The Impact of Unsecured Digital Identities

Sponsored by Keyfactor

Independently conducted by Ponemon Institute LLC

Publication Date: January 2019

The Impact of Unsecured Digital Identities
Ponemon Institute, January 2019

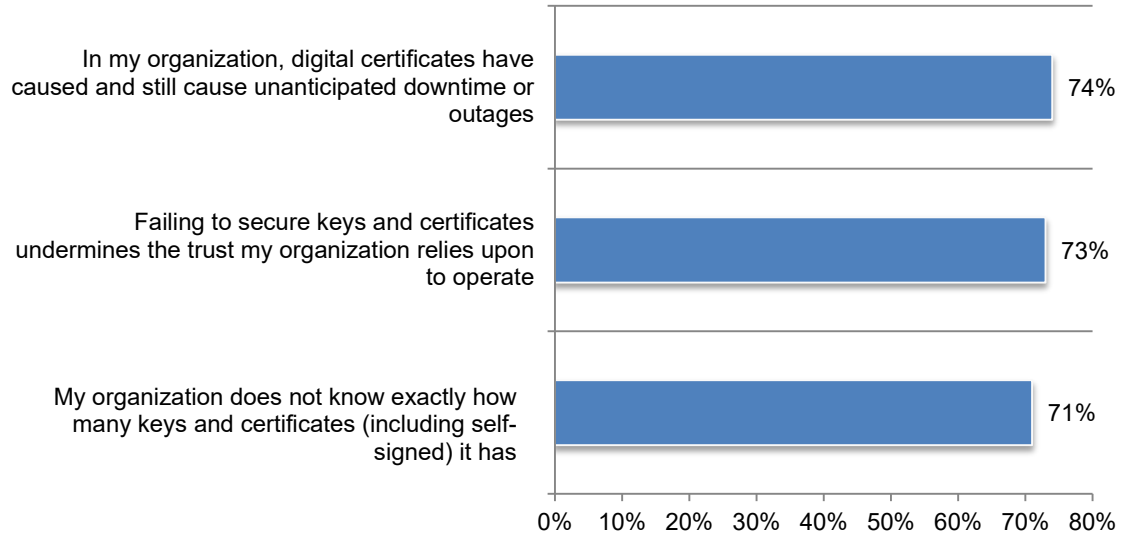
Table of Contents

Part 1. Introduction

The Impact of Unsecured Digital Identities, sponsored by Keyfactor, was conducted to understand the challenges and costs facing organizations in the protection and management (or mismanagement) of cryptographic keys and digital identities. Ponemon Institute surveyed 596 IT and IT security practitioners in the United States who are familiar with their companies' strategy for the protection of digital identities.

As shown in Figure 1, **74 percent of respondents say digital certificates have caused and still cause unanticipated downtime or outages**. Seventy-three percent of respondents are also aware that failing to secure keys and certificates undermines the trust their organization relies upon to operate. And, **71 percent of respondents believe their organizations do not know how many keys and certificates they have**.

Figure 1. Digital certificate challenges
Strongly agree and Agree responses combined



According to the findings, the growth in the use of digital certificates is causing the following operational issues and security threats:

- Operational costs are increasing with the need to add additional layers of encryption of critical data that requires securing keys and the management of digital certificates to comply with data protection regulations.
- Failed audits and lack of compliance are the costliest and most serious threats to an organization's ability to minimize the risk of unsecured digital identities and avoid costly fines.
- The risk of unsecured digital identities is undermining trust with customers and business partners.
- Unanticipated downtime or outages caused by digital certificates are having significant financial consequences in terms of productivity loss, including the diminishment of the IT security team's ability to be productive.
- Most organizations do not have adequate IT security staff to maintain and secure keys and certificates, especially in the deployment of PKI. Further, most organizations do not know how many keys and certificates that IT security needs to manage.

- Pricing models can prevent organizations from investing in solutions that cover every identity across the enterprise.

- Organizations have difficulty in securing keys and certificates through all stages of lifecycle from generation, request, renewal, rotation to revocation.

The total cost for failed certificate management practices

The research reveals the seriousness and cost of the following five cybersecurity risks created by ineffective key or certificate management problems. For the following five scenarios, respondents were asked to estimate operational and compliance costs, the cost of security exploits and the likelihood they will occur over the next two years:

- The cost of unplanned outages due to certificate expiration is estimated to average $11.1 million, and there is a 30 percent likelihood organizations will experience these incidents over the next two years.

- The cost of failed audits or compliance due to undocumented or unenforced key management policies or insufficient key management practices is estimated to average $14.4 million, and there is a 42 percent likelihood that organizations will experience these incidents over the next two years.

- The cost of server certificate and key misuse is estimated to average $13.4 million, and there is a 39 percent likelihood that organizations will experience these incidents over the next two years.

- The cost of code signing certificate and key misuse is estimated to average $15 million, and there is a 29 percent likelihood that organizations will experience these incidents over the next two years.

- The cost of Certificate Authority (CA) compromise or rogue CA for man-in-the-middle (MITM) and phishing attacks is estimated to average $13.2 million, and there is a 38 percent likelihood that organizations will experience these incidents over the next two years.

Based on respondents' estimates, **the average total cost to a single company if all five scenarios occurred would be $67.2 million over a two-year period**. The costliest scenarios would be code signing certificate and key misuse and failed audits or compliance due to undocumented or unenforced key management policies or insufficient key management practices (an average of $15 million and $14.4 million, respectively). The research also reveals how likely these scenarios are to occur and how many times organizations represented in the study have experienced these attacks over a period of 24 months.

Part 2. Key Findings

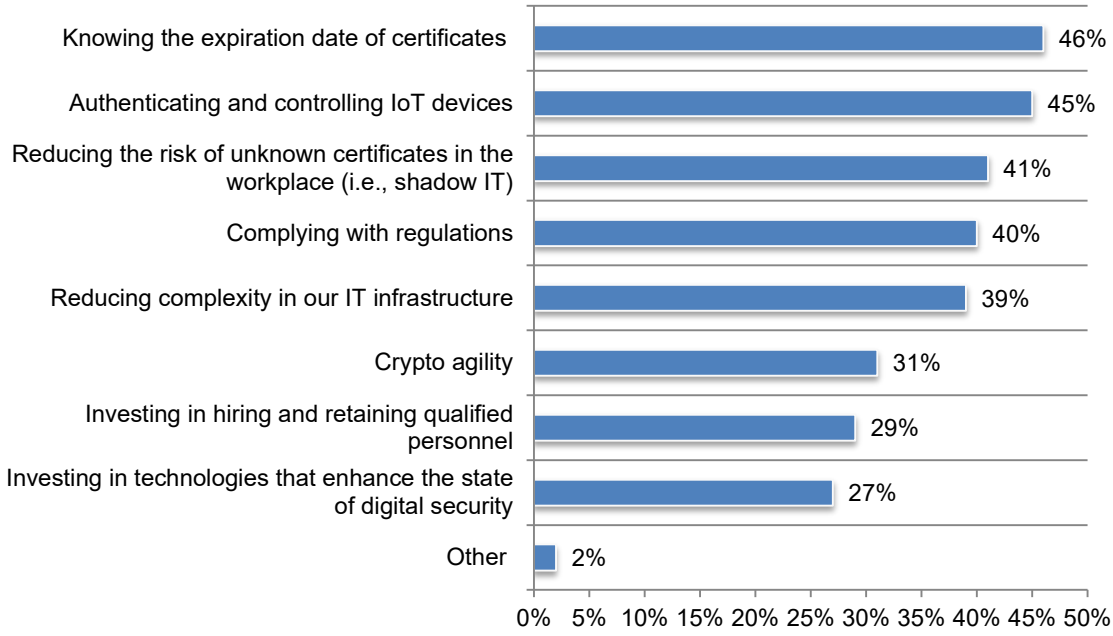
In this section, we present an analysis of the key findings. The complete audited findings are presented in the Appendix of this report. The findings are organized by the following themes:

- Challenges in managing certificates
- Steps taken to improve the security of digital identities
- Total cost for failed certificate management practices
- Conclusion

Challenges in managing certificates

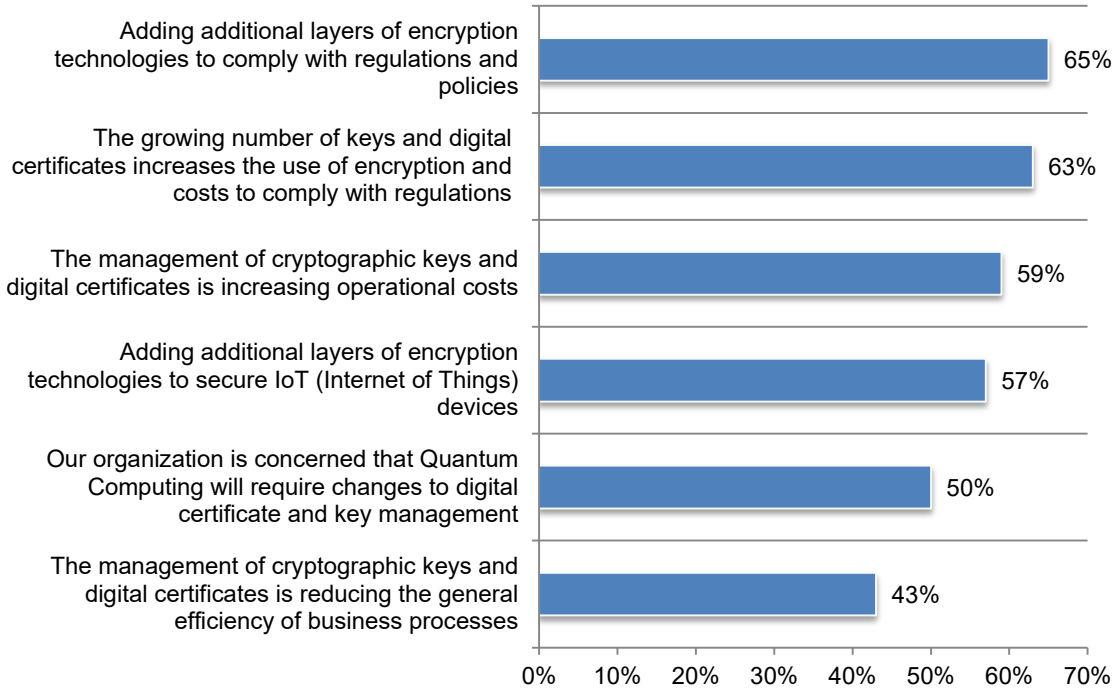
The top priorities in minimizing the risk of unsecured digital identities is to know the expiration date of certificates and to secure IoT devices. As shown in Figure 2, respondents believe their organizations need to address the risks created by not knowing the expiration date of certificates and controlling IoT devices, according to 46 percent and 45 percent of respondents, respectively. Also important is the reduction in the risk of unknown certificates in the workplace and compliance with regulations such as PCI-DSS, HYTRUST, HITECH, California Privacy Act and the EU General Data Protection Regulation (GDPR).

Figure 2. What are your strategic priorities for digital security within your organization?
Three responses permitted



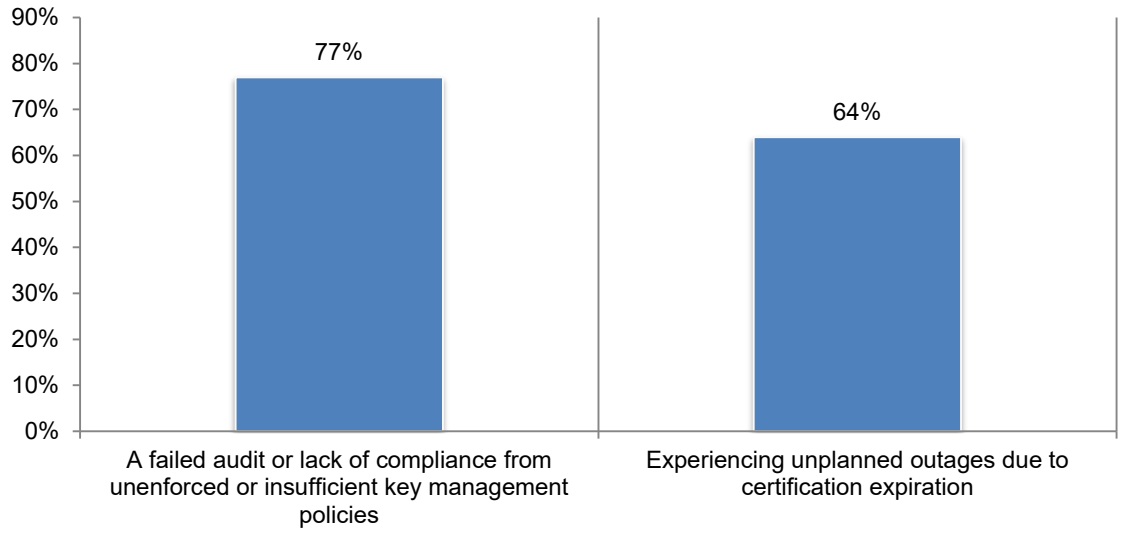
The growing number of digital certificates is increasing operational costs. As shown in Figure 3, the growing number of keys and digital certificates that companies must maintain is increasing their use of encryption. As a result, organizations are incurring higher costs, according to 63 percent of respondents. **Fifty-nine percent of respondents say the management of cryptographic keys and digital certificates is also increasing operational costs.** Another risk to digital certificates is the difficulty to secure keys and certificates throughout all stages of their lifecycle--from generation, request, renewal, rotation to revocation.

Figure 3. Perceptions about the state of certificate management
Strongly agree and Agree responses combined



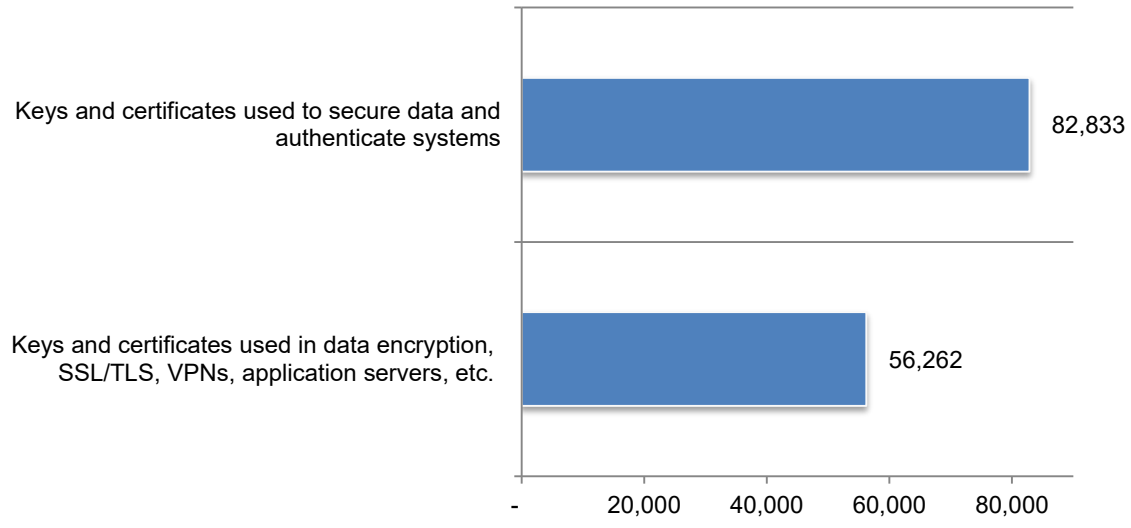
Failed audits and unplanned outages are considered very serious problems for organizations. Respondents were asked to rate the seriousness of two risks caused by the mismanagement of digital certificates from a scale of 1 = not serious to 10 = very serious. As shown in Figure 4, 77 percent of respondents say a failed audit or lack of compliance from unenforced or insufficient key management policies is a serious issue, and 64 percent say having unplanned outages due to certification expiration is also a concern. As will be discussed later, these risks are the threats most likely to occur frequently making them very costly for organizations.

Figure 4. Seriousness of the risk of unsecured digital certificates
From 1 = not serious to 10 = very serious, 7+ responses reported



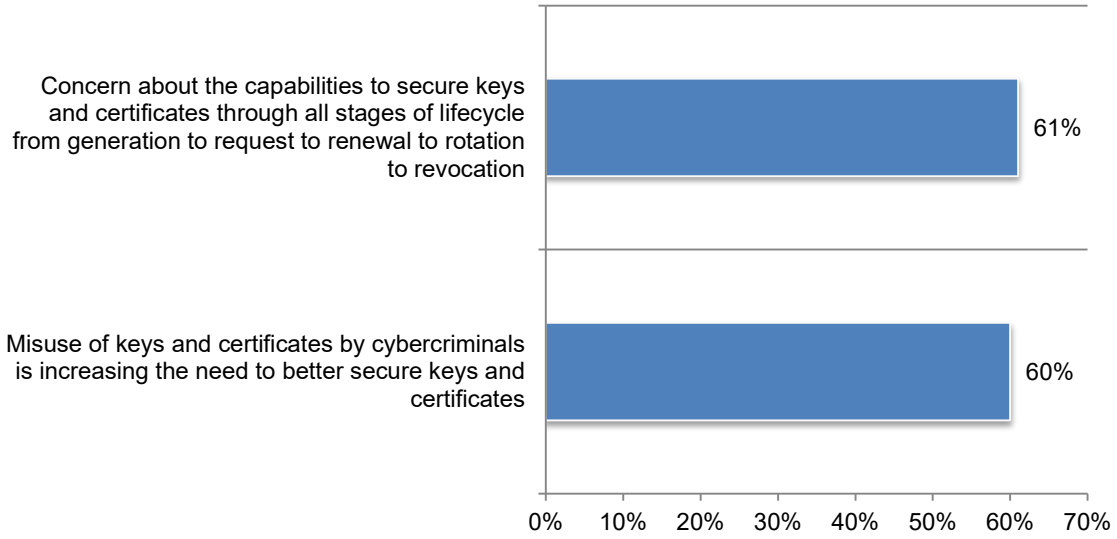
Organizations have difficulty in determining the number of keys and certificates in use. Respondents were asked to estimate the number of keys and certificates currently in use. As shown in Figure 5, the average number of keys and certificates used to secure data and authenticate systems is 82,833 and the average number of keys and certificates used in data encryption, SSL/TLS, VPNs, application services is just over 56,000.

Figure 5. The average number of keys and certificates used to secure data and authenticate systems
Extrapolated values presented



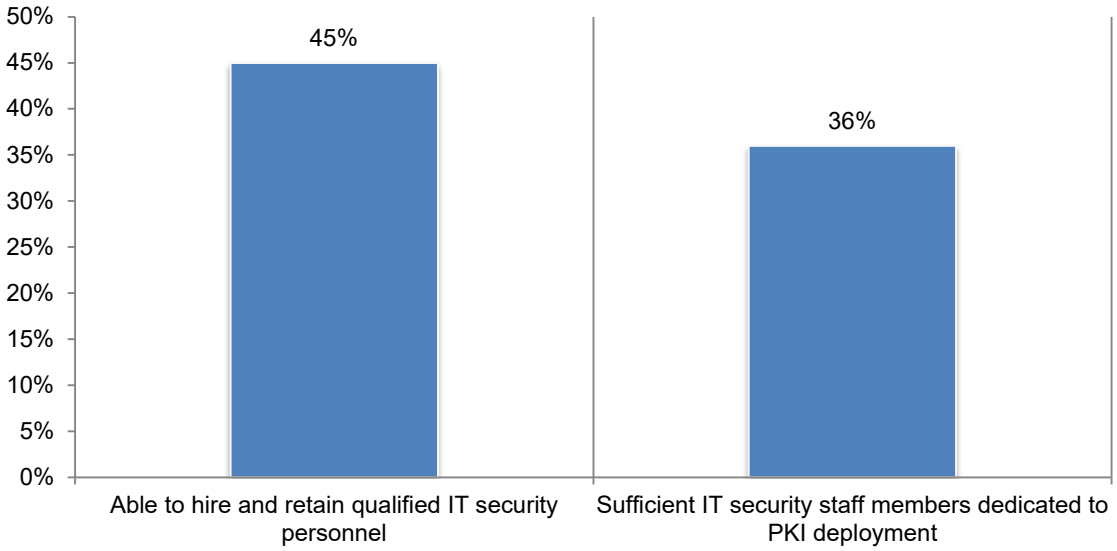
Most organizations are concerned about their ability to secure keys and certificates. According to Figure 6, 61 percent of respondents say their organizations are concerned about the capabilities to secure keys and certificates throughout all stages of their lifecycle from generation to revocation. Sixty percent of respondents say the misuse of keys and certificates by cybercriminals is increasing the need to better secure keys and certificates.

Figure 6. Security concerns
Strongly agree and Agree responses combined



Hiring and retaining IT security personnel is a challenge to securing digital certificates. According to Figure 7, only **45 percent of respondents say their organizations are able to hire and retain qualified IT security personnel**. As a consequence, only 36 percent of respondents say their organizations have sufficient IT security staff members dedicated to PKI deployment.

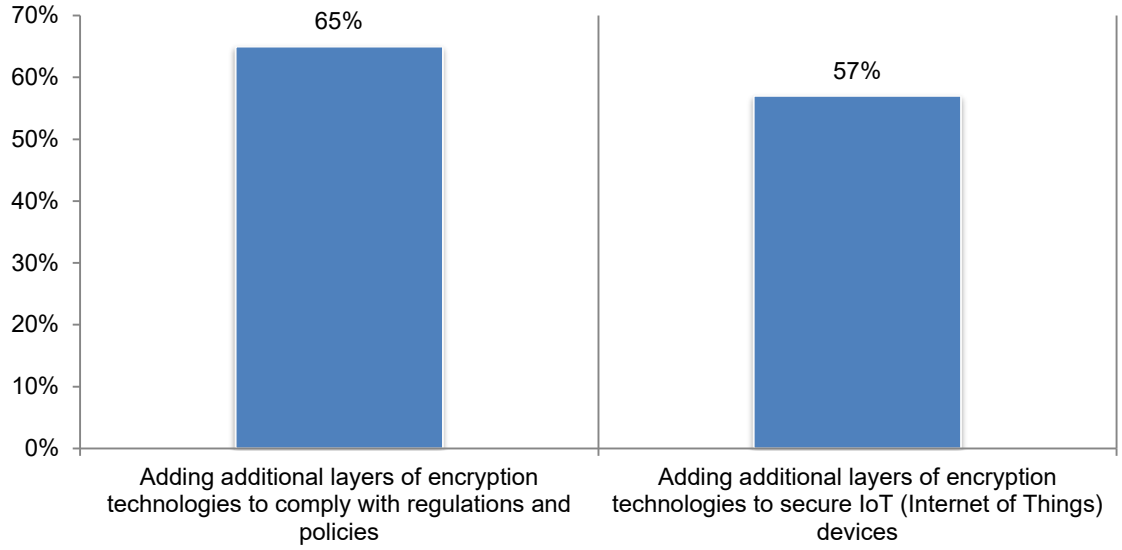
Figure 7. Challenges in staffing IT security
Yes responses presented



Steps taken to improve the security of digital identities

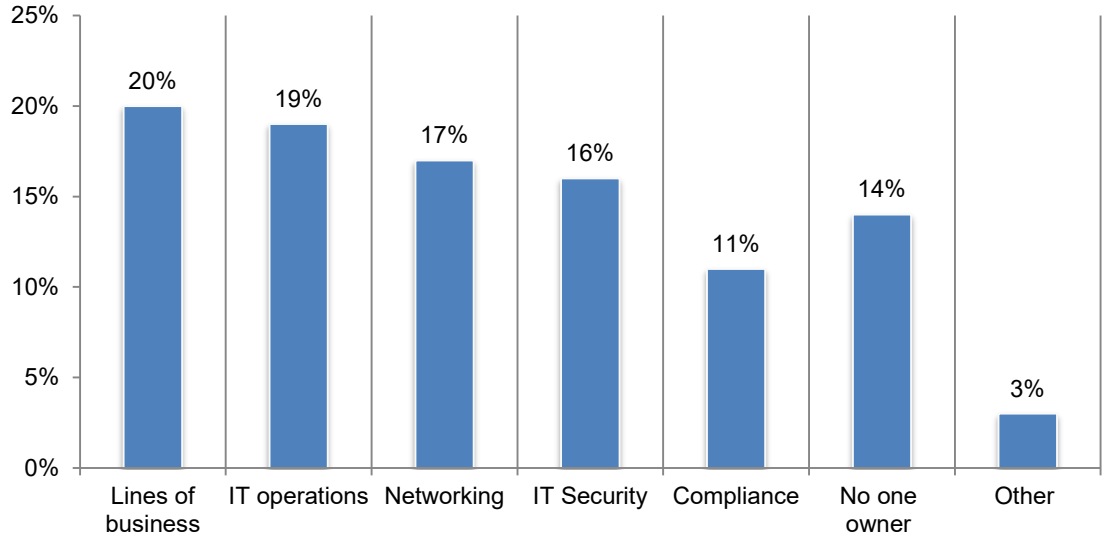
To strengthen the security of keys and digital certificates, many organizations are adding additional layers of encryption. According to Figure 8, 65 percent of respondents say their organizations are adding additional layers of encryption technologies to comply with regulations and policies and **57 percent of respondents say these added layers of encryption are used to secure IoT devices**.

Figure 8. Steps taken to comply with regulations and the IoT
Strongly agree and Agree responses combined



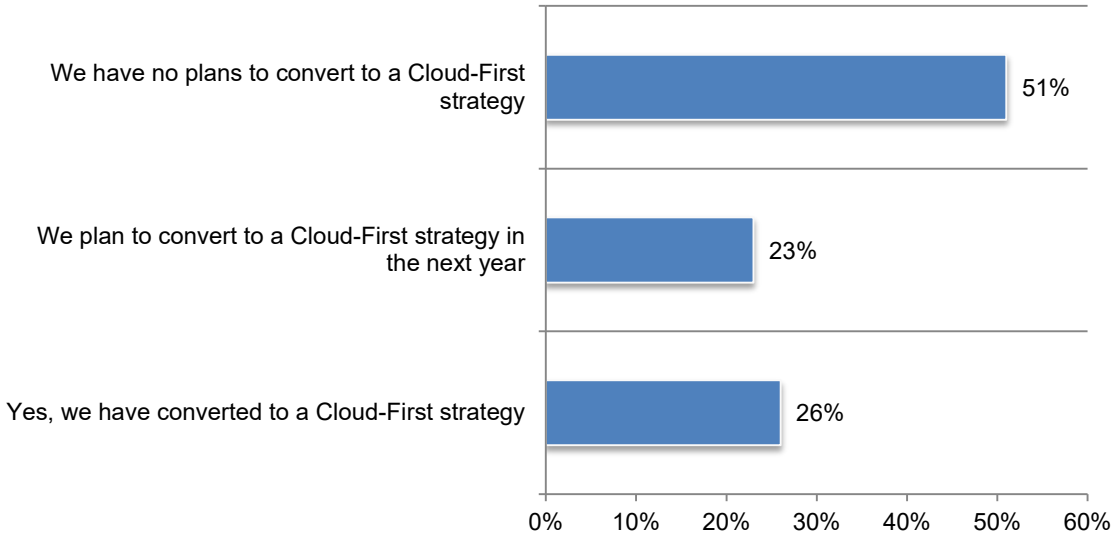
Responsibility for the PKI budget is dispersed throughout the organization. Organizations represented in the study are spending an average of $18.2 million on IT security annually and an average of 14 percent of the budget or approximately $2.5 million on the PKI budget. According to Figure 9, **no one function emerges as the clear owner of the PKI budget.** Twenty percent of respondents say it is the lines of business and 19 percent of respondents say it is IT operations.

Figure 9 Who owns the PKI budget?



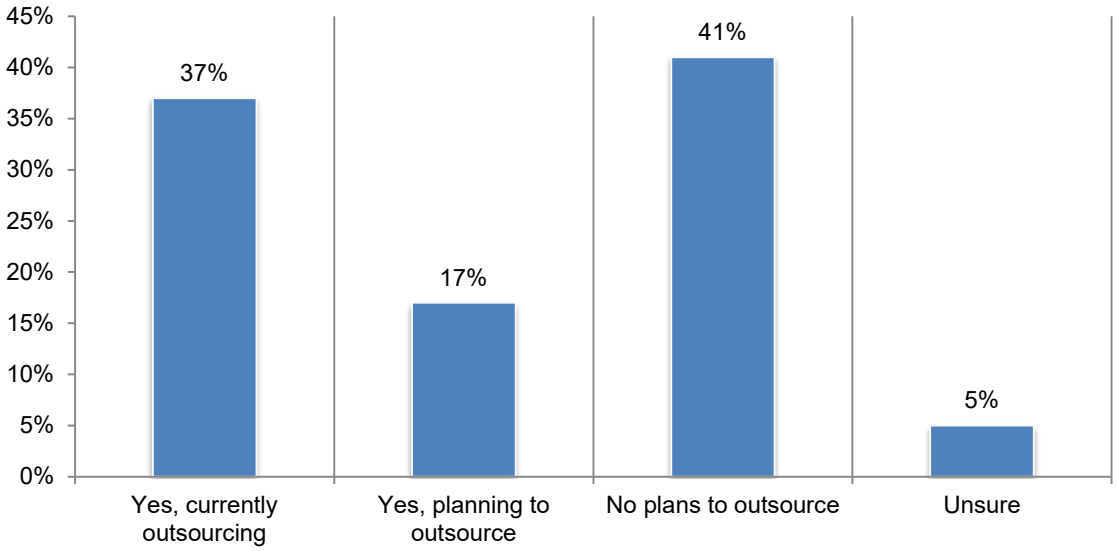
PKI deployment is included in organizations' Cloud-First strategy. Seventy-five percent of respondents say they are familiar with Cloud First and almost half of these respondents (49 percent) say their organizations have converted or plan to convert to a Cloud-First strategy, as shown in Figure 10. Sixty-four percent of respondents in organizations with a Cloud-First strategy say it will include PKI deployment.

Figure 10. Have you or will you be converting to a Cloud-First strategy?



The majority of organizations are or will outsource all or part of its PKI deployment. As the data tells us, organizations are significantly understaffed to deal with PKI deployment and have or are considering outsourcing all or part of its PKI deployment. According to Figure 11, **55 percent of respondents say their organizations are currently outsourcing (37 percent) or planning to outsource their PKI deployment.**

Figure 11. Would your organization consider outsourcing all or part of its PKI deployment?



Total cost for failed certificate management practices

For purposes of estimating the costs of key and certificate compromise, operations, and compliance, respondents were asked to refer to the following cost categories as they relate to the five scenarios. The cost estimate includes all direct cash outlays, direct labor expenditures, indirect labor costs, overhead costs, and lost business opportunities.

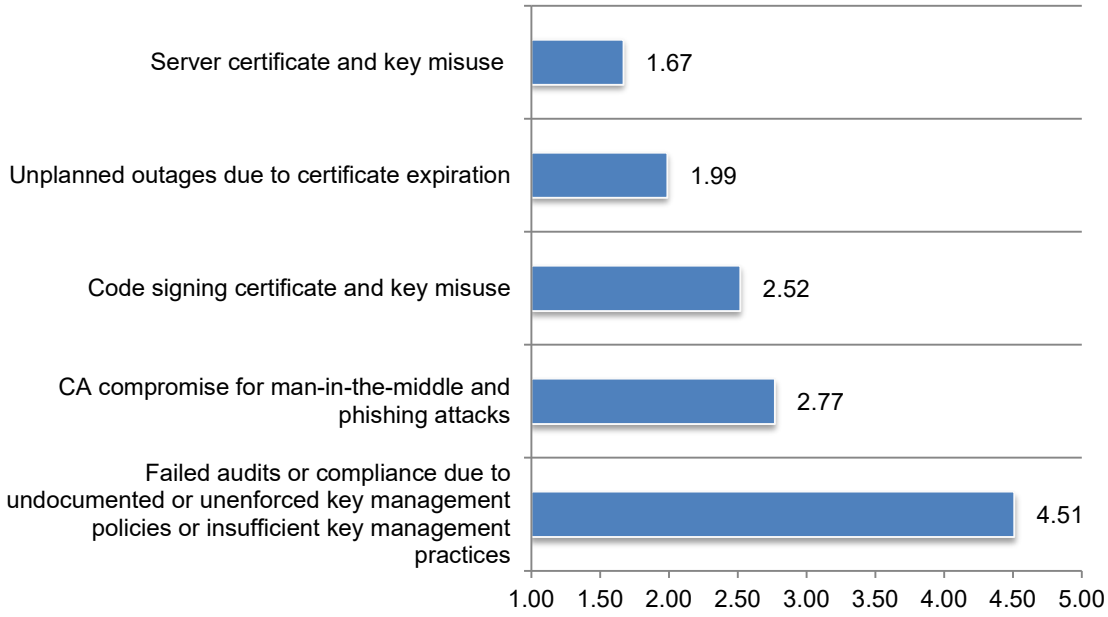
- Cost of technical support including system administration, help desk, and customer service operations
- Cost of users' idle time and lost productivity because of downtime or system performance delays
- Revenues lost because of system availability problems
- Cost associated with reputation and brand damage because of system failure and heightened security risks

The following is a summary of the total cost of the five categories over a two-year period. As shown in Table 1, the total cost if all five scenarios occurred is $67.2 million. **The costliest scenarios are code signing certificate and key misuse and failed audits or compliance due to undocumented or unenforced key management policies or insufficient key management practices** ($15,025,150 and $14,411,500).

Table 1. Total cost for five scenarios	**Extrapolated Cost**
The cost of unplanned outages due to certificate expiration	$11,122,100
Failed audits or compliance due to undocumented or unenforced key management policies or insufficient key management practices	$14,411,500
Server certificate and key misuse	$13,423,250
Code signing certificate and key misuse	$15,025,150
Certificate Authority (CA) compromise or rogue CA for man-in-the-middle (MITM) and phishing attacks	$13,219,850
Total	**$67,201,850**

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 12, the least serious problem is server certificate and key misuse and the most serious problem is a failed audit or compliance miss because of undocumented or unenforced key management policies or insufficient key management practices. **Failed audits are also the most frequent cyber threat experienced.**

Figure 12. How serious is the problem of cybersecurity threats caused by key or certification management problems?
From 1 = least serious problem to 5 = most serious problem



Scenario 1. Unplanned outages due to certificate expiration. Whether by oversight or lack of knowledge, certificates expire. At best, this can cause user confusion and, at worst, systems that stop working completely. Among other things, outages can lead to lost orders, stopped production, SLA violations, and brand damage. As shown in Table 2, **respondents estimate that they experienced an average of four unplanned outages due to certificate expiration in the past two years and the average cost for these events was $11.1 million.** There is a 30 percent likelihood that organizations will experience these events over the next two years.

Table 2. Unplanned outages due to certificate expiration	**Extrapolated Cost**
How many times has this occurred during the past 24 months	4.01
The likelihood this will occur over the next 24 months	30%
Cost due to system administration, replacement of certificates and keys to maintain compliance, help desk and customer support time	$1,987,150
Cost due to lost user productivity	$2,439,550
Cost due to diminished productivity of the IT security team	$2,074,650
Cost due to immediate revenue loss	$2,999,700
Cost due to diminished brand or reputation	$1,621,050
Total	**$11,122,100**

Scenario 2. Failed audits or compliance due to undocumented or unenforced key management policies or from insufficient key management practices. When there are no controls over how administrators generate keys (for data encryption, SSL/TLS, etc.) or request digital certificates, they are likely to violate IT policies. Administrators might create keys with too short key lengths, use unauthorized certificate authorities or fail to enter corporate data correctly into certificate requests. When audited, external auditors will fail organizations for these and other key and certificate policy violations.

Regulators are beginning to make explicit references to key management. PCI-DSS, HYTRUST, HITECH, state breach regulations, and other data protection rules along with best practices from organizations such as NIST now specify or demand key management requirements. For example, when the ICO (UK's primary data protection authority) issued its guidance on cloud computing, it stated "robust key management" was required. As a result, external and internal auditors are closely evaluating key management policies for applications such as data encryption, SSL, etc. Some organizations have already failed audits and had deadlines imposed for remediation while others have been put on notice.

As shown in Table 3, **respondents estimate that they experienced an average of more than five failed audits or compliance in the past two years and the average cost for these events was $14.4 million**. **There is a 42 percent likelihood that these incidents will occur over the next two years.**

Table 3. Failed audits or compliance due to undocumented or unenforced key management policies or from insufficient key management practices	**Extrapolated Cost**
How many times has this occurred during the past 24 months	5.49
The likelihood this will occur over the next 24 months	42%
Cost due to system administration, replacement of certificates and keys to maintain compliance, help desk and customer support time	$2,738,150
Cost due to lost user productivity	$3,093,050
Cost due to diminished productivity of the IT security team	$3,617,150
Cost due to immediate revenue loss	$2,057,550
Cost due to diminished brand or reputation	$2,905,600
Total	**$14,411,500**

Scenario 3. Server certificate and key misuse. To impersonate public websites, application servers, and trusted networks, attackers steal keys and certificates. An example includes the theft of a bank's certificate operated by a third party, which contributed to one of the largest financial institution breaches of all time.

Attackers seeking to gain access to the most sensitive backend or cloud systems target the theft of cryptographic keys used by servers, load balancers, and application servers to communicate with each other. These trusted keys (and their associated certificates) can now be used by attackers to connect at will to other systems that fully trust the connecting system. Attackers can now access sensitive databases or submit false transactions. Uncertain of which key may have been stolen, an organization must generate all new keys and certificates across hundreds or thousands of systems taking thousands of man-hours for remediation.

As shown in Table 4, **respondents estimate that they experienced an average of between four and five server certificate and key misuse occurrences in the past two years and the average cost for these events was $13.4 million.** There is a 39 percent likelihood that organizations will experience such an incident over the next two years.

Table 4. Server certificate and key misuse	**Extrapolated Cost**
How many times has this occurred during the past 24 months	4.60
The likelihood this will occur over the next 24 months	39%
Cost due to system administration, replacement of certificates and keys to maintain compliance, help desk and customer support time	$2,699,900
Cost due to lost user productivity	$2,418,650
Cost due to diminished productivity of the IT security team	$1,522,050
Cost due to immediate revenue loss	$2,435,050
Cost due to diminished brand or reputation	$4,317,600
Total	**$13,423,250**

Scenario 4. Code signing certificate and key misuse. There is a growing interest in the cybercriminal community in code signing certificates. Attackers sign malicious code (malware) to avoid detection of current security controls. Most organizations are not able to track or detect this emerging threat.

As an example, Equifax had allowed over 300 security certificates to expire, including 79 certificates for monitoring business critical domains. Equifax did not see the data exfiltration, because the device used to monitor ACIS network traffic had been inactive for 19 months due to an expired security certificate. On July 29, 2017, Equifax updated the expired certificate and immediately noticed suspicious web traffic.

As shown in Table 5, **respondents estimate that their organizations experienced an average of almost 4 incidents involving code signing certificate and key misuse in the past two years and the average cost for these events was $15 million-making it the costliest of the five incidents**. There is a 29 percent likelihood that organizations will experience such an incident over the next two years.

Table 5. Code signing certificate and key misuse	**Extrapolated Cost**
How many times has this occurred during the past 24 months	3.93
The likelihood this will occur over the next 24 months	29%
Cost due to system administration, replacement of certificates and keys to maintain compliance, help desk and customer support time	$3,715,550
Cost due to lost user productivity	$3,318,350
Cost due to diminished productivity of the IT security team	$1,927,750
Cost due to immediate revenue loss	$2,346,400
Cost due to diminished brand or reputation	$3,717,100
Total	**$15,025,150**

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

To impersonate public websites, application servers, and trusted networks, attackers infiltrate a public or internal CA and issue unauthorized certificates. Now all certificates issued by the CA are suspect and must be revoked because they no longer have value. As a result, organizations must immediately find other bona fide CAs and reissue new certificates.

Attackers look to impersonate organizations such as Google and Facebook. These attacks affect all organizations not just the ones being targeted because their certificates are trusted by operating systems, browsers, and other applications globally. Similar compromises on internal CAs to either impersonate or disrupt organizations have occurred but have gone unreported.

In 2013, one notable man-in-the-middle attack involved Nokia's Xpress Browser decrypting HTTPS traffic on Nokia's proxy servers, giving the company clear text access to its customers' encrypted browser traffic. According to Nokia, the content was not stored permanently, and the company had organizational and technical measures to prevent access to private information.

As shown in Table 6, **respondents estimate that they experienced an average of approximately two CA compromises or rogue CA for man-in-the-middle and phishing attacks in the past two years and the average cost for these two events was $13.2 million**. There is a 38 percent likelihood that organizations will experience such an incident over the next two years.

Table 6. CA compromise or rogue CA for man-in-the-middle and phishing attacks	**Extrapolated Cost**
How many times has this occurred during the past 24 months	2.26
The likelihood this will occur over the next 24 months	38%
Cost due to system administration, replacement of certificates and keys to maintain compliance, help desk and customer support time	$2,000,900
Cost due to lost user productivity	$3,171,100
Cost due to diminished productivity of the IT security team	$1,927,750
Cost due to immediate revenue loss	$2,637,450
Cost due to diminished brand or reputation	$3,482,650
Total	**$13,219,850**

Conclusion

Sixty-one percent of companies represented in this study are not confident they are able to secure keys and certificates throughout all stages of their lifecycle from generation to revocation. The finding underscores the importance of an audit cadence, awareness of certificate expiration dates, as well as understanding of how and where certificates are being used.

According to respondents, an average of more than 48,000 digital certificates are used to encrypt data and authenticate servers and/or domains. However, most organizations, according to the respondents, do not know exactly how many keys and certificates they have. Companies are also failing to know how many expired digital certificates they have. **The solution is to put processes and technologies in place to proactively manage certificates and keys in the enterprise, on mobile devices, and in the cloud**. These processes should include controlling how administrators generate keys or request digital certificates and establishing and enforcing policies regarding the use of authorized certificate authorities.

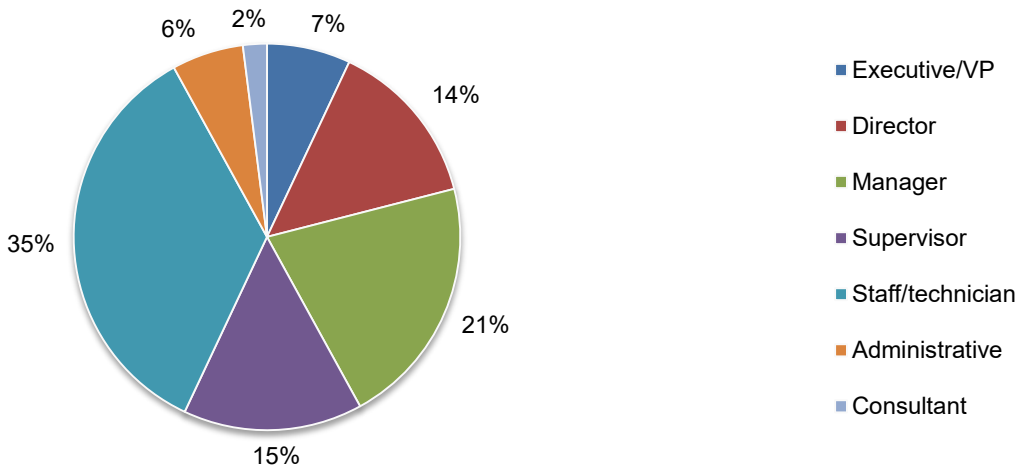
Part 3. Methods

The sampling frame is composed of 17,570 IT and IT security practitioners in the United States. All respondents are familiar with their companies' strategy for the protection of digital identities. As shown in Table 7, 654 respondents completed the survey. Screening removed 58 surveys. The final sample was 596 surveys (or a 3.4 percent response rate).

Table 7. Sample response	Freq	Pct%
Total sampling frame	17,570	100.0%
Total returns	654	3.7%
Rejected or screened surveys	58	0.3%
Final sample	596	3.4%

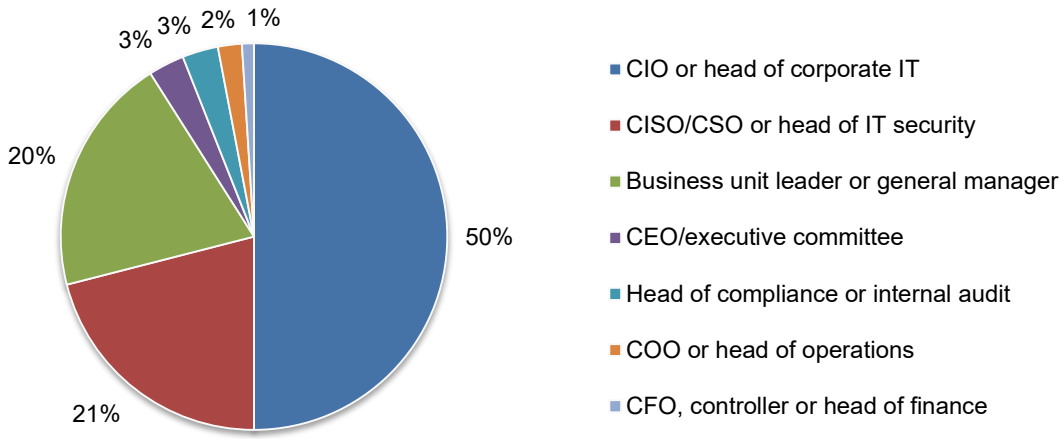
Pie Chart 1 reports the current position or organizational level of the respondents. More than half of respondents (57 percent) reported their current position as supervisory or above and 35 percent of respondents are at the staff/technician level.

Pie Chart 1. Distribution of respondents according to position level



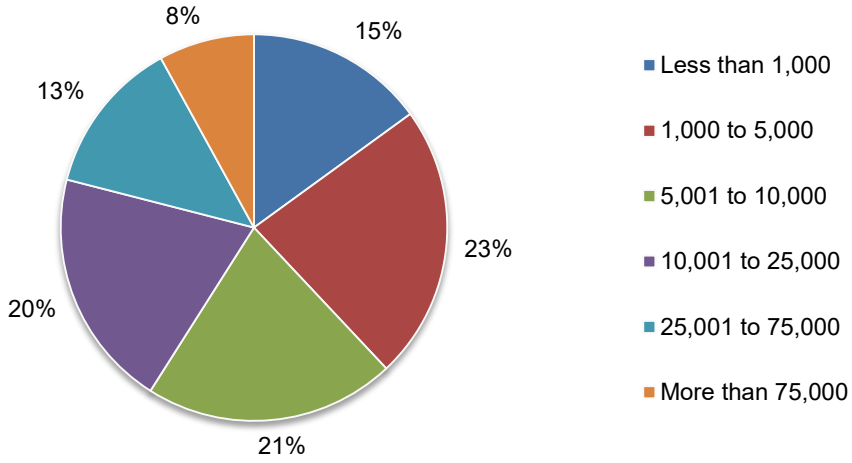
Pie Chart 2 identifies the primary person to whom the respondent or their IT security leader reports. Fifty percent of respondents identified the CIO or head of corporate IT as the person to whom they report. Another 21 percent indicated they report directly to the CISO/CSO or head of IT security and 20 percent of respondents report to the business unit leader or general manager.

Pie Chart 2. Distribution of respondents according to reporting channel



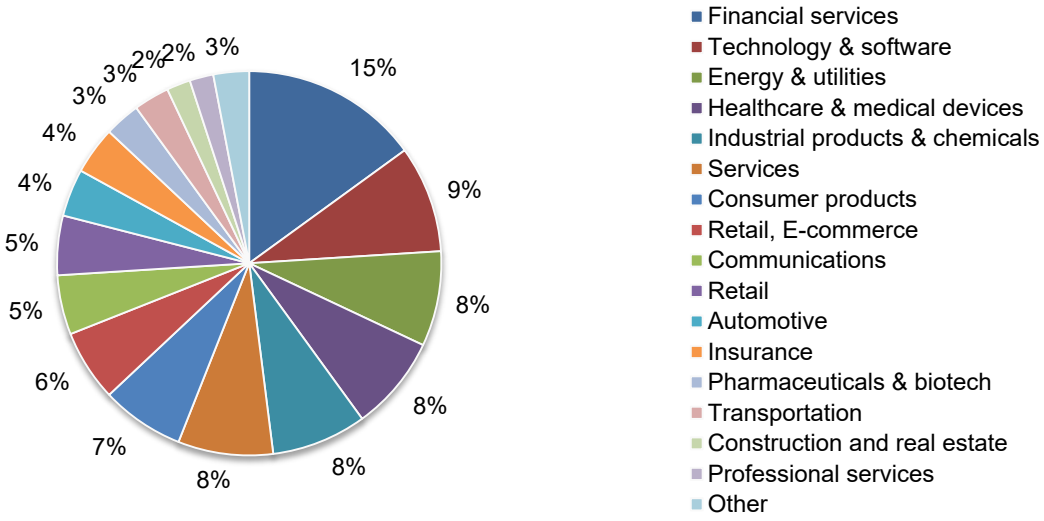
According to Pie Chart 3, more than half of the respondents (62 percent) are from organizations with a global head count of more than 5,000 employees.

Pie Chart 3. Distribution of respondents according to organizational head count



Pie Chart 4 reports the primary industry classification of respondents' organizations. This chart identifies financial services (15 percent of respondents) as the largest segment, followed by technology and software (9 percent of respondents), energy and utilities, healthcare and medical devices, industrial products and chemicals, and services sector (each at 8 percent of respondents).

Pie chart 4. Distribution of respondents according to primary industry classification



Part 4. Caveats

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 the United States. 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

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 October 15, 2018 to November 5, 2018.

Survey response	Freq	Pct%
Total sampling frame	17,570	100.0%
Total returns	654	3.7%
Total rejected surveys	58	0.3%
Final sample	596	3.4%

Please rate the following 15 statements using the five-point scale provided below each item. **Strongly Agree and Agree responses combined.**	Pct%
Q1a. My organization is adding additional layers of encryption (such as data encryption, SSL/TLS, etc.) technologies to comply with regulations and policies.	65%
Q1b. My organization is adding additional layers of encryption (such as data encryption, SSL/TLS, etc.) technologies to secure IoT (Internet of Things) devices.	57%
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.	59%
Q1e. The management of cryptographic keys (for data encryption, SSL/TLS, etc.) and digital certificates is reducing the general efficiency of business processes.	43%
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.	61%
Q1g. My organization does not know exactly how many keys and certificates (including self-signed) it has.	71%
Q1h. In my organization, digital certificates have caused and still cause unanticipated downtime or outages.	74%
Q1i. Failing to secure keys and certificates undermines the trust my organization relies upon to operate.	73%
Q1j. Misuse of keys and certificates by cybercriminals is increasing the need for my organization to better secure keys and certificates.	60%
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.	50%

Q2. Do you believe your organization has lost customers because of outages due to problems with keys and certificates?	Pct%
Yes	63%
No	27%
Unsure	10%
Total	100%

Q3. Is your organization a Certificate Authority (CA)	Pct%
Yes	61%
No	35%
Unsure	4%
Total	100%

Q4. Please rank the following five cyber security threats caused by key or certification management problems in your organization. Here, 1 = least serious problem to 5 = most serious problem.	Average Rank	Rank Order
Unplanned outages due to certificate expiration	1.99	2
Failed audits or compliance due to undocumented or unenforced key management policies or insufficient key management practices	4.51	5
Server certificate and key misuse	1.67	1
Code signing certificate and key misuse	2.52	3
CA compromise for man-in-the-middle and phishing attacks	2.77	4

Q5. How many IT security staff members are dedicated to PKI deployment?	Pct%
None	4%
One	16%
2 to 5	47%
6 to 10	19%
11 to 20	10%
More than 20	4%
Total	100%
Extrapolated value	5.88

Q6. Does your organization have enough IT security staff members dedicated to PKI deployment?	Pct%
Yes	36%
No	64%
Total	100%

Q7. Is your organization able to hire and retain qualified IT security personnel?	Pct%
Yes	45%
No	55%
Total	100%

Q8. How much does your organization spend annually on IT security?	Pct%
Less than $1 million	0%
$1 to 5 million	5%
$6 to $10 million	16%
$11 to $15 million	30%
$16 to $20 million	23%
$21 to $25 million	15%
$26 to $50 million	6%
More than $50 million	5%
Total	100%
Extrapolated value (millions)	$ 18.20

Q9. What percentage of the IT security budget is allocated to PKI deployment annually?	Pct%
Less than 5%	6%
5% to 10%	29%
11% to 20%	44%
More than 20%	21%
Total	100%
Extrapolated value	14%

Q10. Who owns the PKI budget?	Pct%
IT Security	16%
IT operations	19%
Networking	17%
Compliance	11%
Lines of business	20%
No one owner (shared)	14%
Other (please specify)	3%
Total	100%

Q11. How familiar are you with the term Cloud First?	Pct%
Very familiar	31%
Familiar	44%
Not familiar (please skip to Q14)	25%
Total	100%

Q12. If yes, have you or will you be converting to a Cloud First strategy?	Pct%
Yes, we have converted to a Cloud First strategy	26%
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	51%
Total	100%

Q13. If yes, does your current Cloud First strategy include PKI deployment?	Pct%
Yes	64%
No	36%
Total	100%

Q14. Would your organization consider outsourcing all or part of its PKI deployment?	Pct%
Yes, currently outsourcing	37%
Yes, planning to outsource	17%
No plans to outsource	41%
Unsure	5%
Total	100%

Q15. Are you using certificates to secure containers (i.e. Docker, etc.)?	Pct%
Yes	49%
No	51%
Total	100%

Q16. What are your strategic priorities for digital security within your organization? Please select your top 3 choices.	Pct%
Crypto agility	31%
Complying with regulations	40%
Reducing the risk of unknown certificates in the workplace (i.e. shadow IT)	41%
Knowing the expiration date of certificates	46%
Investing in technologies that enhance the state of digital security	27%
Investing in hiring and retaining qualified personnel	29%
Reducing complexity in our IT infrastructure	39%
Authenticating and controlling IoT devices	45%
Other (please specify)	2%
Total	300%

Q17. 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?	Pct%
Less than 1,000	3%
1,00 to 5,000	12%
5,001 to 10,000	35%
10,001 to 50,000	25%
51,000 to 100,000	17%
101,000 to 500,000	6%
500,000 to 1,000,000	2%
More than 1,000,000	0%
Total	100%
Extrapolated value	56,262

Q18. How many keys and certificates do you believe are in use by your organization today to secure data and authenticate systems?	Pct%
Less than 1,000	2%
1,00 to 5,000	8%
5,001 to 10,000	21%
10,001 to 50,000	25%
51,000 to 100,000	30%
101,000 to 500,000	12%
500,000 to 1,000,000	2%
More than 1,000,000	0%
Total	100%
Extrapolated value	82,833

Part 2. Estimating operational and compliance costs and the cost of security exploits

Scenario 1. Unplanned outages due to certificate expiration	
Q19. Using the following 10-point scale, please rate the seriousness of experiencing unplanned outages due to certification expiration 1 = not serious to 10 = very serious.	Pct%
1 to 2	2%
3 to 4	10%
5 to 6	24%
7 or 8	20%
9 or 10	44%
Total	100%
Extrapolated value	7.38

Q20a-1. How many times has this issue occurred in your organization during the **past 24 months**?	Pct%
Zero	12%
1 time	6%
2 times	8%
3 times	20%
4 times	26%
5 times	13%
More than 5 times	15%
Total	100%
Extrapolated value	4.01

Q20a-2. What is the likelihood that this issue will occur in your organization over the next 24 months?	Pct%
Less than 5%	9%
5% to 10%	5%
11% to 15%	6%
16% to 20%	20%
21% to 30%	21%
31% to 40%	10%
41% to 50%	11%
More than 50%	18%
Total	100%
Extrapolated value	0.30

Q21a. Approximately, how much would this incident cost your organization in terms of system administrator, help desk and customer support time responding to this issue?	Pct%
Less than $10,000	0%
$10,001 to $100,000	13%
$100,001 to $250,000	21%
$250,001 to $500,000	19%
$500,001 to $1,000,000	16%
$1,000,001 to $5,000,000	23%
$5,000,001 to $10,000,000	5%
$10,000,001 to $25.000,000	2%
$25,000,001 to $50,000,000	1%
$50,00,001 to $100,000,000	0%
More than $100,000,000	0%
Total	100%
Extrapolated value	$1,987,150

Q21b. Approximately, how much would this incident cost your organization in terms of lost user productivity?	Pct%
Less than $10,000	0%
$10,001 to $100,000	11%
$100,001 to $250,000	12%
$250,001 to $500,000	20%
$500,001 to $1,000,000	23%
$1,000,001 to $5,000,000	21%
$5,000,001 to $10,000,000	9%
$10,000,001 to $25.000,000	3%
$25,000,001 to $50,000,000	1%
$50,00,001 to $100,000,000	0%
More than $100,000,000	0%
Total	100%
Extrapolated value	$2,439,550

Q21c. Approximately, how much would this incident cost your organization in terms of diminished productivity of the IT security team?	Pct%
Less than $10,000	0%
$10,001 to $100,000	13%
$100,001 to $250,000	11%
$250,001 to $500,000	29%
$500,001 to $1,000,000	23%
$1,000,001 to $5,000,000	15%
$5,000,001 to $10,000,000	6%
$10,000,001 to $25.000,000	1%
$25,000,001 to $50,000,000	2%
$50,00,001 to $100,000,000	0%
More than $100,000,000	0%
Total	100%
Extrapolated value	$2,074,650

Q21d. Approximately, how much would this incident cost your organization in terms of immediate revenue loss?	Pct%
Less than $10,000	2%
$10,001 to $100,000	12%
$100,001 to $250,000	14%
$250,001 to $500,000	12%
$500,001 to $1,000,000	23%
$1,000,001 to $5,000,000	25%
$5,000,001 to $10,000,000	5%
$10,000,001 to $25.000,000	3%
$25,000,001 to $50,000,000	1%
$50,00,001 to $100,000,000	1%
More than $100,000,000	0%
Total	98%
Extrapolated value	$2,999,700

Q21e. Approximately, how much would this incident cost your organization in terms of diminished brand or reputation?	Pct%
Less than $10,000	3%
$10,001 to $100,000	8%
$100,001 to $250,000	17%
$250,001 to $500,000	11%
$500,001 to $1,000,000	31%
$1,000,001 to $5,000,000	27%
$5,000,001 to $10,000,000	2%
$10,000,001 to $25.000,000	0%
$25,000,001 to $50,000,000	1%
$50,00,001 to $100,000,000	0%
More than $100,000,000	0%
Total	100%
Extrapolated value	$1,621,050

Scenario 1 recap	Total
Cost of system administrator, help desk and customer support time	$1,987,150
Cost of lost user productivity	$2,439,550
Cost of diminished productivity of the IT security team	$2,074,650
Cost of immediate revenue loss	$2,999,700
Cost your organization in terms of diminished brand or reputation	$1,621,050
Total	$11,122,100

Scenario 2. Failed audits or compliance due to undocumented or unenforced key management policies or from insufficient key management practices:	
Q22. Using the following 10-point scale, please rate the seriousness of a failed audit or lack of compliance from unenforced or insufficient key management policies 1 = not serious to 10 = very serious.	Pct%
1 to 2	1%
3 to 4	7%
5 to 6	15%
7 or 8	34%
9 or 10	43%
Total	100%
Extrapolated value	7.72

Q23a-1. How many times has this occurred in your organization during the **past 24 months**?	Pct%
Zero	4%
1 time	6%
2 times	9%
3 times	8%
4 times	14%
5 times	29%
More than 5 times	30%
Total	100%
Extrapolated value	5.49

Q23a-2. What is the likelihood this will occur in your organization over the **next 24 months**?	Pct%
Less than 5%	4%
5% to 10%	3%
11% to 15%	6%
16% to 20%	5%
21% to 30%	8%
31% to 40%	11%
41% to 50%	23%
More than 50%	40%
Total	100%
Extrapolated value	0.42

Q24a. Approximately, how much would this incident cost your organization in terms of system administrator, help desk and customer support time responding to this issue?	Pct%
Less than $10,000	0%
$10,001 to $100,000	8%
$100,001 to $250,000	11%
$250,001 to $500,000	14%
$500,001 to $1,000,000	38%
$1,000,001 to $5,000,000	21%
$5,000,001 to $10,000,000	4%
$10,000,001 to $25.000,000	2%
$25,000,001 to $50,000,000	1%
$50,00,001 to $100,000,000	1%
More than $100,000,000	0%
Total	100%
Extrapolated value	$2,738,150

Q24b. Approximately, how much would this incident cost your organization in terms of diminished productivity of the IT security team?	Pct%
Less than $10,000	1%
$10,001 to $100,000	12%
$100,001 to $250,000	10%
$250,001 to $500,000	16%
$500,001 to $1,000,000	22%
$1,000,001 to $5,000,000	20%
$5,000,001 to $10,000,000	11%
$10,000,001 to $25.000,000	7%
$25,000,001 to $50,000,000	0%
$50,00,001 to $100,000,000	1%
More than $100,000,000	0%
Total	100%
Extrapolated value	$3,617,150

Q24c. Approximately, how much would this incident cost your organization in terms of lost user productivity?	Pct%
Less than $10,000	1%
$10,001 to $100,000	5%
$100,001 to $250,000	13%
$250,001 to $500,000	20%
$500,001 to $1,000,000	27%
$1,000,001 to $5,000,000	16%
$5,000,001 to $10,000,000	12%
$10,000,001 to $25.000,000	4%
$25,000,001 to $50,000,000	2%
$50,00,001 to $100,000,000	0%
More than $100,000,000	0%
Total	100%
Extrapolated value	$3,093,050

Q24d. How much would this incident cost your organization in terms of immediate revenue loss?	Pct%
Less than $10,000	3%
$10,001 to $100,000	8%
$100,001 to $250,000	11%
$250,001 to $500,000	15%
$500,001 to $1,000,000	31%
$1,000,001 to $5,000,000	25%
$5,000,001 to $10,000,000	4%
$10,000,001 to $25.000,000	2%
$25,000,001 to $50,000,000	1%
$50,00,001 to $100,000,000	0%
More than $100,000,000	0%
Total	100%
Extrapolated value	$2,057,550

Q24e. How much would this incident cost your organization in terms of diminished brand or reputation?	Pct%
Less than $10,000	0%
$10,001 to $100,000	12%
$100,001 to $250,000	18%
$250,001 to $500,000	10%
$500,001 to $1,000,000	18%
$1,000,001 to $5,000,000	23%
$5,000,001 to $10,000,000	13%
$10,000,001 to $25.000,000	6%
$25,000,001 to $50,000,000	0%
$50,00,001 to $100,000,000	0%
More than $100,000,000	0%
Total	100%
Extrapolated value	$2,905,600

Scenario 2 recap	Total
Cost of system administrator, help desk and customer support time	$2,738,150
Cost of lost user productivity	$3,093,050
Cost of diminished productivity of the IT security team	$3,617,150
Cost of lost user productivity	$3,093,050
Cost of immediate revenue loss	$2,057,550
Cost your organization in terms of diminished brand or reputation	$2,905,600
Total	$14,411,500

Estimating the cost of security exploits. Following are three cyber security threats that may result from insecure or poorly managed cryptographic keys and digital certificates. Please provide your **best estimate** to the questions listed below each threat.

Scenario 3. Server certificate and key misuse	
Q25a-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**?	Pct%
Zero	7%
1 time	5%
2 times	13%
3 times	15%
4 times	21%
5 times	18%
More than 5 times	21%
Total	100%
Extrapolated value	4.60

Q25a-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?**	Pct%
Less than 5%	1%
5% to 10%	2%
11% to 15%	8%
16% to 20%	7%
21% to 30%	19%
31% to 40%	16%
41% to 50%	16%
More than 50%	31%
Total	100%
Extrapolated value	0.39

Q26a. Approximately, how much would this incident cost your organization in terms of system administrator, help desk and customer support time responding to this issue?	Pct%
Less than $10,000	1%
$10,001 to $100,000	7%
$100,001 to $250,000	19%
$250,001 to $500,000	13%
$500,001 to $1,000,000	28%
$1,000,001 to $5,000,000	21%
$5,000,001 to $10,000,000	7%
$10,000,001 to $25.000,000	3%
$25,000,001 to $50,000,000	0%
$50,00,001 to $100,000,000	1%
More than $100,000,000	0%
Total	100%
Extrapolated value	$2,699,900

Q26b. Approximately, how much would this incident cost your organization in terms of lost user productivity?	Pct%
Less than $10,000	0%
$10,001 to $100,000	3%
$100,001 to $250,000	11%
$250,001 to $500,000	23%
$500,001 to $1,000,000	27%
$1,000,001 to $5,000,000	21%
$5,000,001 to $10,000,000	11%
$10,000,001 to $25.000,000	4%
$25,000,001 to $50,000,000	0%
$50,00,001 to $100,000,000	0%
More than $100,000,000	0%
Total	100%
Extrapolated value	$2,418,650

Q26c. Approximately, how much would this incident cost your organization in terms of diminished productivity of the IT security team?	Pct%
Less than $10,000	3%
$10,001 to $100,000	8%
$100,001 to $250,000	31%
$250,001 to $500,000	19%
$500,001 to $1,000,000	14%
$1,000,001 to $5,000,000	16%
$5,000,001 to $10,000,000	7%
$10,000,001 to $25.000,000	2%
$25,000,001 to $50,000,000	0%
$50,00,001 to $100,000,000	0%
More than $100,000,000	0%
Total	100%
Extrapolated value	$1,552,050

Q26d. How much would this incident cost your organization in terms of immediate revenue loss?	Pct%
Less than $10,000	1%
$10,001 to $100,000	5%
$100,001 to $250,000	16%
$250,001 to $500,000	11%
$500,001 to $1,000,000	28%
$1,000,001 to $5,000,000	30%
$5,000,001 to $10,000,000	5%
$10,000,001 to $25.000,000	3%
$25,000,001 to $50,000,000	1%
$50,00,001 to $100,000,000	0%
More than $100,000,000	0%
Total	100%
Extrapolated value	$2,435,050

Q26e. How much would this incident cost your organization in terms of diminished brand or reputation?	Pct%
Less than $10,000	0%
$10,001 to $100,000	2%
$100,001 to $250,000	15%
$250,001 to $500,000	23%
$500,001 to $1,000,000	16%
$1,000,001 to $5,000,000	21%
$5,000,001 to $10,000,000	13%
$10,000,001 to $25.000,000	8%
$25,000,001 to $50,000,000	1%
$50,00,001 to $100,000,000	1%
More than $100,000,000	0%
Total	100%
Extrapolated value	$4,317,600

Scenario 3 recap	Total
Cost of system administrator, help desk and customer support time	$2,699,900
Cost of lost user productivity	$2,418,650
Cost of diminished productivity of the IT security team	$1,552,050
Cost of immediate revenue loss	$2,435,050
Cost your organization in terms of diminished brand or reputation	$4,317,600
Total	$13,423,250

Scenario 4. Code signing certificate and key misuse	
Q27a-1. How many times has this issue occurred in your organization during the **past 24 months**?	Pct%
Zero	6%
1 time	3%
2 times	15%
3 times	16%
4 times	33%
5 times	18%
More than 5 times	9%
Total	100%
Extrapolated value	3.93

Q27a-2. What is the likelihood that this issue will occur in your organization over the **next 24 months**?	Pct%
Less than 5%	0%
5% to 10%	2%
11% to 15%	13%
16% to 20%	22%
21% to 30%	29%
31% to 40%	13%
41% to 50%	11%
More than 50%	10%
Total	100%
Extrapolated value	0.29

Q28a. Approximately, how much would this incident cost your organization in terms of system administrator, help desk and customer support time responding to this issue?	Pct%
Less than $10,000	2%
$10,001 to $100,000	9%
$100,001 to $250,000	11%
$250,001 to $500,000	15%
$500,001 to $1,000,000	28%
$1,000,001 to $5,000,000	21%
$5,000,001 to $10,000,000	8%
$10,000,001 to $25.000,000	2%
$25,000,001 to $50,000,000	3%
$50,00,001 to $100,000,000	1%
More than $100,000,000	0%
Total	100%
Extrapolated value	$3,715,550

Q28b. Approximately, how much would this incident cost your organization in terms of lost user productivity?	Pct%
Less than $10,000	0%
$10,001 to $100,000	2%
$100,001 to $250,000	17%
$250,001 to $500,000	20%
$500,001 to $1,000,000	23%
$1,000,001 to $5,000,000	21%
$5,000,001 to $10,000,000	11%
$10,000,001 to $25.000,000	5%
$25,000,001 to $50,000,000	0%
$50,00,001 to $100,000,000	1%
More than $100,000,000	0%
Total	100%
Extrapolated value	$3,318,350

Q28c. Approximately, how much would this incident cost your organization in terms of diminished productivity of the IT security team?	Pct%
Less than $10,000	1%
$10,001 to $100,000	4%
$100,001 to $250,000	21%
$250,001 to $500,000	35%
$500,001 to $1,000,000	13%
$1,000,001 to $5,000,000	16%
$5,000,001 to $10,000,000	7%
$10,000,001 to $25.000,000	2%
$25,000,001 to $50,000,000	1%
$50,00,001 to $100,000,000	0%
More than $100,000,000	0%
Total	100%
Extrapolated value	$1,927,750

Q28d. Approximately, how much would this incident cost your organization in terms of immediate revenue loss?	Pct%
Less than $10,000	0%
$10,001 to $100,000	8%
$100,001 to $250,000	18%
$250,001 to $500,000	16%
$500,001 to $1,000,000	27%
$1,000,001 to $5,000,000	26%
$5,000,001 to $10,000,000	5%
$10,000,001 to $25.000,000	1%
$25,000,001 to $50,000,000	0%
$50,00,001 to $100,000,000	1%
More than $100,000,000	0%
Total	102%
Extrapolated value	$2,346,400

Q28e. Approximately, how much would this incident cost your organization in terms of diminished brand or reputation?	Pct%
Less than $10,000	1%
$10,001 to $100,000	1%
$100,001 to $250,000	14%
$250,001 to $500,000	24%
$500,001 to $1,000,000	18%
$1,000,001 to $5,000,000	23%
$5,000,001 to $10,000,000	16%
$10,000,001 to $25.000,000	5%
$25,000,001 to $50,000,000	0%
$50,00,001 to $100,000,000	1%
More than $100,000,000	0%
Total	103%
Extrapolated value	$3,717,100

Scenario 4 recap	Total
Cost of system administrator, help desk and customer support time	$3,715,550
Cost of lost user productivity	$3,318,350
Cost of diminished productivity of the IT security team	$1,927,750
Cost of immediate revenue loss	$2,346,400
Cost your organization in terms of diminished brand or reputation	$3,717,100
Total	$15,025,150

Scenario 5. Certificate Authority (CA) compromise or rogue CA for man-in-middle (MITM) and phishing attacks	
Q29a-1. How many times has this issue occurred in your organization during the **past 24 months**?	Pct%
Zero	8%
1 time	23%
2 times	36%
3 times	19%
4 times	6%
5 times	6%
More than 5 times	2%
Total	100%
Extrapolated value	2.26

Q29a-2. What is the likelihood that this issue will occur in your organization over the **next 24 months**?	Pct%
Less than 5%	0%
5% to 10%	0%
11% to 15%	8%
16% to 20%	9%
21% to 30%	12%
31% to 40%	25%
41% to 50%	30%
More than 50%	16%
Total	100%
Extrapolated value	0.38

Q30a. Approximately, how much would this incident cost your organization in terms of system administrator, help desk and customer support time responding to this issue?	Pct%
Less than $10,000	6%
$10,001 to $100,000	12%
$100,001 to $250,000	12%
$250,001 to $500,000	26%
$500,001 to $1,000,000	23%
$1,000,001 to $5,000,000	11%
$5,000,001 to $10,000,000	7%
$10,000,001 to $25.000,000	3%
$25,000,001 to $50,000,000	1%
$50,00,001 to $100,000,000	0%
More than $100,000,000	0%
Total	101%
Extrapolated value	$2,000,900

Q30b. Approximately, how much would this incident cost your organization in terms of lost user productivity?	Pct%
Less than $10,000	0%
$10,001 to $100,000	7%
$100,001 to $250,000	15%
$250,001 to $500,000	12%
$500,001 to $1,000,000	20%
$1,000,001 to $5,000,000	24%
$5,000,001 to $10,000,000	16%
$10,000,001 to $25.000,000	6%
$25,000,001 to $50,000,000	0%
$50,00,001 to $100,000,000	0%
More than $100,000,000	0%
Total	100%
Extrapolated value	$3,171,100

Q30c. Approximately, how much would this incident cost your organization in terms of diminished productivity of the IT security team?	Pct%
Less than $10,000	1%
$10,001 to $100,000	4%
$100,001 to $250,000	21%
$250,001 to $500,000	35%
$500,001 to $1,000,000	13%
$1,000,001 to $5,000,000	16%
$5,000,001 to $10,000,000	7%
$10,000,001 to $25.000,000	2%
$25,000,001 to $50,000,000	1%
$50,00,001 to $100,000,000	0%
More than $100,000,000	0%
Total	100%
Extrapolated value	$1,927,750

Q30d. Approximately, how much would this incident cost your organization in terms of immediate revenue loss?	Pct%
Less than $10,000	2%
$10,001 to $100,000	7%
$100,001 to $250,000	19%
$250,001 to $500,000	13%
$500,001 to $1,000,000	25%
$1,000,001 to $5,000,000	23%
$5,000,001 to $10,000,000	8%
$10,000,001 to $25.000,000	2%
$25,000,001 to $50,000,000	0%
$50,00,001 to $100,000,000	1%
More than $100,000,000	0%
Total	100%
Extrapolated value	$2,637,450

Q30e. Approximately, how much would this incident cost your organization in terms of diminished brand or reputation?	Pct%
Less than $10,000	0%
$10,001 to $100,000	8%
$100,001 to $250,000	11%
$250,001 to $500,000	18%
$500,001 to $1,000,000	17%
$1,000,001 to $5,000,000	25%
$5,000,001 to $10,000,000	17%
$10,000,001 to $25.000,000	3%
$25,000,001 to $50,000,000	0%
$50,00,001 to $100,000,000	1%
More than $100,000,000	0%
Total	100%
Extrapolated value	$3,482,650

Scenario 5 recap	Total
Cost of system administrator, help desk and customer support time	$2,000,900
Cost of lost user productivity	$3,171,100
Cost of diminished productivity of the IT security team	$1,927,750
Cost of immediate revenue loss	$2,637,450
Cost your organization in terms of diminished brand or reputation	$3,482,650
Total	$13,219,850

Part 3. Organization and respondents' demographics

D1. What best describes your position level within the organization?	Pct%
Executive/VP	7%
Director	14%
Manager	21%
Supervisor	15%
Staff/technician	35%
Administrative	6%
Consultant	2%
Other	0%
Total	100%

D2. What best describes your direct reporting channel?	Pct%
CEO/executive committee	3%
COO or head of operations	2%
CFO, controller or head of finance	1%
CIO or head of corporate IT	50%
Business unit leader or general manager	20%
Head of compliance or internal audit	3%
CISO/CSO or head of IT security	21%
Other	0%
Total	100%

D3. What range best describes the full-time headcount of your global organization?	Pct%
Less than 1,000	15%
1,000 to 5,000	23%
5,001 to 10,000	21%
10,001 to 25,000	20%
25,001 to 75,000	13%
More than 75,000	8%
Total	100%

D4. What best describes your organization's primary industry classification?	Pct%
Agriculture & food services	1%
Automotive	4%
Communications	5%
Construction and real estate	2%
Consumer products	7%
Energy & utilities	8%
Financial services	15%
Healthcare & medical devices	8%
Industrial products & chemicals	8%
Insurance	4%
Pharmaceuticals & biotech	3%
Professional services	2%
Retail	5%
Retail, E-commerce	6%
Services	8%
Technology & software	9%
Transportation	3%
Other	2%
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.

Keyfactor

Secure Every Digital Identity

Keyfactor, formerly Certified Security Solutions (CSS), is a leading provider of secure digital identity management solutions that enable organizations to confirm authenticity, and ensure the right things are interacting in the right ways in our connected world.

From an enterprise managing millions of devices and applications that affect people's lives every day, to a manufacturer aiming to ensure its product will function safely throughout its life cycle, Keyfactor empowers global enterprises with the freedom to master every digital identity. Its clients are the most innovative brands in the industries where trust and reliability matter most.

Learn more at www.keyfactor.com and @keyfactor.