 21 percent indicated they report directly to the business unit leader or general manager and 20 percent of respondents report to the CISO/CSO or head of IT security.

FIGURE 15.

Distribution of respondents according to reporting channel



According to Figure 16, more than half of the respondents (64 percent) are from organizations with a global head count of more than 5,000 employees.

FIGURE 16.

Distribution of respondents according to organizational head count

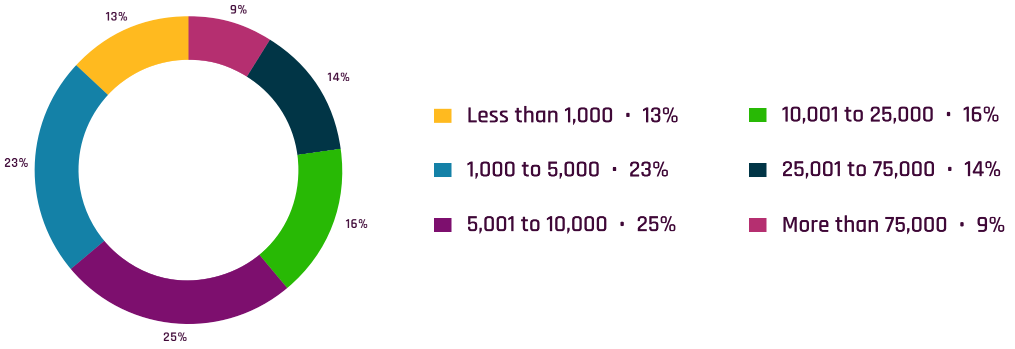
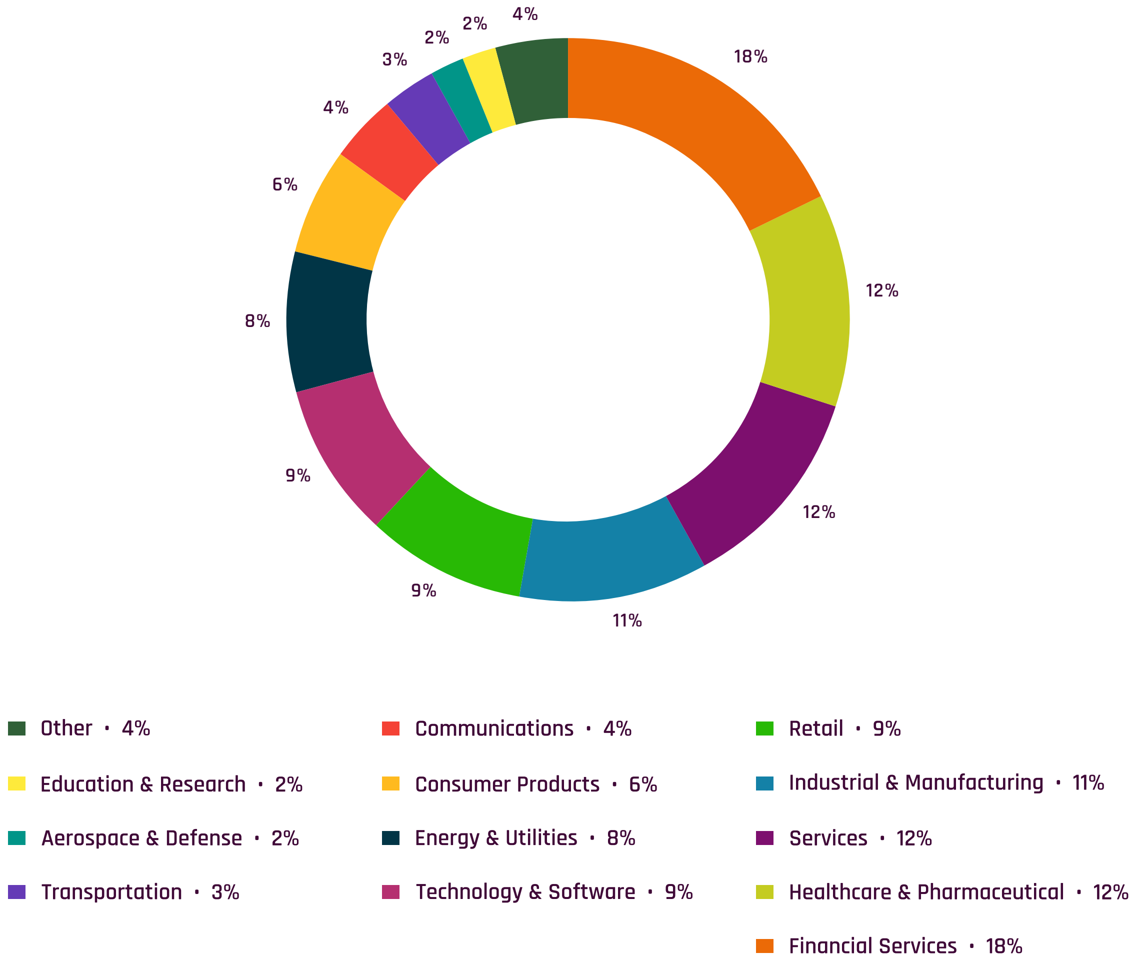


Figure 17 reports the primary industry classification of respondents' organizations. This chart identifies financial services (18 percent of respondents) as the largest segment, which includes banking, investment management, insurance, brokerage, payments and credit cards. This is followed by healthcare and pharmaceutical (12 percent of respondents), services sector (12 percent of respondents), industrial and manufacturing (11 percent of respondents), retail and technology and software (each at 9 percent of respondents).

FIGURE 17.

Distribution of respondents according to primary industry classification



Research Limitations

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 IT or IT security practitioners in various organizations in North America. We also acknowledge that the results may be biased by external events such as media coverage. We also acknowledge bias caused by compensating subjects to complete this research within a specified time period.

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

DETAILED SURVEY RESULTS

The following tables provide the frequency or percentage frequency of responses to all survey questions contained in this study. All survey responses were captured from December 6, 2019 to December 20, 2019.

SURVEY RESPONSE	FREQUENCY	PERCENT %
TOTAL SAMPLING FRAME	16,825	100.0%
TOTAL RETURNS	668	4.0%
REJECTED OR SCREENED SURVEYS	65	0.4%
FINAL SAMPLE	603	3.6%

S1. DOES YOUR ORGANIZATION HAVE A PKI?	PERCENT %
YES	100%
NO (STOP)	0%
TOTAL	100%

S2. WHAT BEST DEFINES YOUR FAMILIARITY WITH THE ORGANIZATION'S PKI?	PERCENT %
VERY FAMILIAR	44%
FAMILIAR	38%
SOMEWHAT FAMILIAR	18%
NOT FAMILIAR (STOP)	0%
TOTAL	100%

S3. WHAT BEST DEFINES YOUR LEVEL OF CRYPTOGRAPHIC KNOWLEDGE	PERCENT %
VERY KNOWLEDGEABLE	40%
KNOWLEDGEABLE	33%
SOMEWHAT KNOWLEDGEABLE	27%
NOT KNOWLEDGEABLE (STOP)	0%
TOTAL	100%

PART 1: BACKGROUND ABOUT YOUR ORGANIZATION

Strongly agree and Agree responses

		AGREEMENT
Q1A	My organization is adding additional layers of encryption (such as data encryption, SSL/TLS, etc.) technologies to comply with regulations and policies.	66%
Q1B	My organization is adding additional layers of encryption (such as data encryption, SSL/TLS, etc.) technologies to secure IoT (Internet of Things) devices.	60%
Q1C	The increased use of encryption (such as data encryption, SSL/TLS, etc.) to comply with IT policies, audits, and regulations is increasing my organization's operational costs as a result of having to maintain a growing number of keys and digital certificates.	63%
Q1D	The management of cryptographic keys (for data encryption, SSL/TLS, etc.) and digital certificates is increasing my organization's operational costs.	58%
Q1E	The management of cryptographic keys (for data encryption, SSL/TLS, etc.) and digital certificates is reducing the general efficiency of business processes.	64%
Q1F	My organization is concerned about its capabilities to secure keys and certificates through all stages of lifecycle from generation to request to renewal to rotation to revocation.	54%
Q1G	My organization does not know how exactly many keys and certificates (including self-signed) it has	74%
Q1H	In my organization, digital certificates have caused and still cause unanticipated downtime or outages.	73%
Q1I	Failing to secure keys and certificates undermines the trust my organization relies upon to operate.	76%
Q1J	Misuse of keys and certificates by cybercriminals is increasing the need for my organization to better secure keys and certificates.	59%
Q1K	Our organization is concerned that the rise of Quantum Computing will require my organization to significantly change its approaches to digital certificate and key management.	47%
Q1L	Migration to the cloud environment requires my organization to significantly change its approach to digital certificate and key management.	71%

PART 2: CRYPTOGRAPHIC READINESS CAPABILITIES

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 index scale:

Very high ability = 10

High ability = 7.5

Unsure = 5

Low ability = 2.5

Very low ability = 0

		SCORE
Q2A	Ability to discover and secure every certificate or key	4.38
Q2B	Ability to respond effectively to cert expiration	3.88
Q2C	Ability to respond effectively to algorithm degradation or breach	3.98
Q2D	Ability to detect and respond to cert/key misuse	4.48
Q2E	Ability to integrate keys and certs with existing systems and workflows	4.70
Q2F	Ability to adapt PKI to M&A activity	4.28
Q2G	Ability to scale keys and certs as business and use cases increase	4.93
Q2H	Ability to drive organizational accountability for PKI	4.83
Q2I	Ability to drive enterprise-wide best practices	4.78
Q2J	Ability to attract and retain skilled PKI staff	4.23
Q2K	Ability to secure C-level support	4.93
Q2L	Confidence in the ability of PKI to support new apps such as Cloud First, DevOps, Zero Trust and more	5.05
Q2M	Ability to respond to changing regulatory requirements	5.05
Q2N	Ability to scale PKI across on-premises, cloud and hybrid environments	5.18
Q2O	Confidence in the security of our Root CA	5.18
Q2P	Ability to maintain IoT device identities and cryptography over device lifetime	4.60
	Average	4.65

PART 3: BACKGROUND AND TRENDS

Q3. PLEASE RANK THE FOLLOWING SIX CYBER SECURITY THREATS CAUSED BY KEY OR CERTIFICATE MANAGEMENT PROBLEMS IN YOUR ORGANIZATION.

Here, 1 = least serious problem to 5 = most serious problem.

	AVG RANK
Unplanned outages due to certificate expiration	2.06
Failed audits or compliance due to undocumented or unenforced key management policies or insufficient key management practices	4.13
Server certificate and key misuse	2.23
Code signing certificate and key misuse	2.46
CA compromise for man-in-the-middle and phishing attacks	3.63

Q4. HOW MANY IT SECURITY STAFF MEMBERS ARE DEDICATED TO PKI DEPLOYMENT?

	PERCENT %
Zero	21%
1 to 5	29%
6 to 10	33%
11 to 20	14%
More than 20	3%
Total	100%
Extrapolated value	6.40

Q5. DOES YOUR ORGANIZATION HAVE ENOUGH IT SECURITY STAFF MEMBERS DEDICATED TO PKI DEPLOYMENT?

	PERCENT %
Yes	38%
No	62%
Total	100%

Q6. IS YOUR ORGANIZATION ABLE TO HIRE AND RETAIN QUALIFIED IT SECURITY PERSONNEL?

	PERCENT %
Yes	47%
No	53%
Total	100%

Q7. HOW MUCH DOES YOUR ORGANIZATION SPEND ANNUALLY ON IT SECURITY?

	PERCENT %
Less than $1 million	2%
$1 to 5 million	5%
$6 to $10 million	14%
$11 to $15 million	23%
$16 to $20 million	24%
$21 to $25 million	16%
$26 to $50 million	11%
More than $50 million	5%
Total	100%
Extrapolated value (US$ millions)	$19.46

Q8. WHAT PERCENTAGE OF THE IT SECURITY BUDGET IS ALLOCATED TO PKI DEPLOYMENT ANNUALLY?

	PERCENT %
Less than 5%	8%
5% to 10%	22%
11% to 20%	37%
More than 20%	33%
Total	100%
Extrapolated value	15.6%

Q9. WHO OWNS THE PKI BUDGET?

	PERCENT %
IT Security	18%
IT Operations	21%
Networking	16%
Compliance	10%
Lines of business	19%
No one owner (shared)	13%
Other (please specify)	3%
Total	100%

Q10. HOW FAMILIAR ARE YOU WITH THE TERM CLOUD FIRST?

	PERCENT %
Very familiar	35%
Familiar	43%
Not familiar (please skip to Q14)	22%
Total	100%

Q11. IF YES, HAVE YOU OR WILL YOU BE CONVERTING TO A CLOUD FIRST STRATEGY?

	PERCENT %
Yes, we have converted to a Cloud First strategy	35%
We plan to convert to a Cloud First strategy in the next year	23%
We have no plans to convert to a Cloud First strategy	42%
Total	100%

Q12. IF YES, DOES YOUR CURRENT CLOUD FIRST STRATEGY INCLUDE PKI DEPLOYMENT?

	PERCENT %
Yes	67%
No	33%
Total	100%

Q13. WOULD YOUR ORGANIZATION CONSIDER OUTSOURCING ALL OR PART OF ITS PKI DEPLOYMENT?

	PERCENT %
Yes, currently outsourcing	41%
Yes, planning to outsource	21%
No plans to outsource	37%
Unsure	1%
Total	100%

Q14. ARE YOU USING CERTIFICATES TO SECURE CONTAINERS (I.E. DOCKER, ETC.)?

	PERCENT %
Yes	52%
No	48%
Total	100%

Q15. APPROXIMATELY, HOW MANY KEYS AND CERTIFICATES FOR USE IN DATA ENCRYPTION, SSL/TLS, VPNS, APPLICATION SERVERS, ETC. ARE USED TO SECURE DATA AND AUTHENTICATE SYSTEMS?

	PERCENT %
Less than 1,000	1%
1,000 to 5,000	15%
5,001 to 10,000	29%
10,001 to 50,000	30%
51,000 to 100,000	13%
101,000 to 500,000	11%
500,000 to 1,000,000	0%
More than 1,000,000	1%
Total	100%
Extrapolated value	65,380

Q16. HOW MANY KEYS AND CERTIFICATES DO YOU BELIEVE ARE IN USE BY YOUR ORGANIZATION TODAY TO SECURE DATA AND AUTHENTICATE SYSTEMS?

	PERCENT %
Less than 1,000	0%
1,000 to 5,000	10%
5,001 to 10,000	30%
10,001 to 50,000	34%
51,000 to 100,000	12%
101,000 to 500,000	10%
500,000 to 1,000,000	2%
More than 1,000,000	2%
Total	100%
Extrapolated value	88,750

PART 4: ESTIMATING OPERATIONAL AND COMPLIANCE COSTS

Scenario 1. Unplanned outages due to certificate expiration.

Q17. USING THE FOLLOWING 10-POINT SCALE, PLEASE RATE THE SERIOUSNESS OF EXPERIENCING UNPLANNED OUTAGES DUE TO CERTIFICATE EXPIRATION

1 = not serious to 10 = very serious.

	PERCENT %
1 or 2	0%
3 or 4	8%
5 or 6	24%
7 or 8	32%
9 or 10	36%
Total	100%
Extrapolated value	7.42

Q18A-1. HOW MANY TIMES HAS THIS ISSUE OCCURRED IN YOUR ORGANIZATION DURING THE PAST **24 MONTHS**?

	PERCENT %
Zero	13%
One	7%
Two	6%
Three	19%
Four	24%
Five	15%
More than 5	16%
Total	100%
Extrapolated value	4.07

Q18A-2. WHAT IS THE LIKELIHOOD THAT THIS ISSUE WILL OCCUR IN YOUR ORGANIZATION OVER THE NEXT **24 MONTHS**?

	PERCENT %
Less than 5 percent	6%
5 to 10%	7%
11 to 15%	16%
16 to 20%	21%
21 to 30%	24%
31 to 40%	9%
41 to 50%	5%
More than 50 percent	12%
Total	100%
Extrapolated value	25.4%

Q19. USING THE FOLLOWING 10-POINT SCALE, PLEASE RATE THE FINANCIAL IMPACT OF UNPLANNED OUTAGES DUE TO CERTIFICATE EXPIRATION

From 1 = no impact to 10 = very serious impact.

	PERCENT %
1 or 2	4%
3 or 4	2%
5 or 6	23%
7 or 8	29%
9 or 10	42%
Total	100%
Extrapolated value	7.56

Scenario 2. Failed audits or compliance due to undocumented or unenforced key management policies.

Q20. USING THE FOLLOWING 10-POINT SCALE, PLEASE RATE THE SERIOUSNESS OF A FAILED AUDIT OR LACK OF COMPLIANCE FROM UNENFORCED OR INSUFFICIENT POLICIES

1 = not serious to 10 = very serious.

	PERCENT %
1 or 2	5%
3 or 4	11%
5 or 6	12%
7 or 8	32%
9 or 10	40%
Total	100%
Extrapolated value	7.32

Q21A-1. HOW MANY TIMES HAS THIS OCCURRED IN YOUR ORGANIZATION DURING THE PAST **24 MONTHS**?

	PERCENT %
Zero	1%
One	3%
Two	7%
Three	8%
Four	21%
Five	29%
More than 5	31%
Total	100%
Extrapolated value	5.80

Q21A-2. WHAT IS THE LIKELIHOOD THIS WILL OCCUR IN YOUR ORGANIZATION OVER THE NEXT **24 MONTHS**?

	PERCENT %
Less than 5 percent	0%
5 to 10%	3%
11 to 15%	8%
16 to 20%	7%
21 to 30%	11%
31 to 40%	17%
41 to 50%	19%
More than 50 percent	35%
Total	100%
Extrapolated value	41.0%

Q22. USING THE FOLLOWING 10-POINT SCALE, PLEASE RATE THE FINANCIAL IMPACT A FAILED AUDIT OR LACK OF COMPLIANCE FROM UNENFORCED OR INSUFFICIENT KEY MANAGEMENT POLICIES

1 = no impact to 10 = very serious impact.

	PERCENT %
1 or 2	1%
3 or 4	5%
5 or 6	19%
7 or 8	35%
9 or 10	40%
Total	100%
Extrapolated value	7.66

Scenario 3. Server certificate and key misuse

Q23A-1. HOW MANY TIMES DID YOUR ORGANIZATION EXPERIENCE THE THEFT OF KEYS OR CERTIFICATES AS A RESULT OF SERVER CERTIFICATE AND KEY MISUSE DURING THE **PAST 24 MONTHS**?

	PERCENT %
Zero	13%
One	13%
Two	12%
Three	6%
Four	5%
Five	19%
More than 5	32%
Total	100%
Extrapolated value	4.90

Q23A-2. WHAT IS THE LIKELIHOOD THAT YOUR ORGANIZATION WILL EXPERIENCE THE THEFT OF KEYS OR CERTIFICATES AS A RESULT OF SERVER CERTIFICATE AND KEY MISUSE OVER THE NEXT **24 MONTHS**?

	PERCENT %
Less than 5 percent	0%
5 to 10%	3%
11 to 15%	8%
16 to 20%	11%
21 to 30%	10%
31 to 40%	9%
41 to 50%	28%
More than 50 percent	31%
Total	100%
Extrapolated value	40.3%

Q24. USING THE FOLLOWING 10-POINT SCALE, PLEASE RATE THE FINANCIAL IMPACT OF SERVER CERTIFICATE AND KEY MISUSE

from 1 = no impact to 10 = very serious impact

	PERCENT %
1 or 2	0%
3 or 4	8%
5 or 6	24%
7 or 8	32%
9 or 10	36%
Total	100%
Extrapolated value	7.42

Scenario 4. Code signing certificate and key misuse

Q25A-1. HOW MANY TIMES HAS THIS ISSUE OCCURRED IN YOUR ORGANIZATION DURING THE PAST **24 MONTHS**?

	PERCENT %
Zero	10%
One	7%
Two	12%
Three	18%
Four	8%
Five	19%
More than 5	26%
Total	100%
Extrapolated value	4.72

Q25A-2. WHAT IS THE LIKELIHOOD THAT THIS ISSUE WILL OCCUR IN YOUR ORGANIZATION OVER THE NEXT **24 MONTHS**?

	PERCENT %
Less than 5 percent	0%
5 to 10%	0%
11 to 15%	4%
16 to 20%	7%
21 to 30%	13%
31 to 40%	21%
41 to 50%	25%
More than 50 percent	30%
Total	100%
Extrapolated value	41.9%

Q26. USING THE FOLLOWING 10-POINT SCALE, PLEASE RATE THE FINANCIAL IMPACT OF CODE SIGNING AND KEY MISUSE

from 1 = no impact to 10 = very serious impact

	PERCENT %
1 or 2	7%
3 or 4	6%
5 or 6	15%
7 or 8	27%
9 or 10	45%
Total	100%
Extrapolated value	7.44

Scenario 5. Certificate Authority (CA) compromise or rogue CA for man-in-middle (MITM) and phishing attacks

Q27A-1. HOW MANY TIMES HAS THIS ISSUE OCCURRED IN YOUR ORGANIZATION DURING THE PAST **24 MONTHS**?

	PERCENT %
Zero	4%
One	12%
Two	9%
Three	16%
Four	12%
Five	19%
More than 5	28%
Total	100%
Extrapolated value	5.01

Q27A-2. WHAT IS THE LIKELIHOOD THAT THIS ISSUE WILL OCCUR IN YOUR ORGANIZATION OVER THE NEXT **24 MONTHS**?

	PERCENT %
Less than 5 percent	1%
5 to 10%	0%
11 to 15%	4%
16 to 20%	8%
21 to 30%	15%
31 to 40%	19%
41 to 50%	28%
More than 50 percent	25%
Total	100%
Extrapolated value	40.3%

Q28. USING THE FOLLOWING 10-POINT SCALE, PLEASE RATE THE FINANCIAL IMPACT OF CA COMPROMISE OR ROGUE CA FOR MAN-IN-THE-MIDDLE (MITM) AND PHISHING ATTACKS

from 1 = no impact to 10 = very serious impact

	PERCENT %
1 or 2	6%
3 or 4	6%
5 or 6	13%
7 or 8	29%
9 or 10	46%
Total	100%
Extrapolated value	7.56

PART 5: ORGANIZATION AND RESPONDENTS' DEMOGRAPHICS

D1. WHAT BEST DESCRIBES YOUR POSITION LEVEL WITHIN THE ORGANIZATION?

	PERCENT %
Executive/VP	8%
Director	17%
Manager	21%
Supervisor	15%
Staff/technician	30%
Administrative	5%
Consultant	3%
Other	1%
Total	100%

D2. WHAT BEST DESCRIBES YOUR DIRECT REPORTING CHANNEL?

	PERCENT %
CEO/executive committee	2%
COO or head of operations	0%
CFO, controller or head of finance	0%
CIO or head of corporate IT	52%
Business unit leader or general manager	21%
Head of compliance or internal audit	2%
CISO/CSO or head of IT security	21%
Other	2%
Total	100%

D3. WHAT RANGE BEST DESCRIBES THE FULL-TIME HEADCOUNT OF YOUR GLOBAL ORGANIZATION?

	PERCENT %
Less than 1,000	13%
1,000 to 5,000	23%
5,001 to 10,000	25%
10,001 to 25,000	16%
25,001 to 75,000	14%
More than 75,000	9%
Total	100%

D4. WHAT BEST DESCRIBES YOUR ORGANIZATION'S PRIMARY INDUSTRY CLASSIFICATION?

	PERCENT %
Agriculture & food services	1%
Aerospace & defense	2%
Communications	4%
Consumer products	6%
Education & research	2%
Energy & utilities	8%
Financial services	18%
Healthcare & pharmaceutical	12%
Industrial & manufacturing	11%
Retail	9%
Services	12%
Technology & software	9%
Transportation	3%
Other (please specify)	3%
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.

About Keyfactor

SECURE EVERY DIGITAL IDENTITY

Keyfactor empowers enterprises of all sizes to escape the exposure epidemic – when breaches, outages and failed audits from digital certificates and keys impact brand loyalty and the bottom line. Powered by the industry's only PKI as-a-service platform, IT and infosec teams can easily manage digital certificates and keys. And product teams can build IoT devices with crypto-agility and at massive scale.

Learn more at www.keyfactor.com.

CONTACT US

About 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.