Ponemon INSTITUTE

November 2018

2018 State of Cybersecurity in Small & Medium Size Businesses

Sponsored by Keeper Security, Inc.
Independently conducted by Ponemon Institute LLC

KEEPER Cybersecurity Starts Here®

2018 State of Cybersecurity in Small & Medium Size Businesses (SMBs)

Ponemon Institute, November 2018

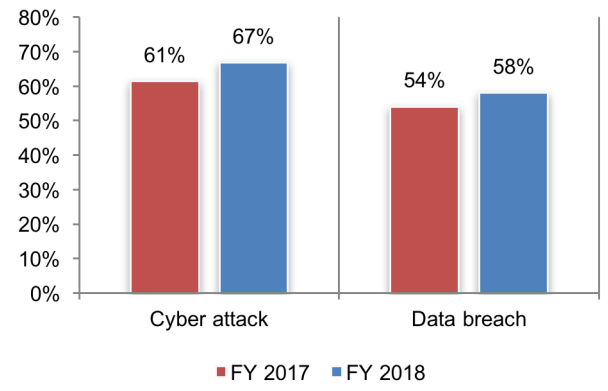
Part 1. Executive summary

Small businesses increasingly face the same cybersecurity risks as larger companies, but only 28 percent of the companies represented in this study rate their ability to mitigate threats, vulnerabilities and attacks as highly effective. Most participants in this research say attacks against their companies are targeted and sophisticated with severe financial consequences. According to this study's findings, the weakest link in these companies' security posture is the negligent insider or contractor as they are considered the number one reason a company can have a data breach, phishing attack or a ransomware attack.

Ponemon Institute is pleased to present the results of *The 2018 State of Cybersecurity in Small and Medium Size Businesses* sponsored by Keeper Security. The goal of this study is to track how small and medium size companies address the same threats faced by larger companies. This report features the findings from 2018 and 2017.

Figure 1. Our company experienced a cyber attack and data breach in the past 12 months

Yes responses



This research's sample included approximately 1,045 individuals from companies in the United States and the United Kingdom; these companies had head counts ranging from less than 100 to 1,000. In this report, we present the consolidated findings for 2017 and 2018.

As Figure 1 illustrates, cyber attacks on SMBs have increased from 61 percent of respondents in 2017 to 67 percent of respondents in 2018. The occurrence of data breaches involving customer and employee information over 12 months also increased from 54 percent of respondents to 58 percent of respondents.

In the aftermath of these incidents, the respondents' companies spent an average of $1.43 million, a 33 percent increase from $1.03 million in 2017, because of the damage or theft of IT assets. In addition, disruption to normal operations cost an average of $1.56 million, a 25 percent increase from $1.21 million in 2017.

Following are the most salient findings of this research.

- Phishing attacks and advanced malware/zero day attacks are increasing. Respondents reported phishing/social engineering attacks increased from 48 percent in 2017 to 52 percent in 2018 and advanced malware/zero day attacks increased from 16 percent to 24 percent.

- The risk of negligent employees and contractors causing a data breach or ransomware is getting worse. Sixty percent of respondents in companies that had a data breach say the root cause of the data breach was a negligent employee or contractor, an increase from 54 percent in 2017. Sixty-one percent of respondents say negligent employees put their company at risk for a ransomware attack, an increase from 58 percent of respondents in 2017.

- More companies are affected by exploits and malware that evaded their intrusion detection system (72 percent of respondents) or anti-virus solution (82 percent of respondents).

- Mobile devices are the most vulnerable endpoints or entry points to networks and enterprise systems, according to 55 percent of respondents. Almost half (49 percent) of respondents say the use of mobile devices to access business-critical applications and IT infrastructure affects their companies' security posture.

- More companies have experienced ransomware attacks (61 percent of respondents vs. 52 percent of respondents in 2017) and 70 percent of respondents in these companies report that the ransom was paid. The average payment in these cases was $1,466.

- To strengthen their cybersecurity postures, companies need more in-house expertise and budget. However, almost half (47 percent) of respondents say they have no understanding of how to protect their companies against cyber attacks.

- Responsibility for determining IT security priorities is dispersed throughout the company. As a result, the ability to have effective leadership in the IT security function is missing in most companies. In fact, 35 percent of respondents say no one function determines IT security priorities.

- Passwords are often compromised or stolen because employees use weak passwords. Forty percent of respondents say their companies experienced an attack involving the compromise of employees' passwords; the average cost of each attack was $383,365.

- A lack of visibility into employees' password practices is exacerbating the likelihood of attacks involving passwords. Protection of passwords mostly involves human memory (53 percent of respondents) and spreadsheets (51 percent of respondents). Only 18 percent of respondents say their organizations rely upon browser extensions.

- More companies are using single sign-on (SSO) to simplify and increase the security of user access to their companies' applications and data.

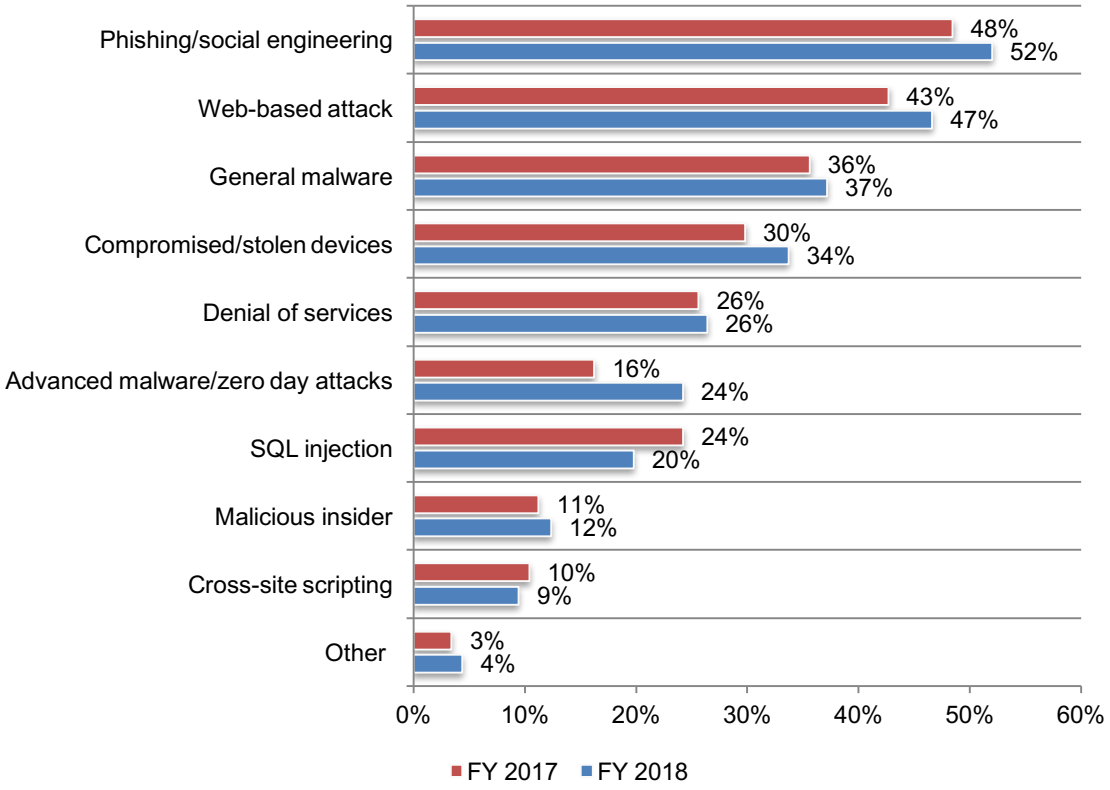
Part 2. Key findings

- Trends in SMB cyber attacks and data breaches
- Ransomware attacks continue to increase
- Password practices and policies
- Cybersecurity posture and governance
- Technologies in place to address the threat

Trends in SMB cyber attacks and data breaches

Cyber attacks and data breaches target SMBs. As discussed, most businesses represented in this study experienced a cyber attack or a data breach with severe financial consequences (67 percent and 58 percent, respectively). As shown in Figure 2, phishing/social engineering continues to be the number one attack SMBs experience (52 percent of respondents). Other frequent attacks are web-based attacks and general malware (47 percent and 37 percent of respondents, respectively). The type of attack that increased the most is advanced malware/zero day attacks (from 16 percent of respondents in 2017 to 24 percent of respondents in 2018).

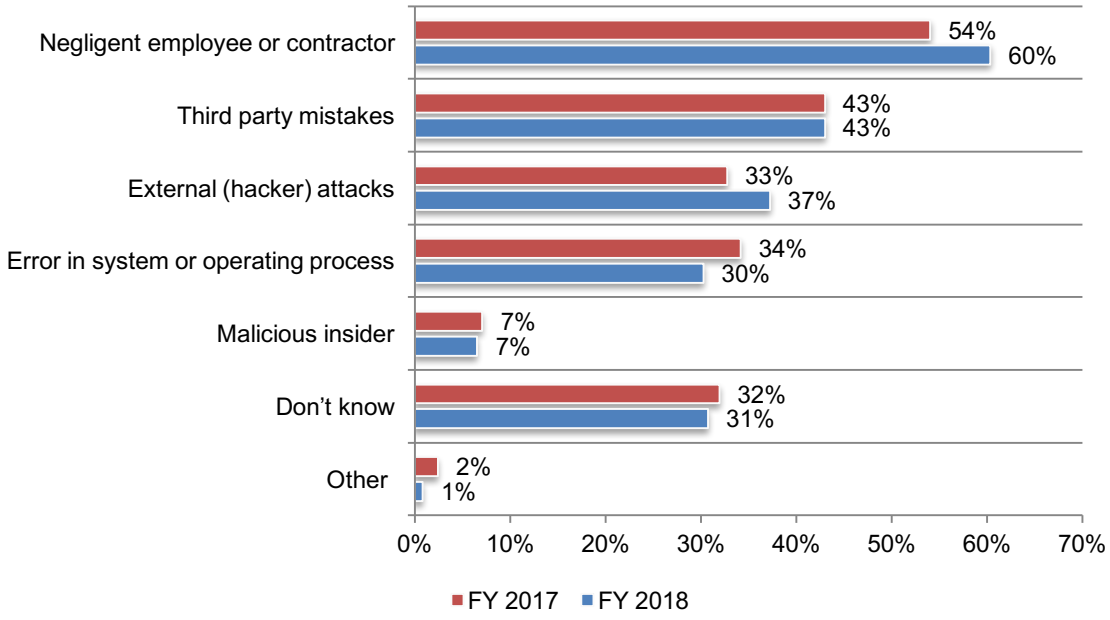
Figure 2. What types of attacks did your business experience?
More than one choice allowed



Businesses are losing more records in a data breach. Companies represented in this research lost an average of 10,848 individual records over the past 12 months as a result of the data breach, an increase from an average of 9,350 in last year's study.

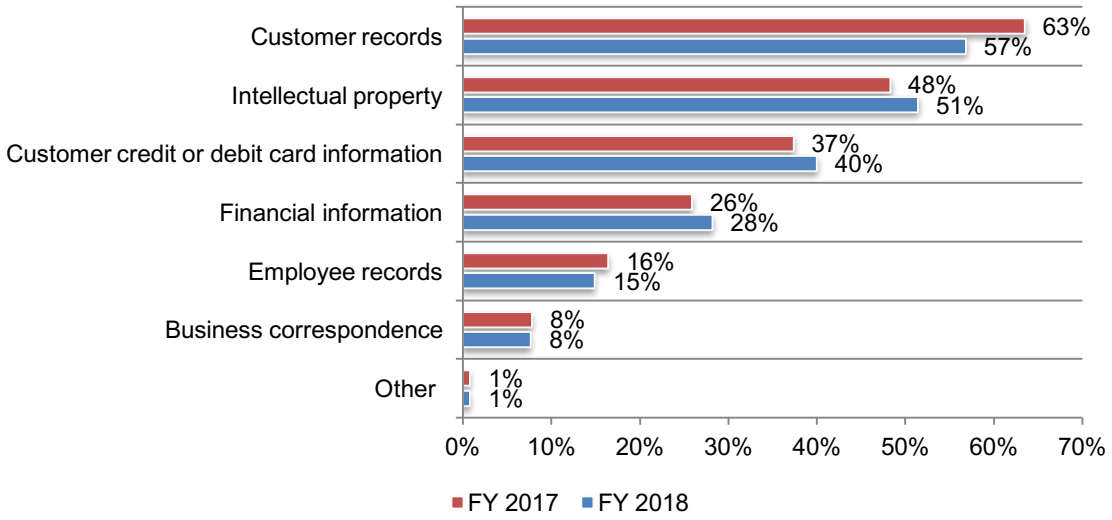
As shown in Figure 3, of the 58 percent of respondents who say their company had a data breach, they cite the root cause as negligent employees or contractors (60 percent of respondents), which increased from 54 percent in 2017. This is followed by third party mistakes (43 percent of respondents) and external (hacker) attacks (37 percent of respondents). However, almost a third of respondents (31 percent) say their companies could not determine the cause of the incident.

Figure 3. What was the root cause of the data breaches your business experienced?
More than one choice allowed



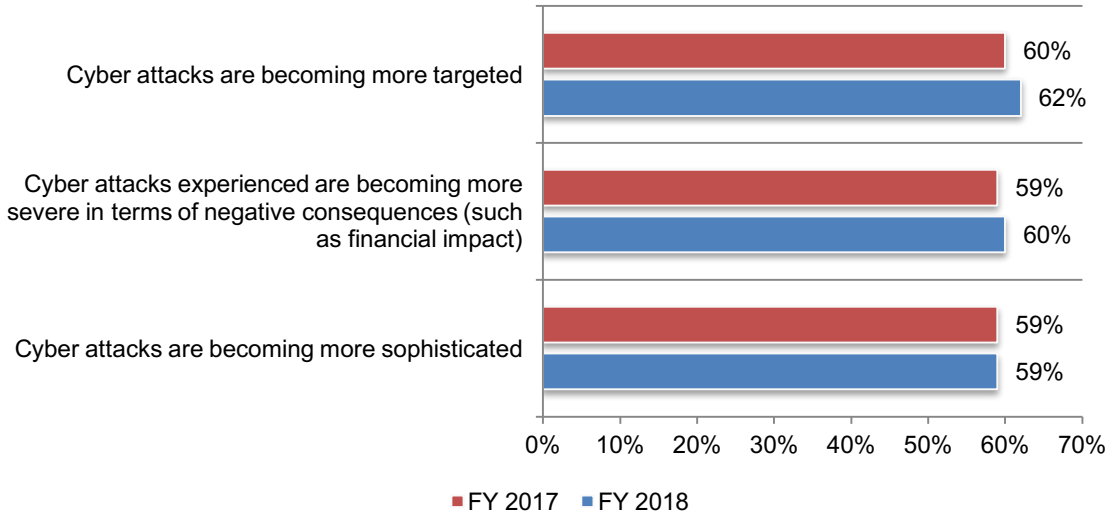
B**usinesses are most concerned about protecting customer records and intellectual property.** When asked what information cyber attackers are most likely to target, 57 percent of respondents say customer records are their biggest concern. More than half of respondents (51 percent) say they worry about the protection of their intellectual property.

Figure 4. What types of information are you most concerned about protecting from cyber attackers?
Two choices allowed



Cyber attacks against SMBs are not diminishing. Most respondents say cyber attacks against their companies are targeted, severe and sophisticated (62 percent, 60 percent and 59 percent, respectively); these values have not changed significantly since 2017, as shown in Figure 5.

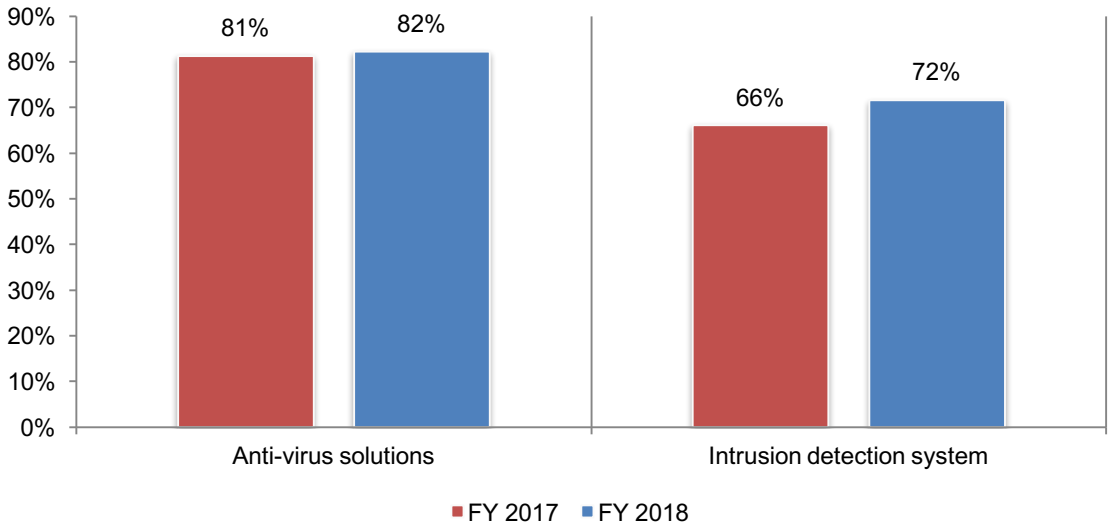
Figure 5. Perceptions about cyber attacks against their companies
Strongly Agree and Agree responses combined



Businesses are vulnerable to exploits and malware. Only 40 percent of respondents say the technologies currently used by their organization can detect and block most cyber attacks. As discussed previously, SMBs have experienced more advanced malware and zero day attacks in 2018.

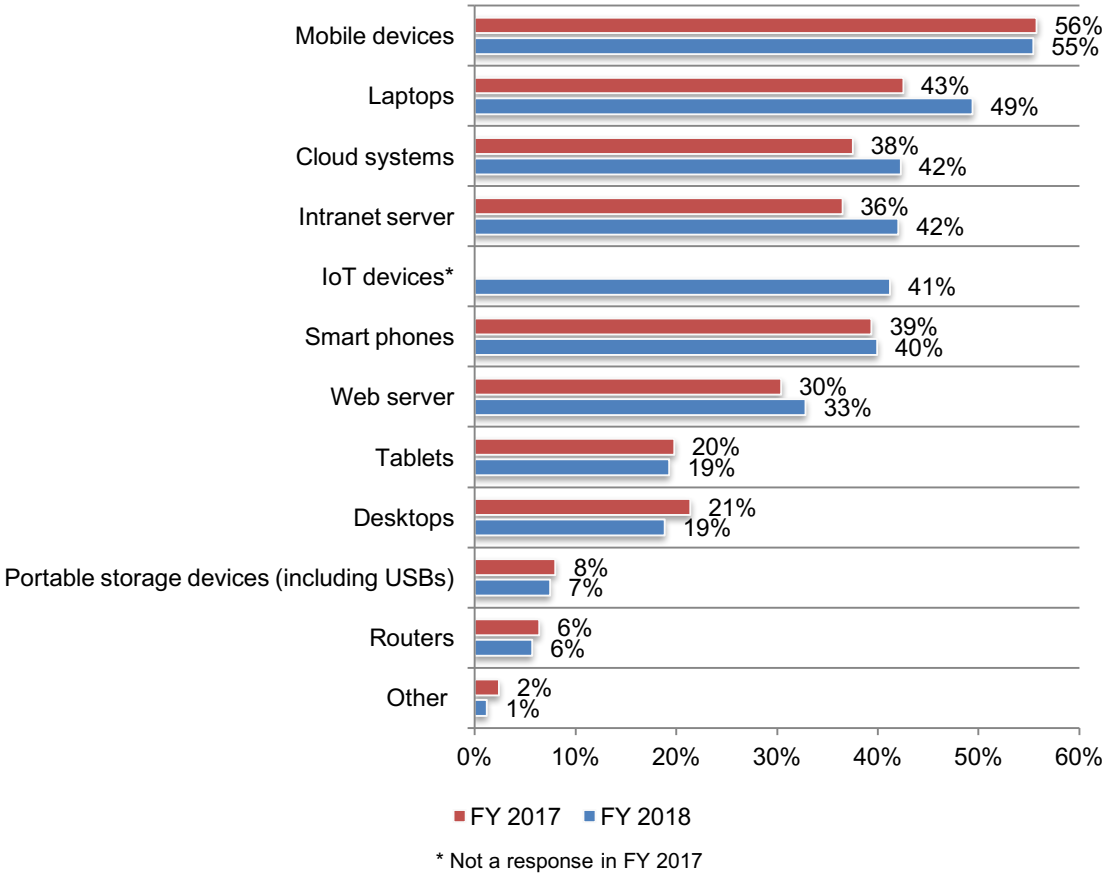
Figure 6 reveals that 72 percent of respondents (an increase from 66 percent in the previous study) say exploits and malware evaded intrusion detection systems moreover, 82 percent of respondents (an increase from 81 percent last year) say they have evaded their anti-virus solutions.

Figure 6. Has your business experienced situations when exploits and malware have evaded their intrusion detection system or anti-virus solutions?
Yes responses presented



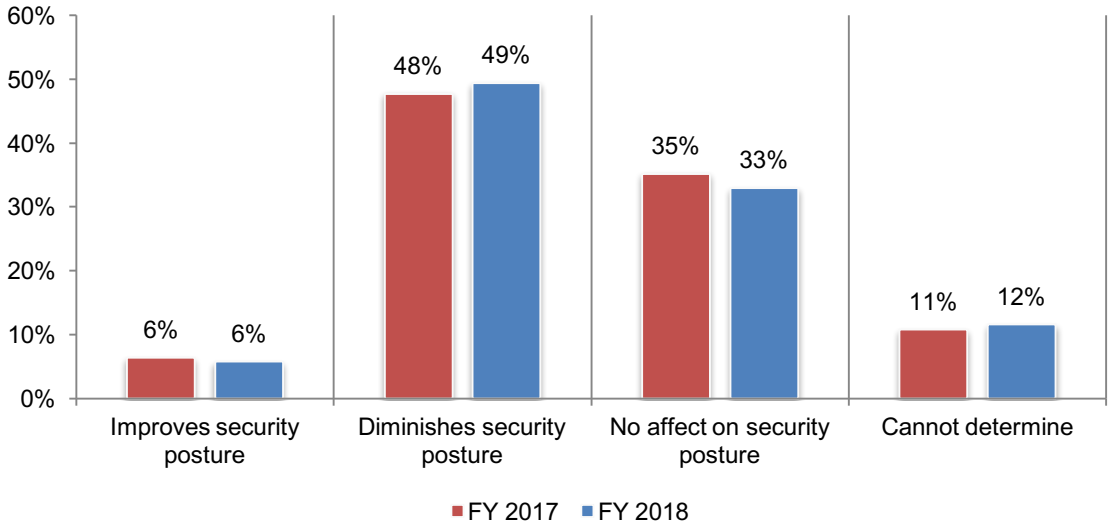
Mobile devices are the most vulnerable endpoints or entry points to networks and enterprise systems. As shown in Figure 7, mobile devices are considered, by far, the most vulnerable endpoint or entry point to respondents' companies' networks and enterprise systems. However, laptops and intranet servers have increased in their vulnerability. For the first time, IoT devices were included and 41 percent say they are a very vulnerable entry point.

Figure 7. What are the most vulnerable endpoints or entry points to your organization's networks and enterprise systems?
Three choices allowed



More mobile devices will be used to access business-critical applications and IT infrastructure. Currently, an average of 45 percent of business-critical applications are accessed from mobile devices such as smartphones and tablets. As shown in Figure 8, nearly half (49 percent) of respondents say these devices diminish their companies' security posture.

Figure 8. How does the use of mobile devices to access business-critical applications and IT infrastructure affect your organization's security posture?

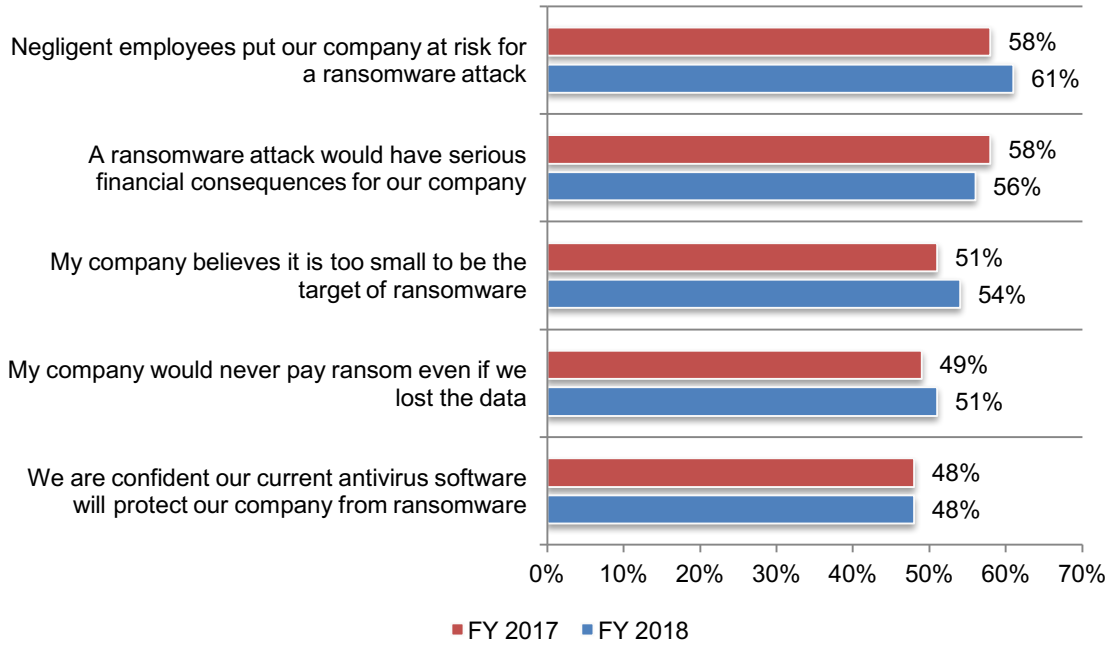


Ransomware attacks continue to increase

The weakest link in a company's ability to stop a ransomware attack is the negligent employee. In the context of this research, ransomware is defined as a sophisticated piece of malware that blocks victims' access to their files.

Sixty-one percent of respondents say negligent employees put their company at risk for a ransomware attack and 56 percent of respondents say these attacks can have serious financial consequences, as shown in Figure 9. Less than half (48 percent) of respondents are confident that their current anti-virus software will protect their company from ransomware.

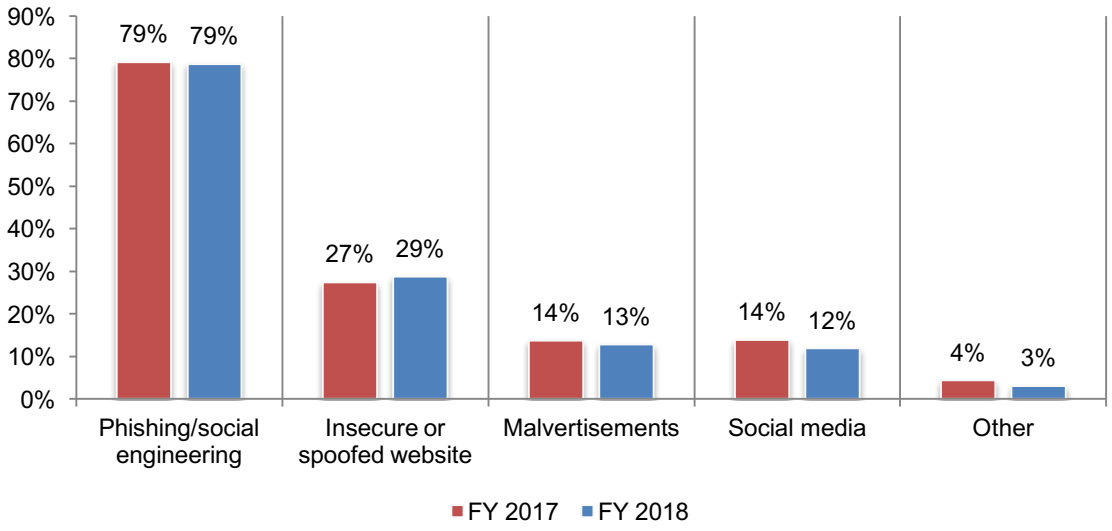
Figure 9. Perceptions regarding ransomware
Strongly agree and Agree responses combined



Ransomware attacks increase significantly since last year. Sixty-one percent of respondents say their company experienced either unsuccessful or successful ransomware attacks within the past three months (11 percent), within the past 6 months (17 percent), within the past 12 months (19 percent) or more than 12 months ago (14 percent). In 2017, 52 percent of respondents said they experienced a ransomware attack.

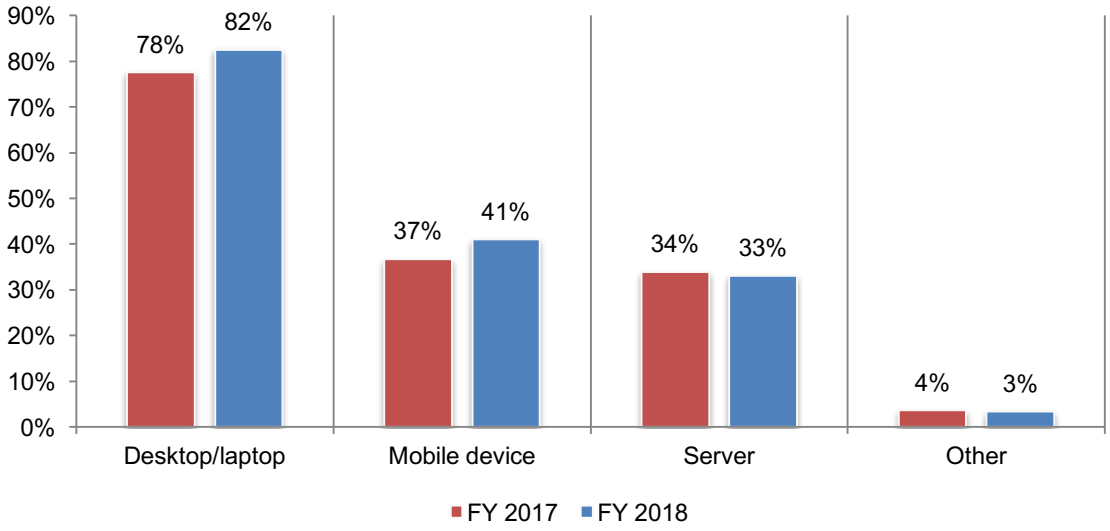
As shown in Figure 10, the ransomware experienced by companies in this study was mainly unleashed via phishing/social engineering attacks (79 percent of respondents) followed by an insecure or spoofed website (29 percent of respondents). This finding coincides with both the increase in phishing/social engineering and the increase in negligent employees as the root cause of a data breach.

Figure 10. How was the ransomware unleashed?
More than one choice allowed



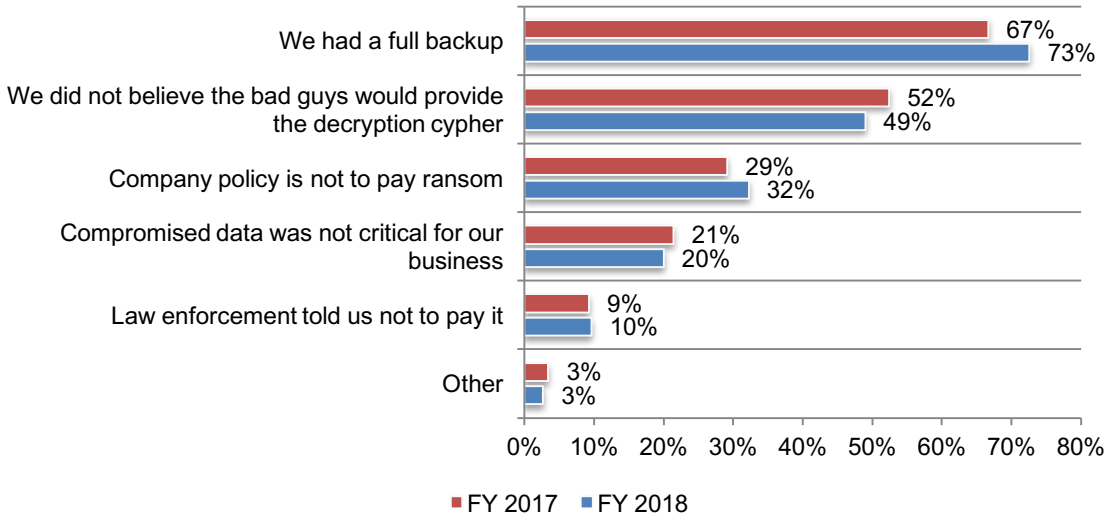
The devices considered the most vulnerable as a point of entry are the ones most often attacked. As shown in Figure 11, the devices most often compromised by ransomware were desktop/laptop (82 percent) and mobile device (41 percent), as shown in Figure 11.

Figure 11. What type of device(s) was compromised by ransomware?
More than one choice allowed



For successful ransomware attacks, more companies are paying the ransom. The average ransom was $1,466, and 70 percent of respondents say their companies paid the ransom. Last year, 60 percent of respondents said they paid the ransom. As shown in Figure 12, companies that **did not** pay the ransom attributed the decision to having a full backup (73 percent of respondents) or not trusting the criminals to provide the decryption cypher (49 percent of respondents).

Figure 12. Why did your company not pay the ransom?
More than one choice allowed

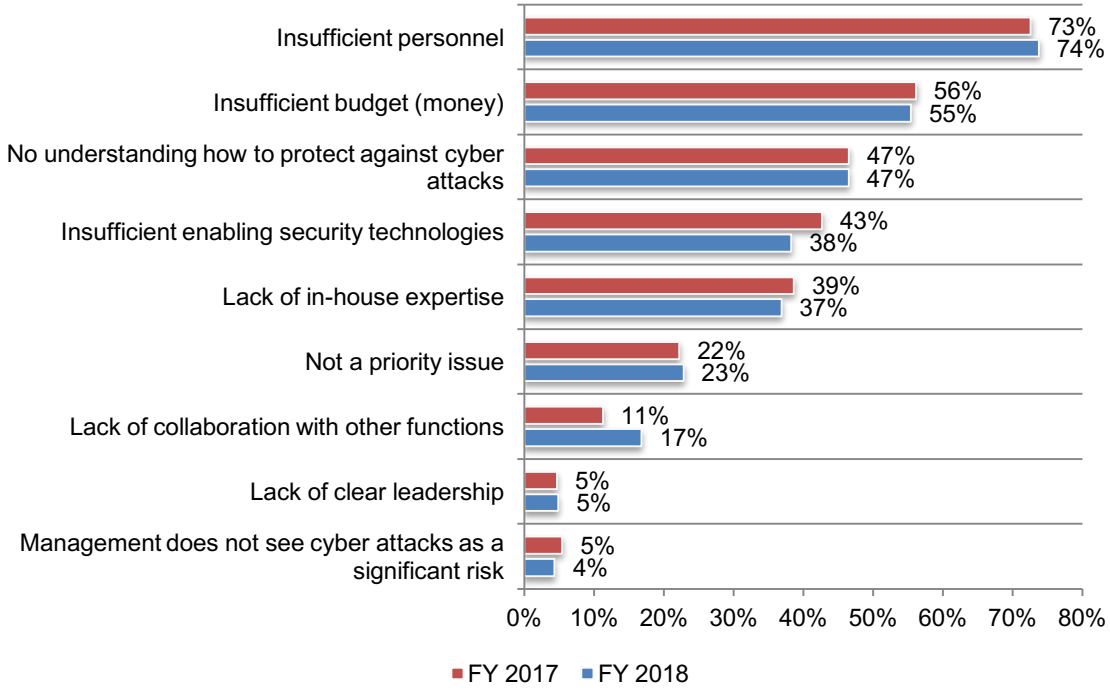


Cybersecurity posture and governance

SMBs continue to struggle with insufficient personnel and money. Figure 13 lists the challenges companies face when trying to create a stronger security posture.

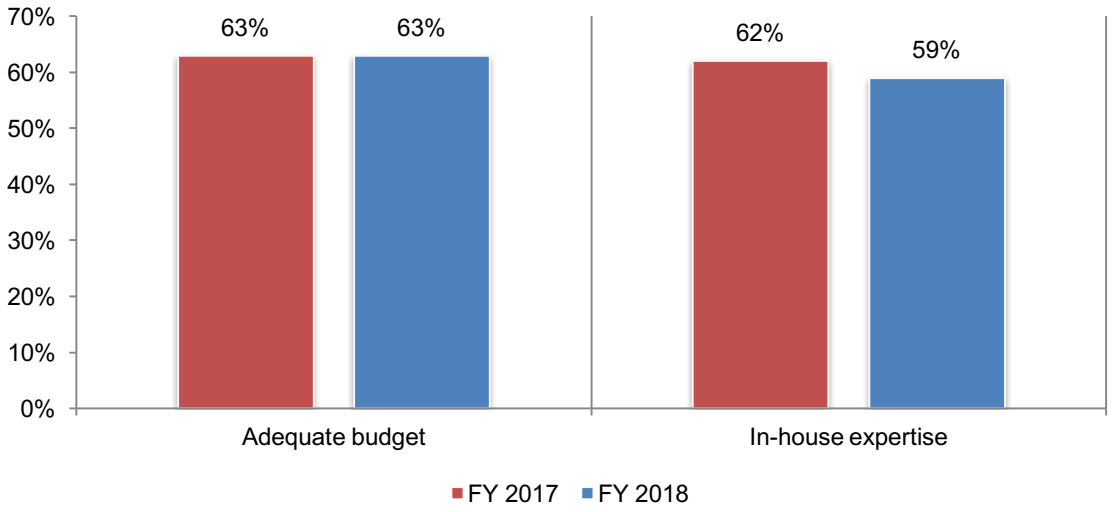
The biggest problem is not having the personnel to mitigate cyber risks, vulnerabilities and attacks (74 percent of respondents). The next biggest challenges are insufficient budget (55 percent of respondents) and no understanding of how to protect against cyber attacks (47 percent of respondents).

Figure 13. What challenges keep your IT security posture from being fully effective?
Three choices allowed



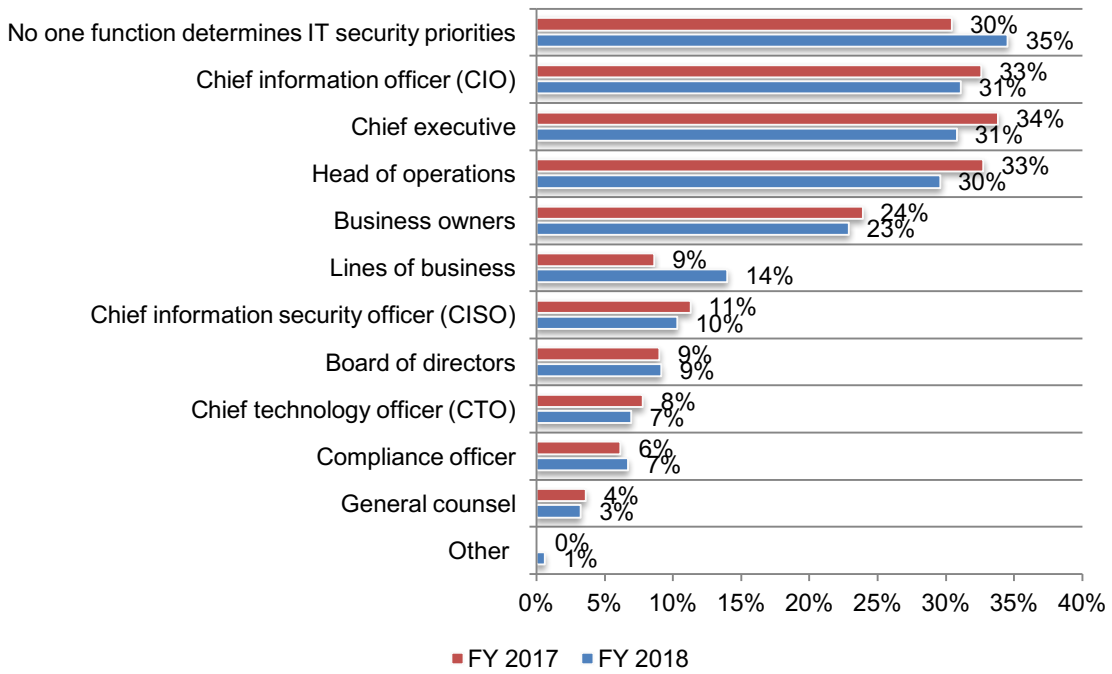
As Figure 14 shows, 63 percent of respondents say their companies do not have an adequate budget to achieve a strong cybersecurity posture. Fifty-nine percent of respondents say their companies do not have adequate in-house expertise to achieve a strong cybersecurity posture.

Figure 14. Does your organization have an adequate budget and in-house expertise to achieve a strong cybersecurity posture?
No and Unsure responses combined



Leadership is lacking when determining IT security priorities. As shown in Figure 15, 35 percent of respondents say no one person is responsible for determining IT security priorities, an increase from 30 percent of respondents in last year's research. According to the findings, responsibility for companies' IT security strategy is dispersed throughout the company.

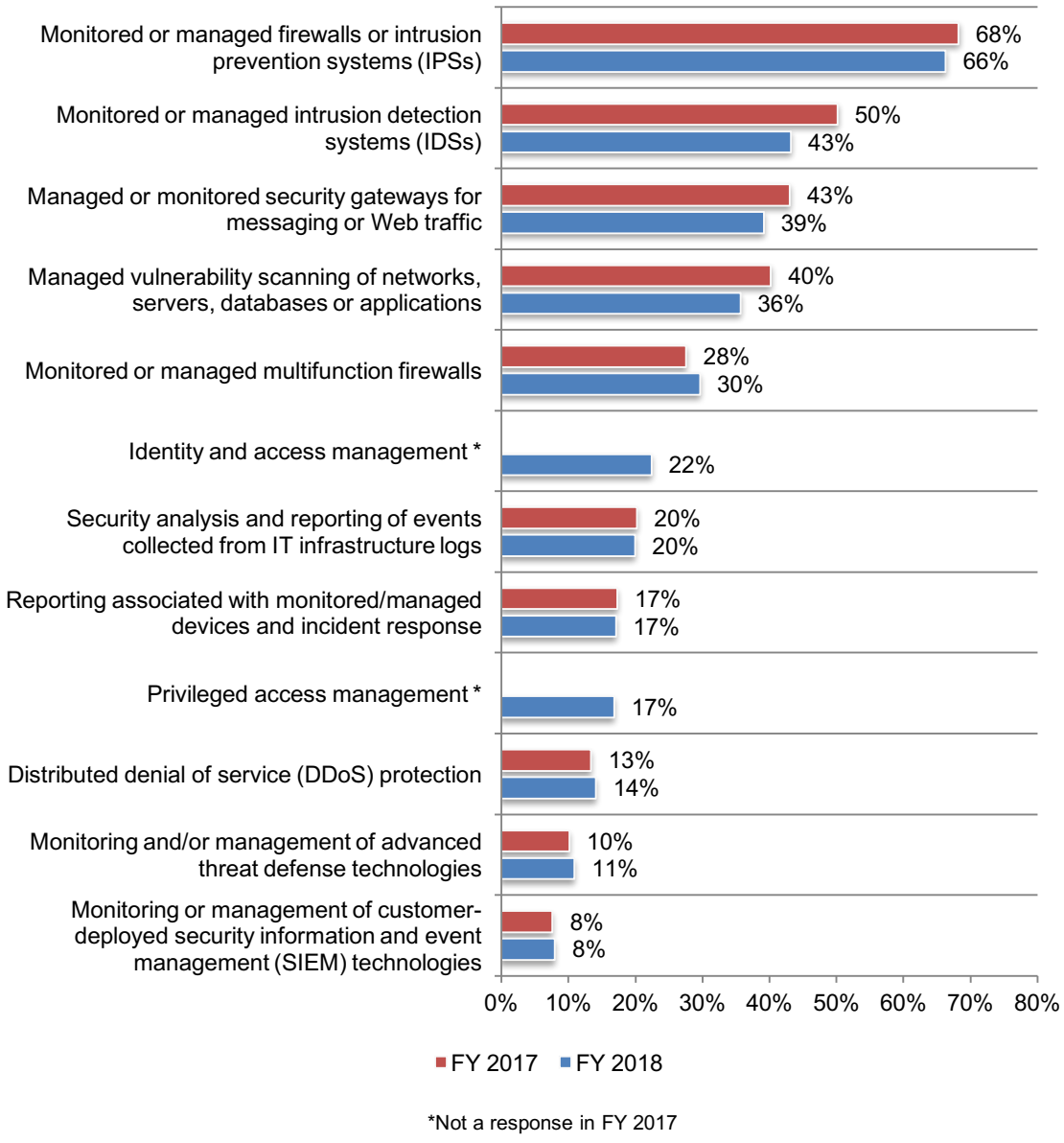
Figure 15. Who determines IT security priorities?
Two choices allowed



More SMBs are engaging managed security services providers (MSSPs) to support the IT security function. On average, 29 percent of a company's IT security operations are supported by MSSPs, this is an increase from 21 percent in last year's study.

According to Figure 16, 66 percent of respondents say their MSSP monitors or manages firewalls or intrusion prevention systems (IPS). Forty-three percent say they use MSSPs to monitor or manage intrusion detection systems (IDSs).

Figure 16. What services are provided by MSSPs to support your IT security posture?
More than one choice permitted

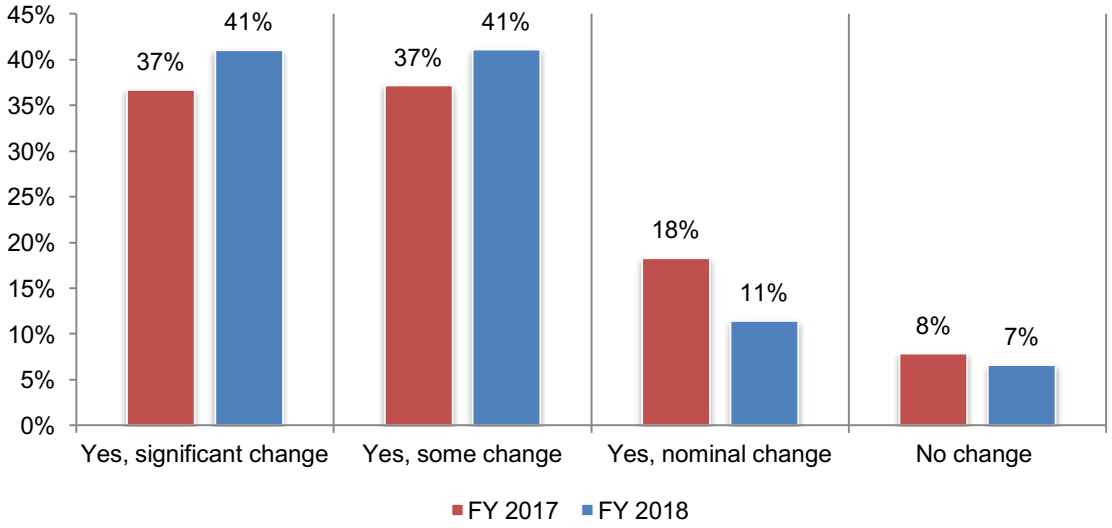


*Not a response in FY 2017

Compliance with the new General Data Protection Regulation (GDPR) is a burden for SMBs already challenged with not having an adequate IT security budget. The GDPR took effect on May 25, 2018. It establishes new requirements related to the export of personal data outside the European Union. In last year's research, respondents were asked to predict if the GDPR would require significant changes to their companies' privacy and security strategies.

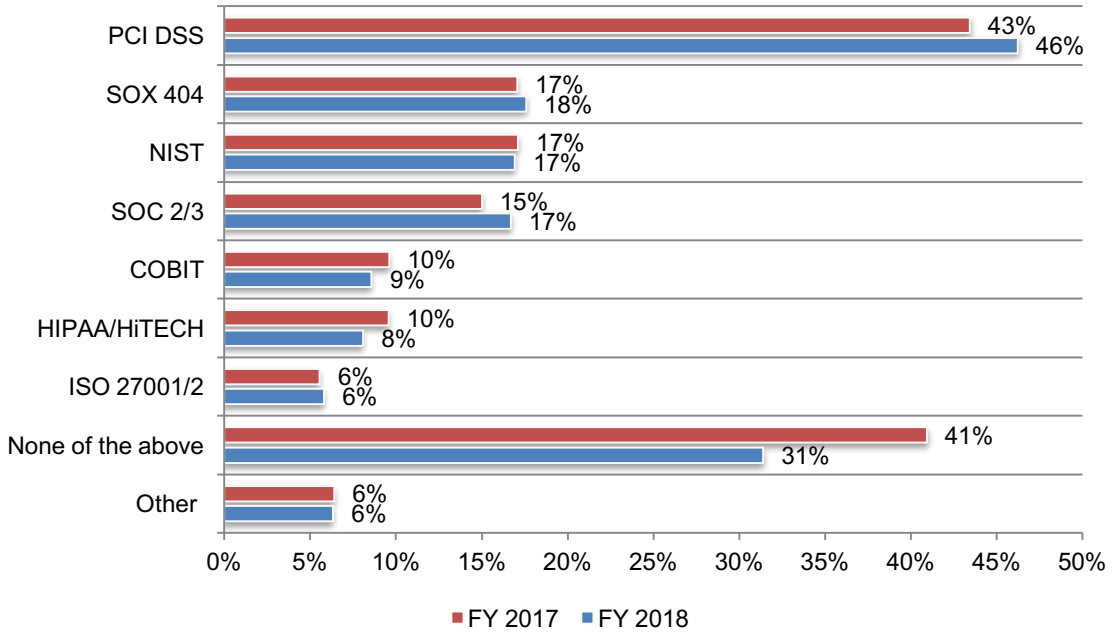
As Figure 17 shows, last year 92 percent of respondents said the new regulations would require changes to their privacy and security strategy. Similarly, in 2018, 93 percent of respondents say the new regulation did require significant changes. Only 19 percent of respondents say they have achieved a high level of compliance with GDPR.

Figure 17. Will the GDPR require significant changes in your privacy and security strategy?



More SMBs are adopting IT security guidelines or standards. Figure 18 presents the leading IT security guidelines and standards. Forty-six percent of respondents say they comply with PCI DSS. Thirty-one percent of respondents say they do not comply with any of the standards, a significant decline from 41 percent of respondents in the 2017 study.

Figure 18. Which IT security guidelines or standards does your company comply with?
More than one choice permitted



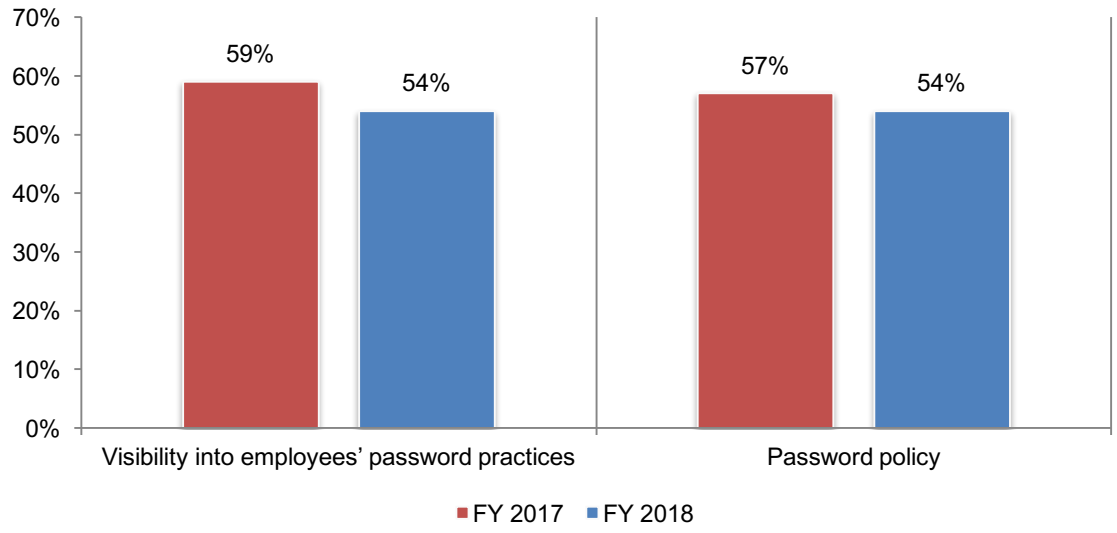
Password practices and policies

Strong passwords and biometrics are an essential part of a company's security defense. Forty percent of respondents say their companies had an attack involving the compromise of employees' passwords in the past year, and the average cost of each attack was $383,365.

Similar to last year's findings, 62 percent of respondents say they rely upon strong passwords and/or biometrics to reduce the risk of attack. In 2017, 60 percent of respondents agreed with this risk mitigation strategy.

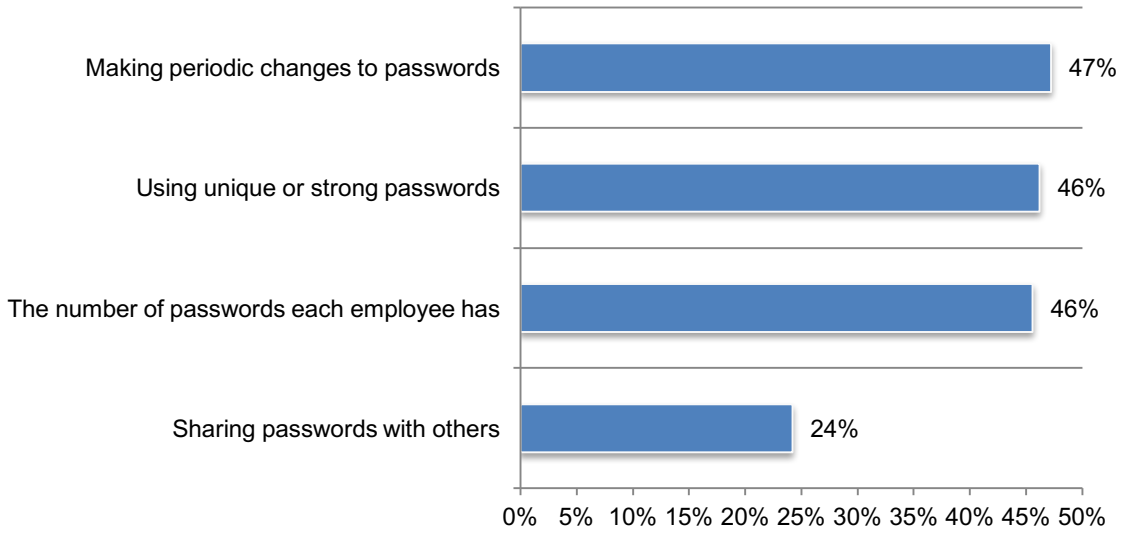
However, as Figure 19 demonstrates, 54 percent of respondents say they do not have, or are unsure if they have, visibility into employees' password practices such as the use of unique or strong passwords and sharing passwords with others. Fifty-four percent of respondents do not have, or are unsure their company has, a policy pertaining to employees' use of passwords and/or biometrics, such as a fingerprint.

Figure 19. Does your organization have visibility into employees' password practices and a password policy?
No and Unsure responses combined



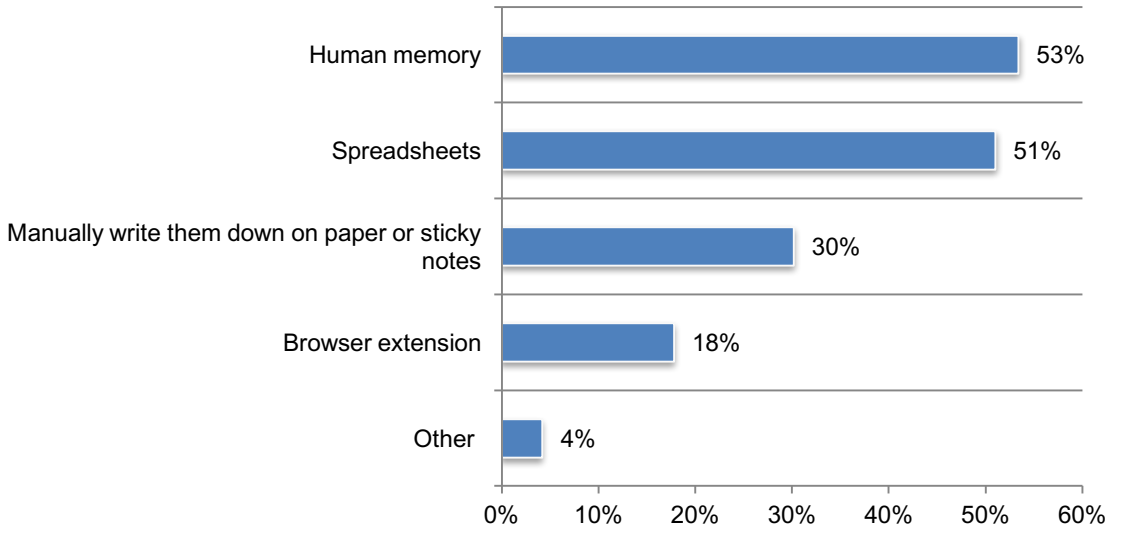
The ability to determine employees' password practices is not effective. Of the 45 percent of respondents who say they have visibility into employees' password practices, less than half of respondents say they are able to determine if employees are making periodic changes to passwords (47 percent), using unique or strong passwords (46 percent) and determining the number of passwords each employee has (46 percent). Only 24 percent of respondents say they are able to determine if employees are sharing passwords.

Figure 20. Is your company able to determine employees' password practices?
More than one choice allowed



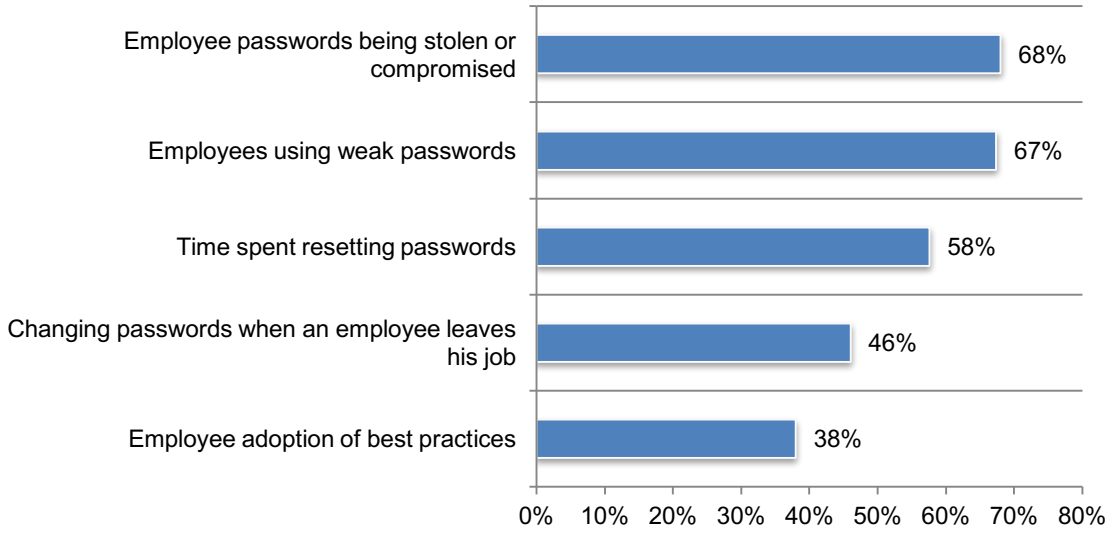
Human memory and spreadsheets are used to protect passwords. Only 22 percent of respondents say their companies require employees to use a password manager. Of the 74 percent of respondents who say password managers are not required, 53 percent of respondents say their companies rely upon human memory and 51 percent of respondents say they use spreadsheets.

Figure 21. What does your organization use to manage and protect its passwords?
More than one choice allowed



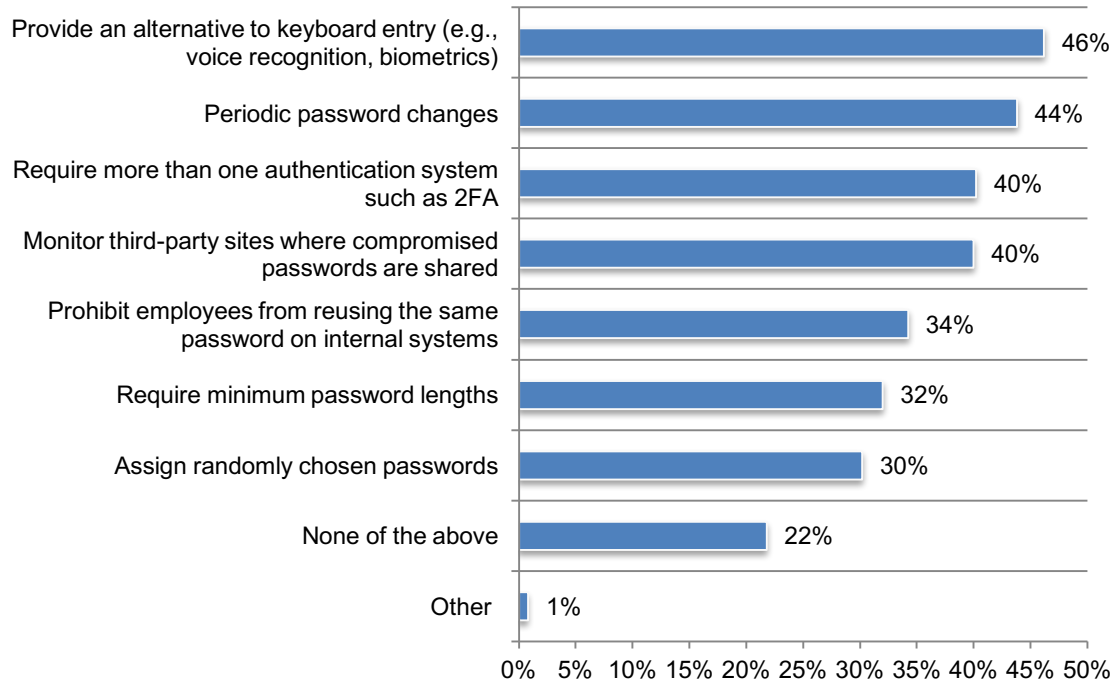
Employees' use of weak passwords leads to stolen or otherwise compromised passwords. Figure 22 lists what respondents think are the biggest pain points in managing employees' passwords. As shown, 68 percent of respondents say having to deal with passwords being stolen or compromised followed by employees using weak passwords (67 percent of respondents).

Figure 22. What is your biggest pain point about employees and their passwords?
Two choices allowed



Biometrics or voice recognition are most often used to protect passwords. Figure 23 lists possible measures companies can take to safeguard employees' passwords. The top choices are to have an alternative to keyboard entry (46 percent of respondents), mandate periodic password changes (44 percent of respondents), require more than one authentication system such as 2FA (40 percent of respondents) and monitor third-party sites where compromised passwords are shared (40 percent of respondents).

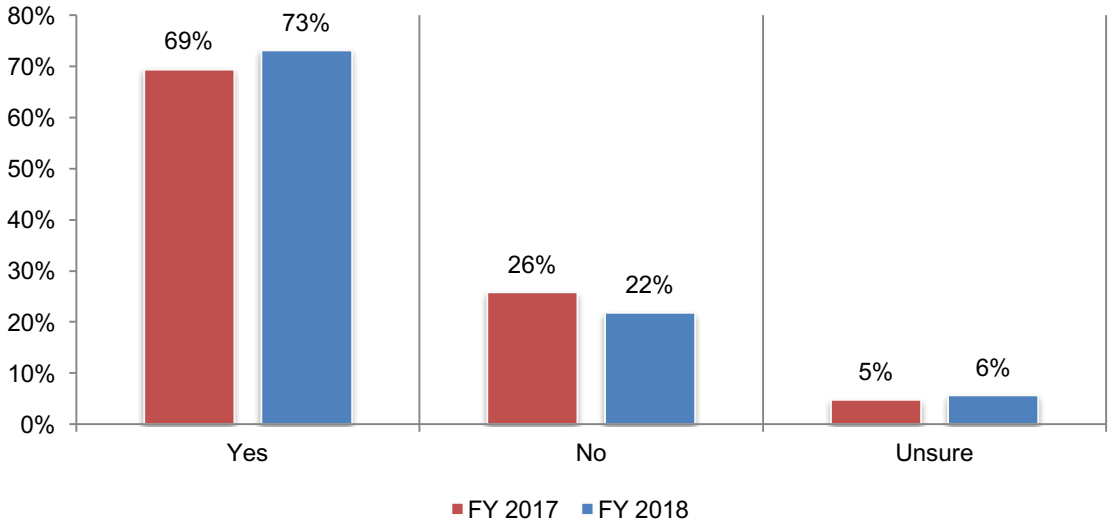
Figure 23. Does your organization take any of the following steps to safeguard passwords?
More than one choice allowed



More respondents in this year's research say their companies have implemented SSO either fully (31 percent) or partially implemented (27 percent). SSO is defined as a property of access control of multiple related, yet independent, software systems. A user logs in with a single ID and password to gain access to a connected system or systems without using different usernames or passwords; or, in some configurations, seamlessly sign on at each system.

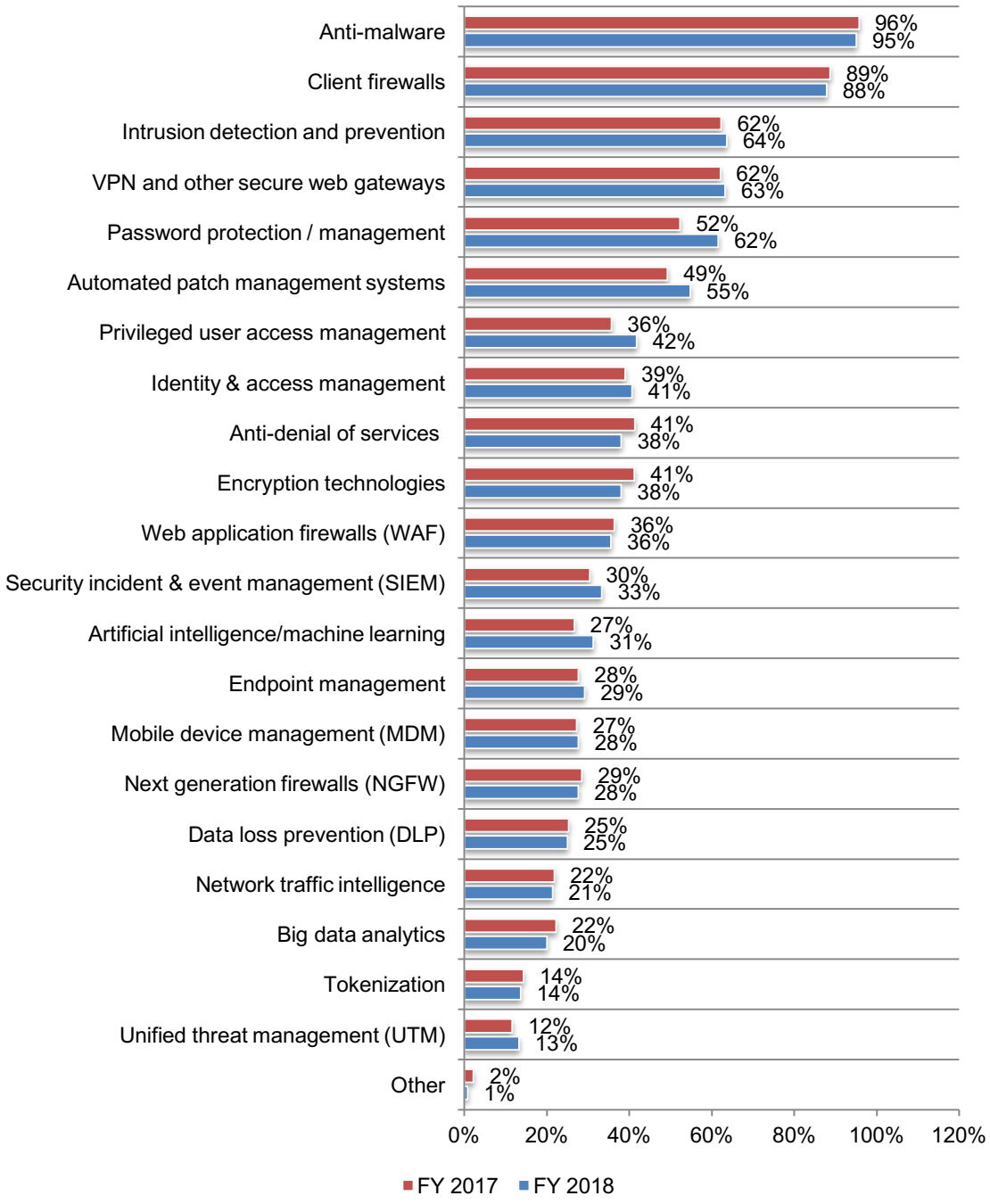
As can be seen in Figure 24, these respondents largely believe SSO increases the security of user access to their companies' applications and data (73 percent).

Figure 24. Does SSO simplify and increase the security of user access to your organization's applications and data?



Password protection and management has increased in importance. According to Figure 25, almost all (95 percent) respondents believe anti-malware is critical. Nearly as many say client firewalls (88 percent of respondents) are important. Password protection and management has increased significantly in importance since 2017 (from 52 percent of respondents to 62 percent of respondents). Also increasing are automated patch management systems (49 percent of respondents to 55 percent of respondents) and privileged user access management (from 36 percent of respondents to 42 percent of respondents).

Figure 25. Security technologies considered essential and very important
More than one choice allowed



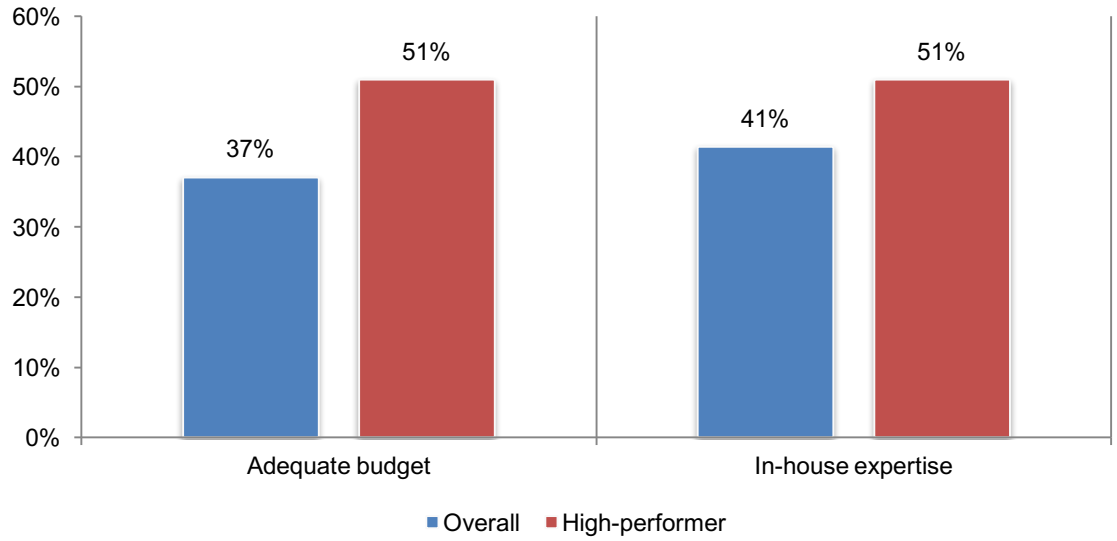
The best practices of high-performing companies

In this section, we present a special analysis of the 115 respondents from high-performing companies. These respondents say their companies are highly effective at mitigating risks, vulnerabilities and attacks across the enterprise. We compare their responses to the overall sample of respondents to learn the best practices of companies that are highly effective in mitigating the risk of data breaches and cyber attacks.

High-performing companies have higher budgets and in-house expertise. As shown in Figure 26, more than half of respondents (51 percent) in high-performing companies vs. 37 percent of respondents in the overall sample say their budget is adequate for achieving a strong IT security posture. High-performing companies are also allocating a higher percentage of the IT budget to IT security (15 percent vs. 12 percent).

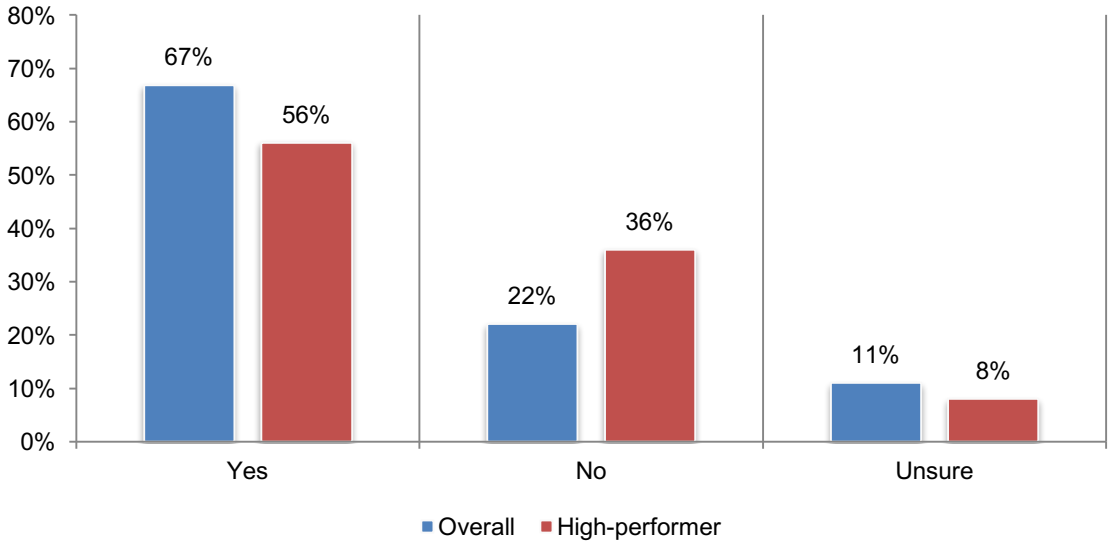
A larger budget is helpful in staffing the IT security function with experts. Fifty-one percent of respondents say their companies have the necessary in-house expertise for achieving a strong security posture. An average of 41 percent of the IT staff support IT security operations. In contrast, an average of only 36 percent of the IT staff supports IT security operations in the overall sample.

Figure 26. Differences in perceptions about budget and in-house expertise
Yes responses presented



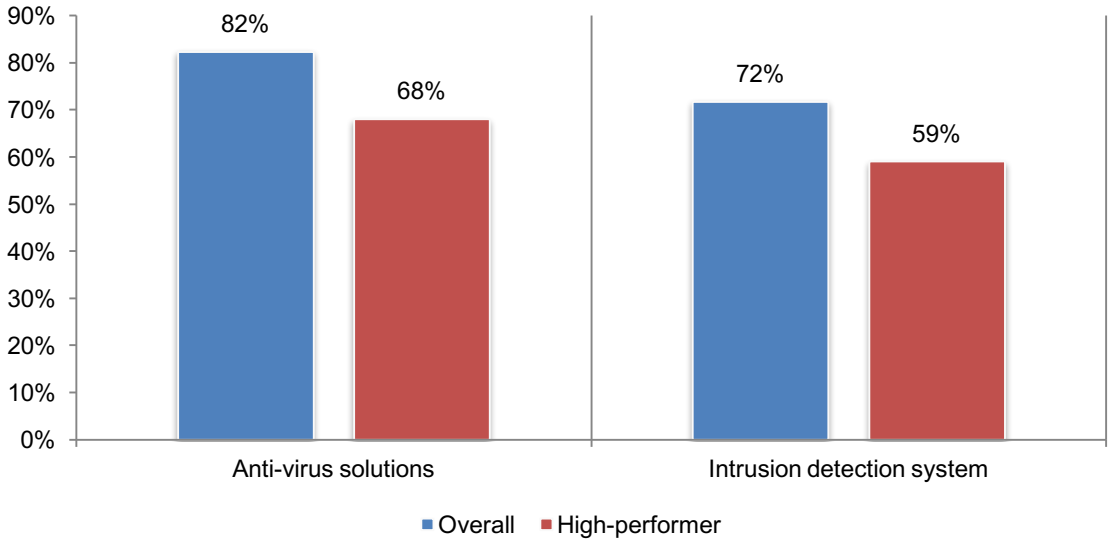
High-performing companies are less likely to experience a cyber attack. As shown in Figure 27, 67 percent of respondents in the overall sample had a cyber attack in the past 12 months as opposed to 56 percent of respondents in high-performing companies.

Figure 27. Has your organization experienced a cyber attack in the past 12 months?



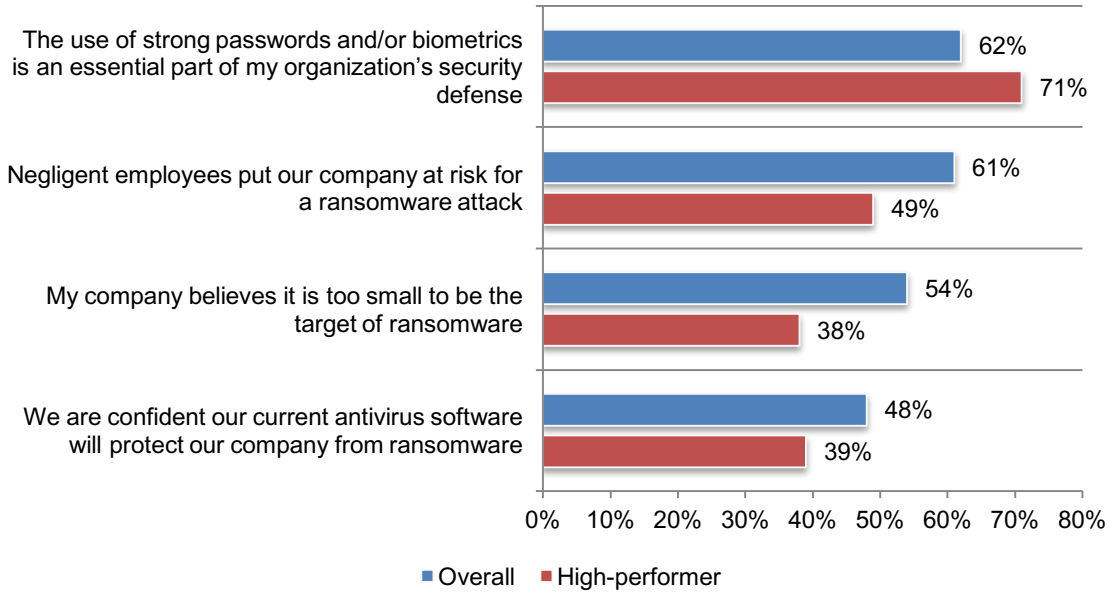
As shown in Figure 28, high-performing companies are less likely to experience exploits where malware evaded intrusion detection systems and anti-virus solutions.

Figure 28. Has your organization experienced exploits where malware evaded intrusion detection systems and anti-virus solutions?
Yes responses presented



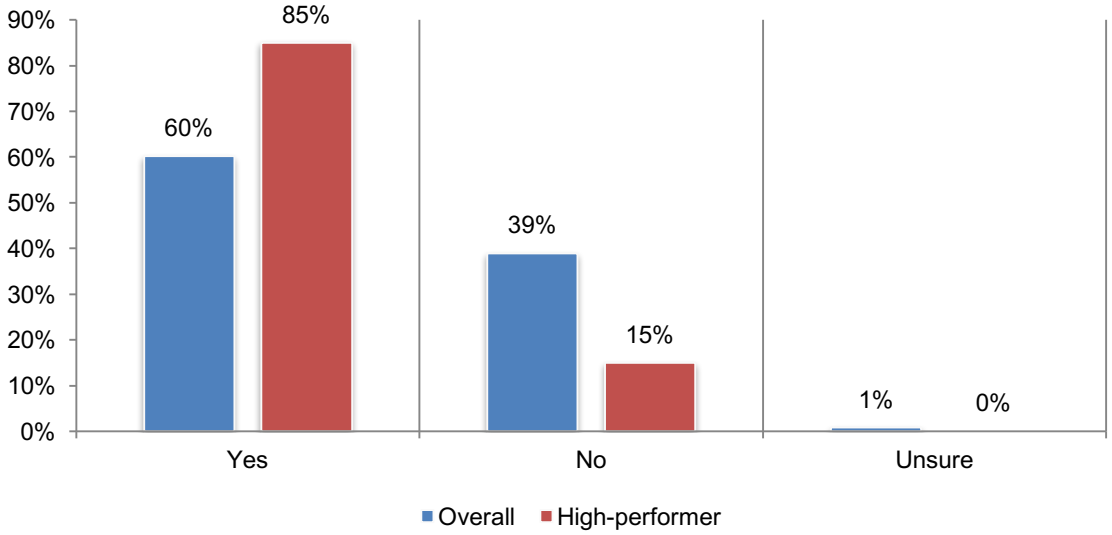
High-performing companies are more likely to require the use of strong passwords and/or biometrics. According to Figure 29, 71 percent of respondents from high-performing companies vs. 62 percent of respondents in the overall sample say the use of strong passwords and/or biometrics is an essential part of their organization's security defense. Respondents in high-performing companies are less likely to agree that negligent employees put their companies at risk for a ransomware attack, that their companies are too small to be a target of ransomware. They are also less confident that their current antivirus software will protect their companies from ransomware.

Figure 29. Perceptions about password security and ransomware
Strongly agree and Agree responses combined



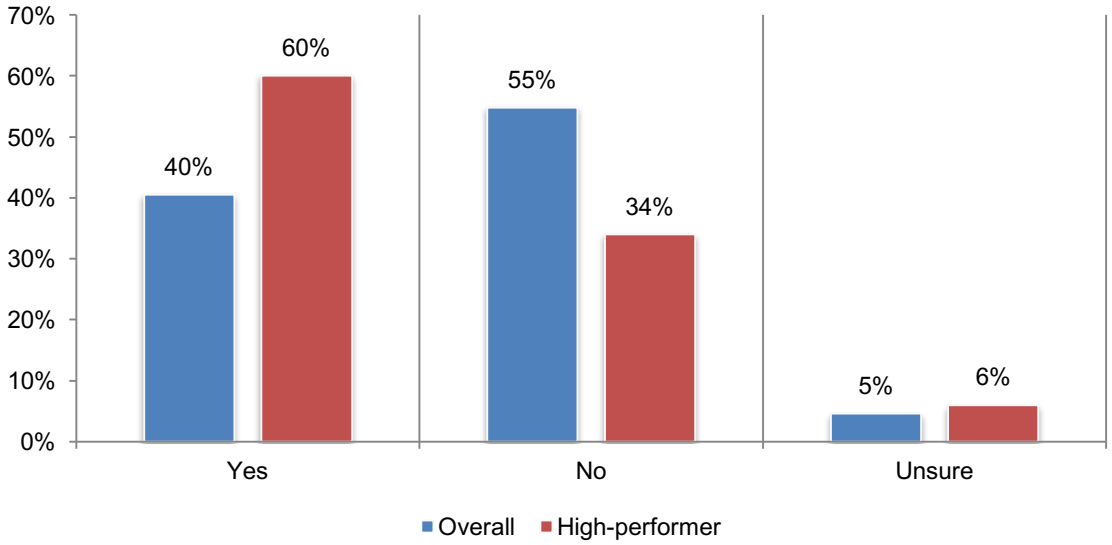
High-performing companies are more likely to have an incident response plan. According to Figure 30, 85 percent of respondents from high-performing companies have an incident response plan vs. 60 percent of the overall sample of respondents say they have such a plan.

Figure 30. Does your company have an incident response plan?



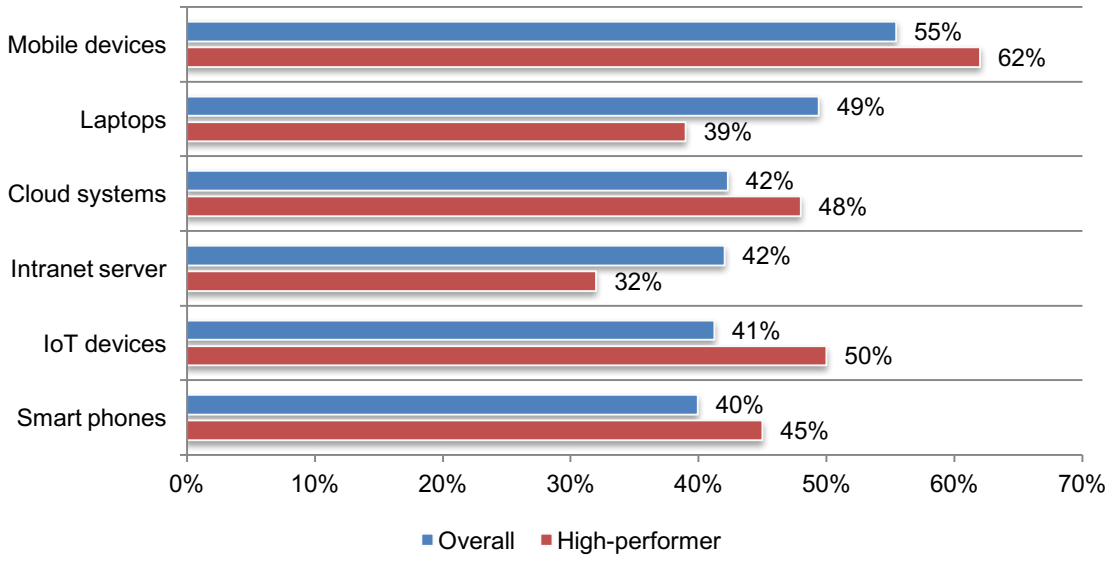
More high-performing companies have password policies for employees. As shown in Figure 31, 60 percent of respondents from high-performing companies say their companies have a password policy vs. 40 percent of respondents in the overall sample.

Figure 31. Does your company have a password policy for employees?



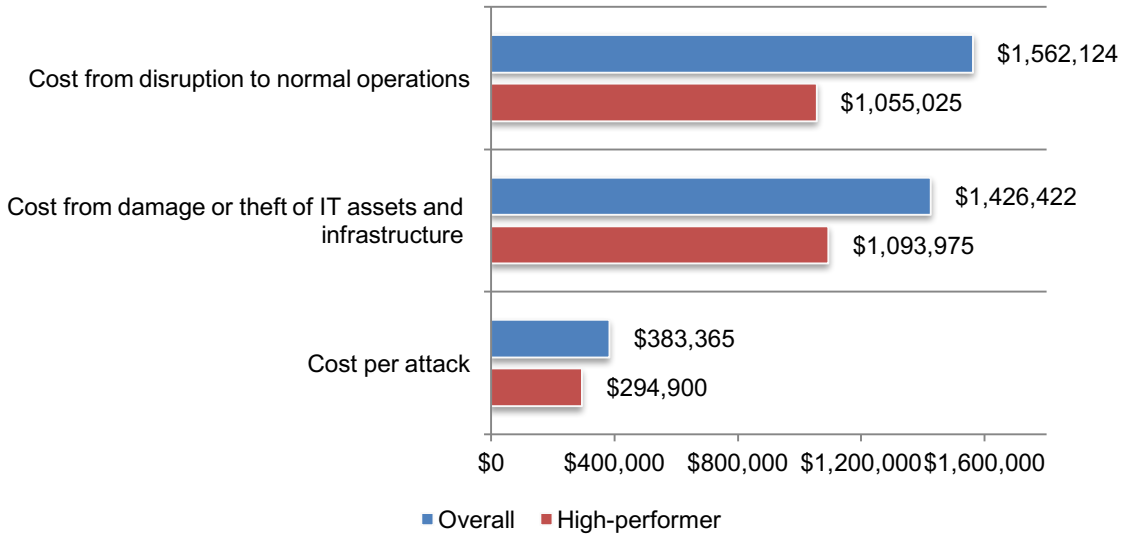
High-performing companies are most likely to believe mobile devices are the most vulnerable endpoints. These companies are also most likely to say IoT devices and cloud systems are vulnerable entry points and less likely to consider laptops and Intranet servers to be vulnerable entry points.

Figure 32. What are the most vulnerable endpoints or entry points to your companies' networks and enterprise systems?
More than one response permitted



The financial consequences following a security incident are much less severe for high-performing companies. According to Figure 33, the benefit of having a more effective security strategy is a lower cost of the compromises companies experienced. The biggest difference between the two groups of respondents is the cost from disruption to normal operations.

Figure 33. The cost of compromises
Extrapolated values (US$)



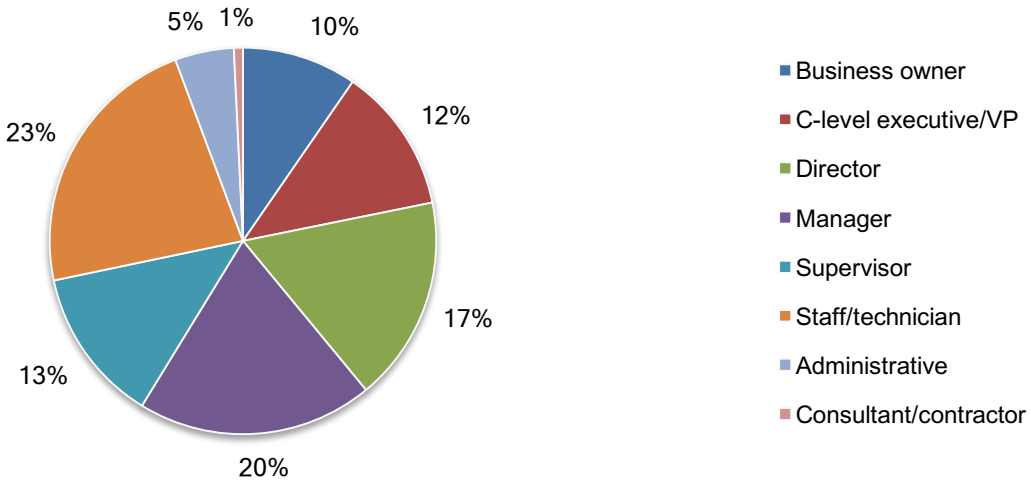
Part 3. Methods

The survey's sampling frame comprised of 28,919 IT practitioners and IT security practitioners from companies in the United States and United Kingdom; these companies had headcounts ranging from less than 100 to 1,000. Table 1 shows that there were 1,149 returned surveys. After screening and reliability checks, we removed 104 surveys. Thus, the final sample consisted of 1,045 surveys (a 3.6 percent response rate).

Table 1. Sample response	Freq	Pct%
Sampling frame	28,919	100.0%
Total returns	1,149	4.0%
Rejected or screened surveys	104	0.4%
Final sample	1,045	3.6%

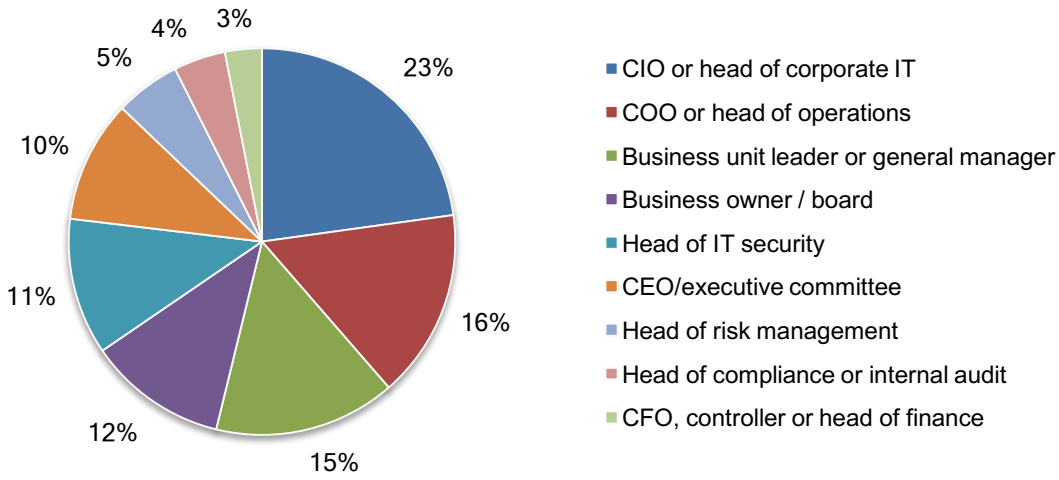
Pie Chart 1 reports the respondents' organizational level within their companies. By design, 72 percent of respondents are at or above the supervisory levels.

Pie Chart 1. Position level within the organization



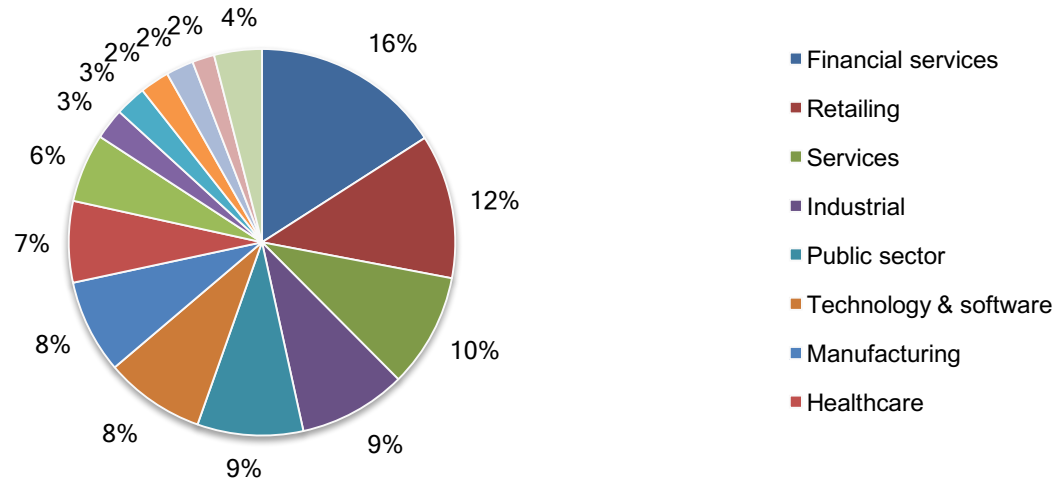
As shown in Pie Chart 2, 23 percent of respondents report directly to their company's CIO or head of corporate IT, 16 percent report to the company's COO or head of operations, 15 percent report to the company's business unit leader or general manager, 12 percent report to the business owner or board, and 11 percent of respondents report to the company's head of IT security.

Pie Chart 2. The commands reported to in your current role



Pie Chart 3 provides the industries of the respondents' companies. Financial services (16 percent of respondents) is the largest segment, followed by retail (12 percent of respondents), services (10 percent of respondents), and industry (9 percent of respondents) and the public sector (also 9 percent of respondents).

Pie Chart 3. Primary industry focus



Part 4. Caveats to this study

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

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

- Sampling-frame bias: The accuracy is based on contact information and the degree to which the list is representative of individuals who are IT or IT security practitioners. We also acknowledge that the results may be biased by external events such as media coverage. Finally, because we used a Web-based collection method, it is possible that non-Web responses by mailed survey or telephone call would result in a different pattern of findings.

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

Appendix: Detailed Survey Results

The following tables provide the frequency or percentage frequency of responses to all survey questions contained in this study. All survey responses were captured from July 19 2018 to July 31, 2018.

Survey response	FY 2018	FY 2017
Total sampling frame	28,919	29,988
Total returns	1,149	1,152
Rejected surveys	104	112
Final sample	1,045	1,040
Response rate	3.6%	3.5%
Sample weight	1.00	1.00

Part 1. Screening Questions

S1. What range best describes the full-time employee headcount of your organization?	FY 2018	FY 2017
Less than 100	157	168
100 to 250	160	172
251 to 500	229	209
501 to 750	245	252
751 to 1,000	254	239
More than 1,000 [STOP]	-	-
Total	1,045	1,040

S2. What best describes your role in managing the IT security function or activities within your organization? Check all that apply.	FY 2018	FY 2017
Setting IT security priorities	66%	62%
Managing IT security budgets	57%	57%
Selecting vendors and contractors	46%	49%
Determining IT security strategy	45%	46%
Evaluating program performance	44%	44%
None of the above [STOP]	0%	0%
Total	259%	257%

S3. How do you rate your level of involvement in the evaluation, selection, and/or implementation of IT security products or services in your organization?	FY 2018	FY 2017
Very high level of involvement	33%	34%
High level of involvement	43%	43%
Moderate level of involvement	19%	19%
Low level of involvement	5%	5%
Not involved [STOP]	0%	0%
Total	100%	100%

Part 2: Security Posture

Q1. How would you describe your organization's IT security posture (in terms of its effectiveness at mitigating risks, vulnerabilities and attacks across the enterprise)? 1 = not effective to 10 = very effective	FY 2018	FY 2017
1 or 2	9%	11%
3 or 4	34%	38%
5 or 6	28%	30%
7 or 8	17%	14%
9 or 10	11%	7%
Total	100%	100%
Extrapolated value	5.24	4.87

Q2. What challenges keep your organization's IT security posture from being fully effective? Please choose the top three challenges.	FY 2018	FY 2017
Insufficient budget (money)	55%	56%
Insufficient personnel	74%	73%
Lack of in-house expertise	37%	39%
Lack of clear leadership	5%	5%
Insufficient enabling security technologies	38%	43%
No understanding how to protect against cyber attacks	47%	47%
Management does not see cyber attacks as a significant risk	4%	5%
Lack of collaboration with other functions	17%	11%
Not a priority issue	23%	22%
Other	0%	0%
Total	300%	300%

Q3. What types of information are you most concerned about protecting from cyber attackers? Please choose two top choices.	FY 2018	FY 2017
Customer credit or debit card information	40%	37%
Financial information	28%	26%
Intellectual property	51%	48%
Customer records	57%	63%
Employee records	15%	16%
Business correspondence	8%	8%
Other (please specify)	1%	1%
Total	200%	200%

Q4. Who determines IT security priorities in your organization? Top two choices.	FY 2018	FY 2017
Business owners	23%	24%
Board of directors	9%	9%
Chief executive	31%	34%
Head of operations	30%	33%
Chief information officer (CIO)	31%	33%
Chief technology officer (CTO)	7%	8%
Chief information security officer (CISO)	10%	11%
Compliance officer	7%	6%
General counsel	3%	4%
Lines of business	14%	9%
No one function determines IT security priorities	35%	30%
Other (please specify)	1%	0%
Total	200%	200%

Q5. Is your organization's budget adequate for achieving a strong IT security posture?	FY 2018	FY 2017
Yes	37%	37%
No	52%	52%
Unsure	11%	11%
Total	100%	100%

Q6. What percentage of your organization's IT budget is dedicated to IT security activities?	FY 2018	FY 2017
Less than 5%	16%	19%
5 to 10%	31%	27%
11 to 15%	23%	25%
16 to 20%	18%	19%
21 to 25%	6%	6%
26 to 30%	3%	3%
31 to 40%	3%	1%
41 to 50%	0%	0%
More than 50%	0%	0%
Total	100%	100%
Extrapolated value	12.1%	11.6%

Q7. Does your organization have the in-house expertise necessary for achieving a strong IT security posture?	FY 2018	FY 2017
Yes	41%	38%
No	48%	52%
Unsure	11%	10%
Total	100%	100%

Q8. What percentage of your organization's IT personnel support IT security operations?	FY 2018	FY 2017
Less than 5%	0%	0%
5 to 10%	4%	5%
11 to 15%	7%	8%
16 to 20%	10%	12%
21 to 25%	14%	15%
26 to 30%	10%	11%
31 to 40%	8%	8%
41 to 50%	11%	8%
More than 50%	35%	33%
Total	100%	100%
Extrapolated value	36%	36%

Q9a. What percentage of your organization's IT security operations are supported by managed security service providers (MSSPs)?	FY 2018	FY 2017
None [Skip Q10]	41%	47%
Less than 10%	9%	10%
10% to 25%	8%	12%
26% to 50%	11%	11%
51% to 75%	18%	9%
76% to 100%	14%	10%
Total	100%	100%
Extrapolated value	29%	21%

Q9b. Following are core services typically provided by MSSPs. Please check all services provided by MSSPs to support your organization's IT security posture. *not a response in 2017	FY 2018	FY 2017
Monitored or managed firewalls or intrusion prevention systems (IPSs)	66%	68%
Monitored or managed intrusion detection systems (IDSs)	43%	50%
Monitored or managed multifunction firewalls	30%	28%
Managed or monitored security gateways for messaging or Web traffic	39%	43%
Security analysis and reporting of events collected from IT infrastructure logs	20%	20%
Reporting associated with monitored/managed devices and incident response	17%	17%
Managed vulnerability scanning of networks, servers, databases or applications	36%	40%
Distributed denial of service (DDoS) protection	14%	13%
Monitoring or management of customer-deployed security information and event management (SIEM) technologies	8%	8%
Monitoring and/or management of advanced threat defense technologies	11%	10%
Identity and access management *	22%	
Privileged access management *	17%	
Total	323%	298%

Q10. Does your organization strive to comply with leading IT security guidelines or standards? Please check the standards that your organization attempts to comply with.	FY 2018	FY 2017
PCI DSS	46%	43%
ISO 27001/2	6%	6%
SOC 2/3	17%	15%
COBIT	9%	10%
SOX 404	18%	17%
NIST	17%	17%
HIPAA/HiTECH	8%	10%
None of the above	31%	41%
Other (please specify)	6%	6%
Total	158%	165%

Q11. What percent of your organization's business-critical applications are accessed from mobile devices such as smart phones, tablets and others? Your best guess is welcome.	FY 2018
Zero	0%
Less than 10%	5%
11 to 25%	17%
36 to 50%	37%
51 to 75%	30%
76 to 100%	11%
Total	100%
Extrapolated value	45%

Part 3: Cyber Attacks

Q12a. Has your organization experienced a cyber attack in the past 12 months?	FY 2018	FY 2017
Yes	67%	61%
No	22%	24%
Unsure	11%	14%
Total	100%	100%

Q12b. If yes, what best describes the type of attacks experienced by your organization? Please select all that apply.	FY 2018	FY 2017
Advanced malware / zero day attacks	24%	16%
Phishing / social engineering	52%	48%
SQL injection	20%	24%
Cross-site scripting	9%	10%
Denial of services	26%	26%
Compromised / stolen devices	34%	30%
Malicious insider	12%	11%
General malware	37%	36%
Web-based attack	47%	43%
Other (please specify)	4%	3%
Total	266%	248%

Q13a. Has your organization ever experienced situations when exploits and malware have evaded your intrusion detection system?	FY 2018	FY 2017
Yes	72%	66%
No	20%	22%
Unsure	8%	12%
Total	100%	100%

Q13b. Has your organization ever experienced situations when exploits and malware have evaded your anti-virus solutions?	FY 2018	FY 2017
Yes	82%	81%
No	12%	13%
Unsure	6%	5%
Total	100%	100%

Please rate the following statements using the five-point scale provided below each item.		
Q14a. Cyber attacks experienced by my organization are becoming more **targeted**.	**FY 2018**	**FY 2017**
Strongly agree	28%	27%
Agree	34%	33%
Unsure	16%	19%
Disagree	13%	13%
Strongly disagree	9%	9%
Total	100%	100%

Q14b. Cyber attacks experienced by my organization are becoming more **sophisticated**.	**FY 2018**	**FY 2017**
Strongly agree	23%	26%
Agree	36%	33%
Unsure	21%	21%
Disagree	13%	12%
Strongly disagree	8%	8%
Total	100%	100%

Q14c. Cyber attacks experienced by my organization are becoming more **severe** in terms of negative consequences (such as financial impact).	**FY 2018**	**FY 2017**
Strongly agree	26%	27%
Agree	34%	32%
Unsure	22%	24%
Disagree	12%	12%
Strongly disagree	5%	5%
Total	100%	100%

Q14d. The use of strong passwords and/or biometrics is an essential part of my organization's security defense.	**FY 2018**	**FY 2017**
Strongly agree	31%	28%
Agree	31%	32%
Unsure	20%	19%
Disagree	12%	13%
Strongly disagree	7%	7%
Total	100%	100%

Q15a. My company believes it is too small to be the target of ransomware.	**FY 2018**	**FY 2017**
Strongly agree	22%	20%
Agree	32%	31%
Unsure	15%	15%
Disagree	22%	23%
Strongly disagree	10%	11%
Total	100%	100%

Q15b. My company would never pay ransom even if we lost the data.	FY 2018	FY 2017
Strongly agree	25%	22%
Agree	26%	27%
Unsure	26%	26%
Disagree	16%	17%
Strongly disagree	7%	8%
Total	100%	100%

Q15c. Negligent employees put our company at risk for a ransomware attack.	FY 2018	FY 2017
Strongly agree	24%	24%
Agree	37%	34%
Unsure	14%	15%
Disagree	18%	18%
Strongly disagree	7%	8%
Total	100%	100%

Q15d. A ransomware attack would have serious financial consequences for our company.	FY 2018	FY 2017
Strongly agree	25%	23%
Agree	31%	35%
Unsure	21%	21%
Disagree	18%	16%
Strongly disagree	5%	6%
Total	100%	100%

Q15e. We are confident our current antivirus software will protect our company from ransomware.	FY 2018	FY 2017
Strongly agree	22%	22%
Agree	26%	26%
Unsure	20%	19%
Disagree	24%	24%
Strongly disagree	9%	9%
Total	100%	100%

Q16. Have you or your company experienced ransomware?	FY 2018	FY 2017
Yes, within the past 3 months	11%	10%
Yes, within the past 6 months	17%	14%
Yes, within the past 12 months	19%	18%
Yes, more than 12 months ago	14%	9%
No (Skip to Part 4)	39%	48%
Total	100%	100%

Q17. How many ransomware incidents have you or your company experienced?	FY 2018	FY 2017
1	44%	47%
2 to 5	36%	31%
6 to 10	15%	17%
Greater than 10	5%	5%
Total	100%	100%

Q18. How was the ransomware unleashed? Please select all that apply.	FY 2018	FY 2017
Phishing/social engineering	79%	79%
Insecure or spoofed website	29%	27%
Social media	12%	14%
Malvertisements	13%	14%
Other	3%	4%
Total	135%	139%

Q19. What type of device was compromised by ransomware? Please select all that apply.	FY 2018	FY 2017
Desktop/laptop	82%	78%
Mobile device	41%	37%
Server	33%	34%
Other	3%	4%
Total	160%	152%

Q20. How much was the ransom?	FY 2018	FY 2017
Less than $100	10%	13%
$100 to $500	26%	30%
$501 to $1,000	30%	30%
$1,001 to $5,000	12%	13%
$5,001 to $10,000	10%	7%
More than $10,000	12%	8%
Total	100%	100%
Extrapolated value (US$)	1,466	$941

**UK amount was converted from GBP to dollars*

Q21a. Did your company pay the ransom?	FY 2018	FY 2017
Yes	70%	60%
No	30%	40%
Total	100%	100%

Q21b. If you did not pay a ransom, why not?	FY 2018	FY 2017
We had a full backup	73%	67%
Company policy is not to pay ransom	32%	29%
Law enforcement told us not to pay it	10%	9%
We did not believe the bad guys would provide the decryption cypher	49%	52%
Compromised data was not critical for our business	20%	21%
Other	3%	3%
Total	186%	182%

Part 4. Data breach experience

Q22a. Has your organization experienced an incident involving the loss or theft of sensitive information about customers, target customers or employees (a.k.a. data breach) in the past 12 months?	FY 2018	FY 2017
Yes	58%	54%
No [skip to Part 5]	42%	46%
Total	100%	100%

Q22b. If yes, with respect to your organization's largest breach over the past 12 months, how many individual records were lost or stolen?	FY 2018	FY 2017
Less than 100	33%	33%
100 to 500	23%	26%
501 to 1,000	15%	15%
1,001 to 10,000	14%	14%
10,001 to 50,000	8%	7%
50,001 to 100,000	6%	4%
100,001 to 1,000,000	1%	1%
More than 1,000,000	0%	0%
Total	100%	100%
Extrapolated value	10,848	9,350

Q22c. If yes, what were the root causes of the data breaches experienced by your organization? Please select that apply.	FY 2018	FY 2017
Malicious insider	7%	7%
External (hacker) attacks	37%	33%
Negligent employee or contractor	60%	54%
Error in system or operating process	30%	34%
Third party mistakes	43%	43%
Other (please specify)	1%	2%
Don't know	31%	32%
Total	209%	206%

Q23. Does your organization have an incident response plan for responding to cyber attacks and data breaches?	FY 2018	FY 2017
Yes	60%	55%
No	39%	44%
Unsure	1%	1%
Total	100%	100%

Part 5. Password practices and policies

Q24a. Does your organization have **visibility in**to employees' password practices?	FY 2018	FY 2017
Yes	45%	41%
No	50%	52%
Unsure	4%	7%
Total	100%	100%

Q24b. If yes, are you able to determine the following steps taken by employees? Please select all that apply.	FY 2018
Using unique or strong passwords	46%
Making periodic changes to passwords	47%
Sharing passwords with others	24%
The number of passwords each employee has	46%
Total	163%

Q25a. Does your organization have a policy pertaining to employees' use of passwords?	FY 2018	FY 2017
Yes	47%	43%
No	49%	52%
Unsure	5%	5%
Total	100%	100%

Q25b. If yes, does your organization strictly enforce this policy?	FY 2018	FY 2017
Yes	32%	32%
No	64%	63%
Unsure	4%	5%
Total	100%	100%

Q26a. Does your organization require employees to use a password manager?	FY 2018
Yes	22%
No	74%
Unsure	4%
Total	100%

Q26b. If no, what does your organization use to manage and protect its passwords?	FY 2018
Spreadsheets	51%
Manually write them down on paper or sticky notes	30%
Human memory	53%
Browser extension	18%
Other (please specify)	4%
Total	157%

Q27. What is your biggest pain point about employees and their passwords? Please select your top two choices.	FY 2018
Time spent resetting passwords	58%
Changing passwords when an employee leaves his job	46%
Employees using weak passwords	67%
Employee passwords being stolen or compromised	68%
Employee adoption of best practices	38%
Total	277%

Q28. Does your organization take any of the following steps? Please select all that apply.	FY 2018
Periodic password changes	44%
Assign randomly chosen passwords	30%
Require minimum password lengths	32%
Prohibit employees from reusing the same password on internal systems	34%
Provide an alternative to keyboard entry (i.e., voice recognition, biometrics)	46%
Require more than one authentication system such as 2FA	40%
Monitor third-party sites where compromised passwords are shared	40%
None of the above	22%
Other (please specify)	1%
Total	289%

Q29. What would prevent your organization from adopting biometrics?	FY 2018
Too costly	43%
Difficult to enforce	48%
Too risky if biometric information was lost	43%
Still need passwords as backup	39%
Total	172%

Single sign-on (SSO) is a property of access control of multiple related, yet independent, software systems. With this property, a user logs in with a single ID and password to gain access to a connected system or systems without using different usernames or passwords, or in some configurations seamlessly sign on at each system.

Q30. Does your organization use SSO?	FY 2018	FY 2017
Yes, fully implemented across the enterprise	31%	27%
Yes, partially implemented across the enterprise	27%	24%
No (skip to Q32)	42%	50%
Total	100%	100%

Q31. Do you believe that SSO increases the security of user access to your organization's applications and data?	FY 2018	FY 2017
Yes	73%	69%
No	22%	26%
Unsure	6%	5%
Total	101%	100%

Q32. In your opinion, how does the use of mobile devices such as tablets and smart phones to access business-critical applications and IT infrastructure affect your organization's security posture?	FY 2018	FY 2017
Improves security posture	6%	6%
Diminishes security posture	49%	48%
No affect on security posture	33%	35%
Cannot determine	12%	11%
Total	100%	100%

Part 6. Enabling Security Technologies

Q33. Do the security technologies currently used by your organization detect and block most cyber attacks?	FY 2018	FY 2017
Yes	40%	39%
No	60%	61%
Total	100%	100%

Q34. How important are each of the following security technologies used your organization **today**? Please use the following importance scale for each technology listed. Leave blank if a given technology is not deployed by your organization. % Essential and Very Important responses combined.	FY 2018	FY 2017
Anti-malware	95%	96%
Anti-denial of services	38%	41%
Artificial intelligence/machine learning	31%	27%
Privileged user access management	42%	36%
Automated patch management systems	55%	49%
Password protection / management	62%	52%
Big data analytics	20%	22%
Data loss prevention (DLP)	25%	25%
Encryption technologies	38%	41%
Tokenization	14%	14%
Endpoint management	29%	28%
Mobile device management (MDM)	28%	27%
Client firewalls	88%	89%
Identity & access management	41%	39%
Intrusion detection and prevention	64%	62%
Network traffic intelligence	21%	22%
Next generation firewalls (NGFW)	28%	29%
VPN and other secure web gateways	63%	62%
Security incident & event management (SIEM)	33%	30%
Unified threat management (UTM)	13%	12%
Web application firewalls (WAF)	36%	36%
Other	1%	2%
Total	864%	842%

Q35. In your opinion, what are the most vulnerable endpoints or entry points to your organization's networks and enterprise systems?	FY 2018	FY 2017
Desktops	19%	21%
Laptops	49%	43%
Tablets	19%	20%
Smart phones	40%	39%
Web server	33%	30%
Intranet server	42%	36%
Routers	6%	6%
Portable storage devices (including USBs)	7%	8%
Cloud systems	42%	38%
Mobile devices	55%	56%
IoT devices*	41%	
Other (please specify)	1%	2%
Total	356%	300%

**Internet of things*

Part 7. The cost of compromises

Q36a. Approximately, how much did damage or theft of IT assets and infrastructure cost your organization over the past 12 months?	FY 2018	FY 2017
We had no compromises	32%	34%
Less than $5,000	8%	8%
$5,001 to $10,000	2%	2%
$10,001 to $50,000	5%	6%
$50,001 to $100,000	5%	6%
$100,001 to $250,000	7%	8%
$250,001 to $500,000	9%	8%
$500,001 to $999,999	8%	9%
$1 million to $5 million	11%	10%
$5 million to $10 million	11%	6%
More than $10 million	2%	1%
Total	100%	99%
Extrapolated value (US$)	$1,426,422	$1,027,053

**UK amount was converted from GBP to dollars*

Q36b. Approximately, how much did disruption to normal operations cost your organization over the past 12 months?	FY 2018	FY 2017
We had no compromises	32%	33%
Less than $5,000	8%	8%
$5,001 to $10,000	2%	2%
$10,001 to $50,000	6%	6%
$50,001 to $100,000	4%	4%
$100,001 to $250,000	7%	10%
$250,001 to $500,000	9%	9%
$500,001 to $999,999	8%	9%
$1 million to $5 million	10%	9%
$5 million to $10 million	7%	6%
More than $10 million	5%	3%
Total	100%	100%
Extrapolated value (US$)	$1,562,124	$1,207,965

Q37a. Have you had an attack involving the compromise of employees' passwords in the past year?	FY 2018
Yes	40%
No	52%
Unsure	8%
Total	100%

Q37b. If yes, how much did each attack cost your organization?	FY 2018
Less than $10,000	3%
$10,001 to $50,000	7%
$50,001 to $100,000	14%
$100,001 to $250,000	29%
$250,001 to $500,000	22%
$500,001 to $1,000,000	13%
More than $1,000,000	12%
Total	100%
Extrapolated value (US$)	$383,365

Part 8. General Data Protection Regulation (GDPR)	
Q38. Is your organization required to comply with GDPR?	FY 2018
Yes	72%
No [Skip to Part 9]	19%
Unsure [Skip to Part 9]	9%
Total	100%

Q39. If yes, did compliance require significant changes in your privacy and security strategies?	FY 2018	FY 2017
Yes, significant change	41%	37%
Yes, some change	41%	37%
Yes, nominal change	11%	18%
No change	7%	8%
Total	100%	100%

Q40. Using the following 10-point scale, please rate your organization's level of compliance with the GDPR. 1 = not ready and 10 = ready.	FY 2018
1 or 2	18%
3 or 4	23%
5 or 6	20%
7 or 8	21%
9 or 10	19%
Total	100%
Extrapolated value	5.48

Part 9. Role & Organizational Characteristics

D1. What best describes your position level within the organization?	FY 2018	FY 2017
Business owner	10%	10%
C-level executive/VP	12%	11%
Director	17%	17%
Manager	20%	21%
Supervisor	13%	12%
Staff/technician	23%	24%
Administrative	5%	4%
Consultant/contractor	1%	1%
Total	100%	100%

D2. Which of the following commands do you report to in your current role?	FY 2018	FY 2017
Business owner / board	12%	12%
CEO/executive committee	10%	9%
COO or head of operations	16%	16%
CFO, controller or head of finance	3%	3%
CIO or head of corporate IT	23%	27%
Business unit leader or general manager	15%	13%
Head of compliance or internal audit	4%	4%
Head of risk management	5%	5%
Head of IT security	11%	11%
Total	100%	100%

D3. What best describes your organization's primary industry classification?	FY 2018	FY 2017
Aerospace & defense	1%	1%
Agriculture & food services	1%	2%
Communications	2%	2%
Construction and real estate	3%	3%
Consumer goods	6%	6%
Education & research	2%	2%
Entertainment, media and publishing	1%	3%
Financial services	16%	14%
Healthcare	7%	7%
Industrial	9%	9%
Logistics and distribution	1%	1%
Manufacturing	8%	8%
Pharmaceuticals	2%	3%
Public sector	9%	9%
Retailing	12%	12%
Services	10%	9%
Technology & software	8%	7%
Transportation	3%	2%
Total	100%	100%

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

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 companies.

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.

About Keeper Security, Inc.

Keeper Security, Inc. ("Keeper") is transforming the way organizations and individuals protect their passwords and sensitive digital assets to significantly reduce cyber theft. Keeper is the leading provider of *zero-knowledge* security and encryption software covering password management, cybersecurity, dark web monitoring, digital file storage and messaging. Keeper is trusted by millions of people and thousands of businesses to protect their digital assets and help mitigate the risk of a data breach. Keeper is SOC-2 Certified and is also certified for use by the Federal government through the System for Award Management (SAM) and the General Services Administration (GSA). Keeper protects businesses of all sizes across every major industry sector.