2017 State of Cybersecurity in Small & Medium-Sized Businesses (SMB)

Sponsored by Keeper Security

Independently conducted by Ponemon Institute LLC

Publication Date: September 2017

2017 State of Cybersecurity in Small and Medium-Sized Businesses (SMB)

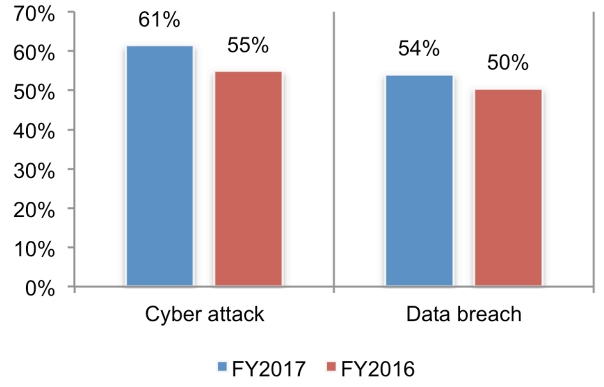
Ponemon Institute, September 2017

Part 1. Introduction

Cyber attacks, ransomware and disruptive technologies, such as the Internet of Things (IoT), challenge the ability of small businesses to safeguard their information assets. In fact, only 21 percent of the companies represented in this study rate their ability to mitigate cyber risks, vulnerabilities and attacks as highly effective. Moreover, more than half (51 percent) have experienced either a successful or unsuccessful ransomware attack.

Ponemon Institute is pleased to present the results of the second annual study on *the State of Cybersecurity in Small and Medium-Sized Businesses* sponsored by Keeper Security. The goal of the study is to track how smaller companies are addressing the same threats larger companies face. Approximately 600 individuals in companies with a headcount from less than 100 to 1,000 participated in this research.

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



As shown in Figure 1, 61 percent of these respondents say their companies have experienced a cyber attack in the past 12 months, and 54 percent report they had data breaches involving customer and employee information in the past 12 months. In the aftermath of these incidents, these companies spent an average of $1,027,053 because of damage or theft of IT assets. In addition, disruption to normal operations cost an average of $1,207,965.

The following are the top 10 trends in the state of cybersecurity in SMBs

1. Cyber attacks affected more SMBs in the past 12 months, an increase from 55 percent to 61 percent of respondents. The most prevalent attacks against smaller businesses are phishing/social engineering and web-based (48 percent and 43 percent of respondents, respectively). More respondents in this year's study say cyber attacks are more targeted, severe and sophisticated.

2. The rise of ransomware is affecting SMBs. In last year's research, only two percent of respondents described the cyber attacks they experienced as ransomware. This year, 52 percent of respondents say their companies experienced a ransomware attack and 53 percent of these respondents say they had more than two ransomware incidents in the past 12 months. Seventy-nine percent of respondent say the ransomware was unleashed through a phishing/social engineering attack.

3. SMBs are having slightly more data breaches involving personal information and the size of data breaches is larger. In the past 12 months, 54 percent of respondents report they had a breach involving sensitive information about customers, target customers or employees, an increase from 50 percent in last year's study. The average size of the breach involved 9,350 individual records, an increase from an average of 5,079 records.

4. Of the respondents who say their organization had a data breach, 54 percent say negligent employees were the root cause of data, an increase from 48 percent of respondents in last year's study. However, similar to last year, almost one-third of companies in this research could not determine the root cause.

5. While only 23 percent of respondents report their organization had a data breach or security incident due to the use of the Internet of Things (IoT), 67 percent of respondents say their organizations are very concerned or concerned about the security of IoT devices in the workplace. Moreover only 29 percent of respondents say they have confidence in their ability to contain or minimize the risk of insecure IoT. In fact, 56 percent of respondents say IoT and mobile devices are the most vulnerable endpoint their organization's networks and enterprise systems.

6. More SMBs are experiencing situations when exploits and malware have evaded their intrusion detection system (an increase from 57 percent of respondents to 66 percent of respondents) and anti-virus solutions (an increase from 76 percent of respondents to 81 percent of respondents).

7. Strong passwords and biometrics continue to be an essential part of the security defense. However, 59 percent of respondents say they do not have visibility into employees' password practices such as the use of unique or strong passwords and sharing passwords with others. This has not improved since last year.

8. Password policies are still not strictly enforced. If a company has a password policy (43 percent of respondents), 68 percent of respondents say they do not strictly enforce it or are unsure. However, more SMBs are requiring employees to use password or biometric to secure access to mobile devices, an increase from 42 percent of respondents to 51 percent of respondents.

9. Personnel, budget and technologies continue to be insufficient to have a strong security posture. As a result, some companies engage managed security service providers to support an average of 36 percent of their IT security operations. The services most often used are monitored or managed firewalls or intrusion prevention systems and intrusion detection systems and security gateways for messaging or Web traffic.

10. Cyber attacks are more costly. The average cost due to damage or theft of IT assets and infrastructure increased from $879,582 to $1,027,053. The average cost due to disruption to normal operations increased from $955,429 to $1,207,965.

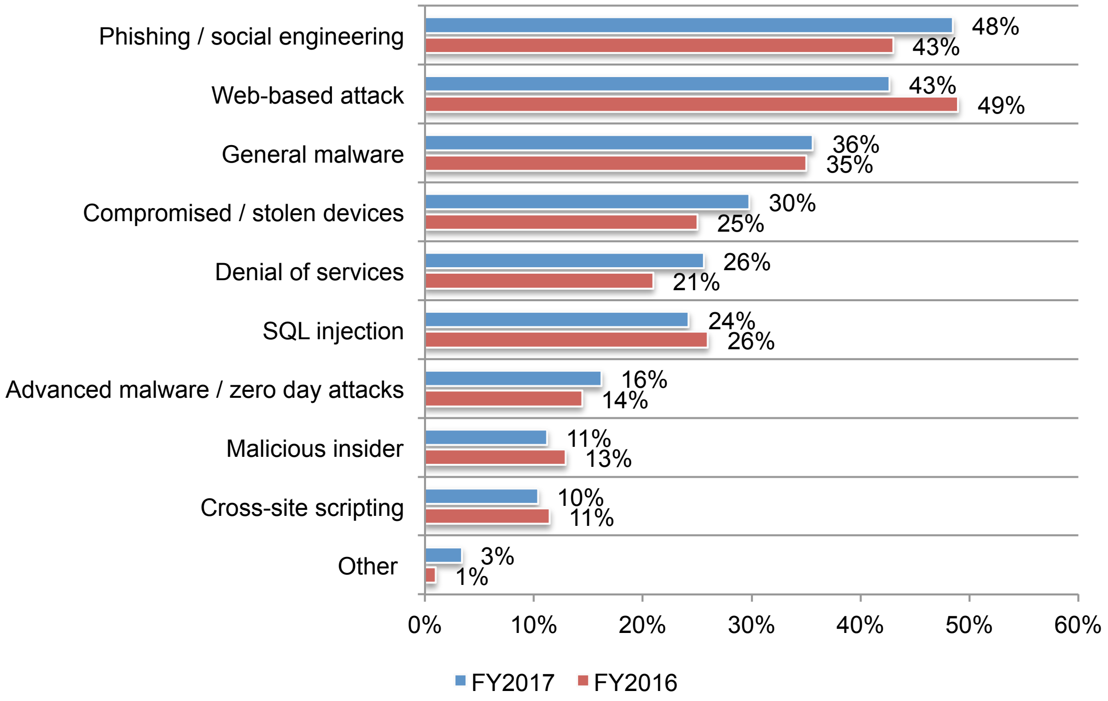
Part 2. Key findings

- Trends in SMB cyber attacks and data breaches
- The rise of SMB ransomware attacks
- IT security posture and governance
- Technologies in place to address the threat
- The impact of the Cloud and mobile on IT security posture

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 and data breach with severe financial consequences (61 percent and 54 percent, respectively). Since last year, phishing/social engineering has replaced web-based attacks (48 percent and 43 percent of respondents, respectively) as the most frequent type of attack, as shown in Figure 2. Compromised/stolen devices and denial of services attacks increased from last year's study (30 percent and 26 percent, respectively).

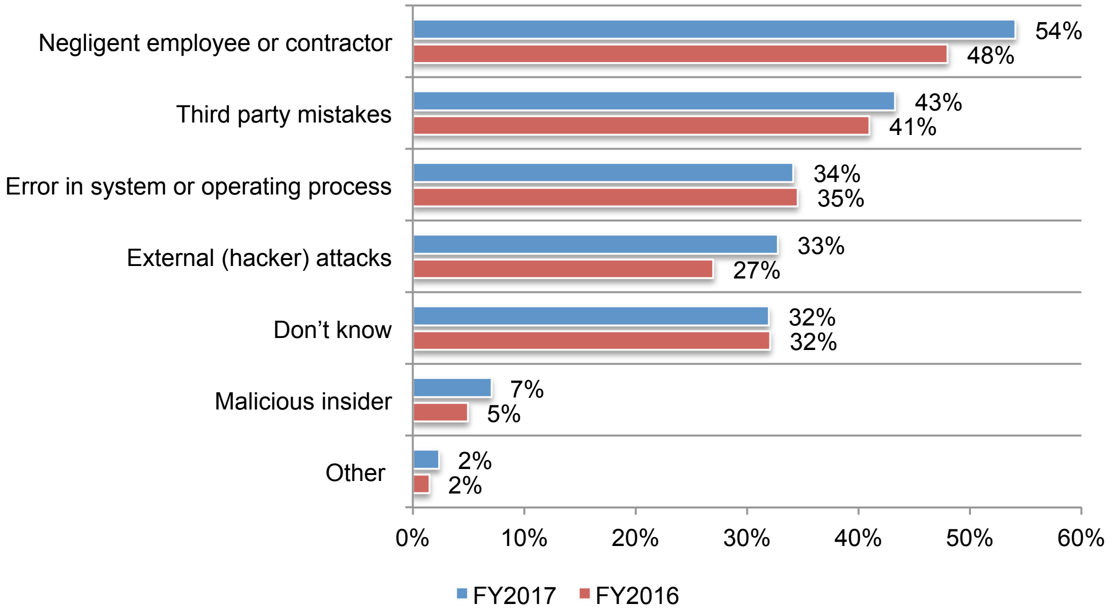
Figure 2. What types of attacks did your business experience?
More than one choice allowed



Businesses are losing more records in a data breach. Companies represented in this research lost an average of more than 9,350 individual records as a result of the data breach, a significant increase from an average of 5,079 in last year's study.

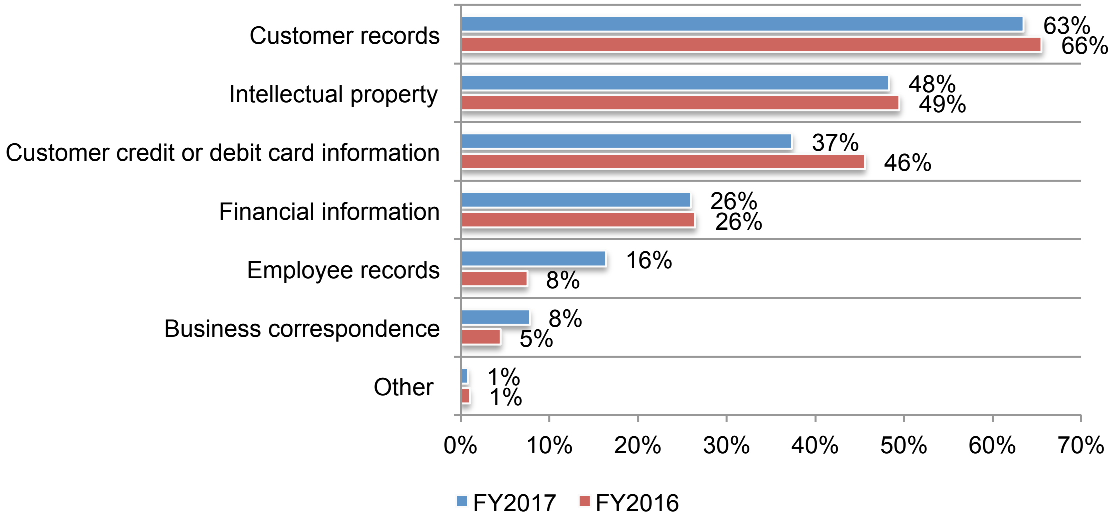
As shown in Figure 3, data breaches due to negligent employees or contractors (54 percent of respondents) increased significantly from 48 percent in 2016. This is followed by third party mistakes (43 percent of respondents) and errors in system or operating processes (34 percent of respondents). However, almost one-third of respondents say their companies could not determine what caused the incident.

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



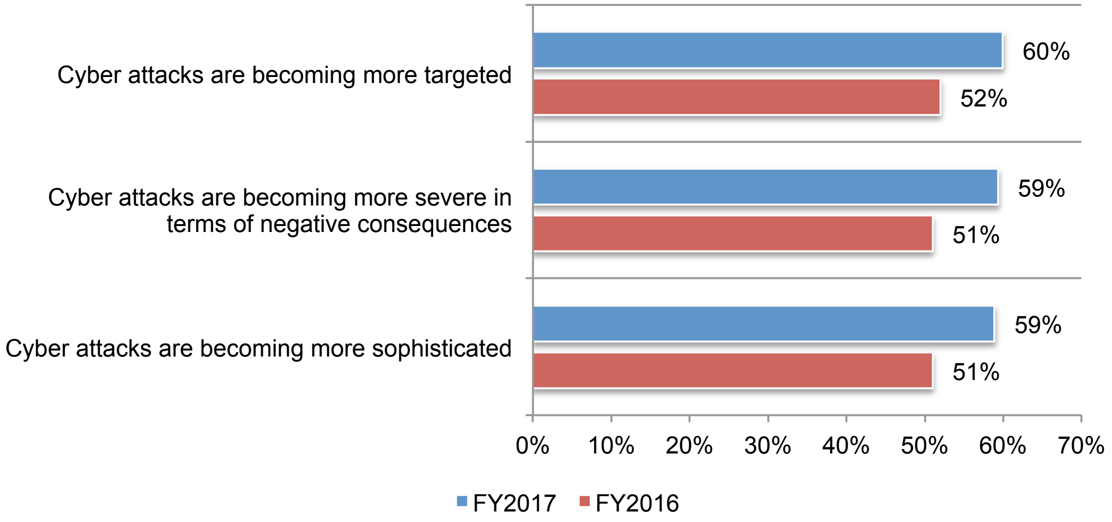
Businesses are most concerned about customer records and intellectual property. When asked what information cyber attackers are most likely to target, 63 percent of respondents say customer records are their biggest concern. Possibly because this is the information smaller companies most often use. Almost half of respondents (48 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



Since last year, SMB cyber attacks have become more targeted, sophisticated and severe. Figure 5 shows dramatic increases in respondents' perceptions about the threats posed by cyber attacks.

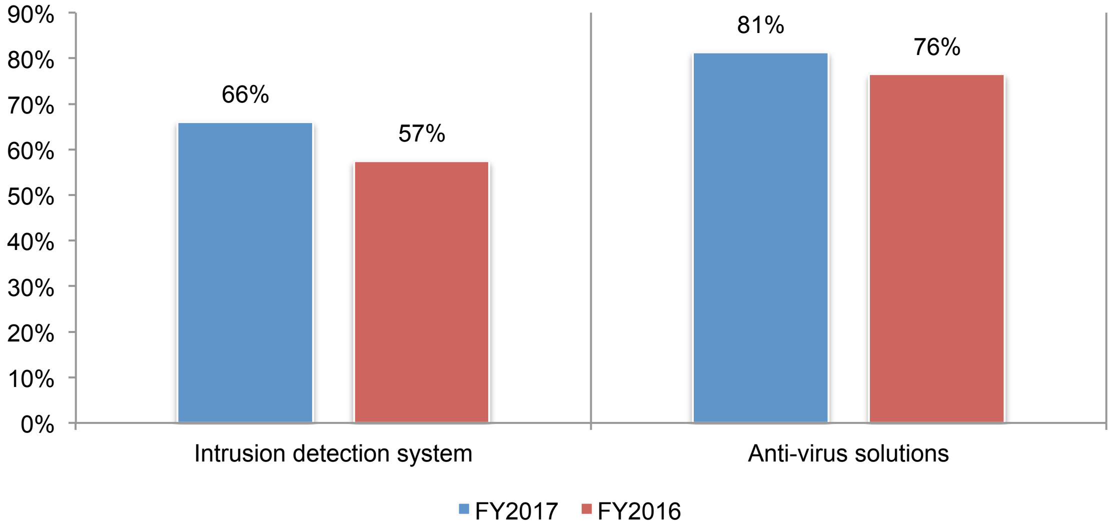
Figure 5. Perceptions about cyber attacks against their companies
Strongly Agree and Agree responses combined



Businesses are vulnerable to exploits and malware. Only 39 percent of respondents say the technologies currently used by their organization can detect and block most cyber attacks.

According to Figure 6, 66 percent of respondents (an increase from 57 percent) say exploits and malware evaded intrusion detection systems and 81 percent of respondents (an increase from 76 percent) 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



The rise of SMB ransomware attacks

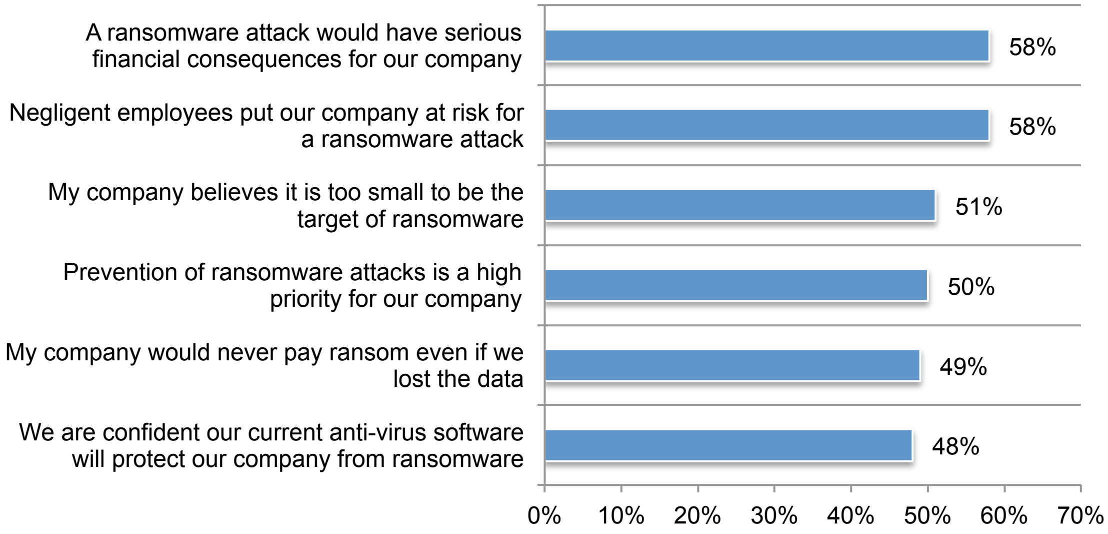
In the context of this research, ransomware is defined as a sophisticated piece of malware that blocks the victim's access to his/her files. While there are many strains of ransomware today, the two prominent types are:

Encrypting ransomware, which incorporates advanced encryption algorithms. It's designed to block system files and demand payment to provide the victim with the key that can decrypt the blocked content.

Locker ransomware locks the victim out of the operating system making it impossible to access the desktop and any apps or files. The files are not encrypted in this case, but the attackers still ask for a ransom to unlock the infected computer.

Companies are aware of the ransomware threat but believe they are too small to be a target. While 58 percent of respondents believe ransomware is a serious financial threat and are concerned that negligent employees put their company at risk, only half (50 percent) say prevention of such attacks is a priority, as shown in Figure 7. Many are not confident that their current anti-virus software will protect their company from ransomware.

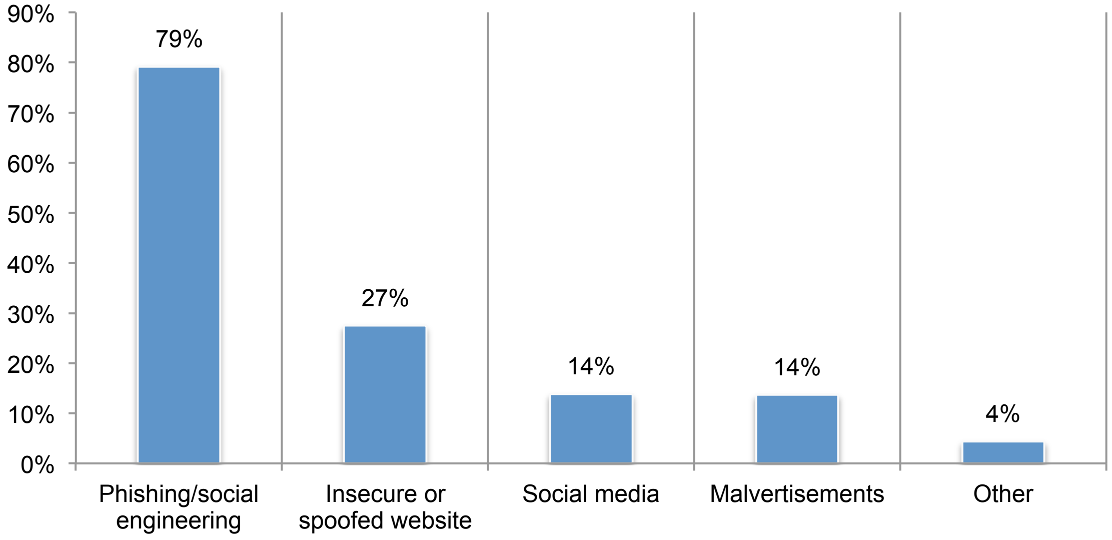
Figure 7. Perceptions about ransomware
Strongly agree and Agree responses combined



Fifty-one percent of respondents say they experienced either unsuccessful or successful ransomware attacks within the past three months (10 percent), within the past 6 months (14 percent), within the past 12 months (18 percent) or more than 12 months ago (9 percent). As defined above, 39 percent of these respondents say their organizations experienced encrypting ransomware, 30 percent experienced locker ransomware and 31 percent say their organizations experienced both.

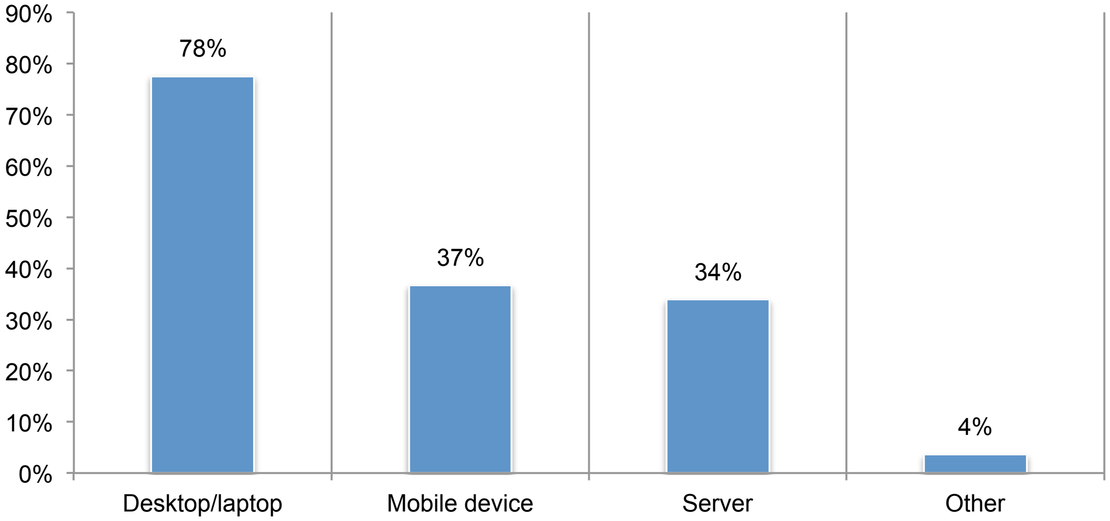
As shown in Figure 8, the ransomware experienced by companies in this study was mainly unleashed through phishing/social engineering attacks (79 percent of respondents) followed by an insecure or spoofed website. This finding coincides with both the increase in phishing/social engineering and the increase in negligent employees being the root cause of the data breach.

Figure 8. How was the ransomware unleashed?
More than one choice allowed



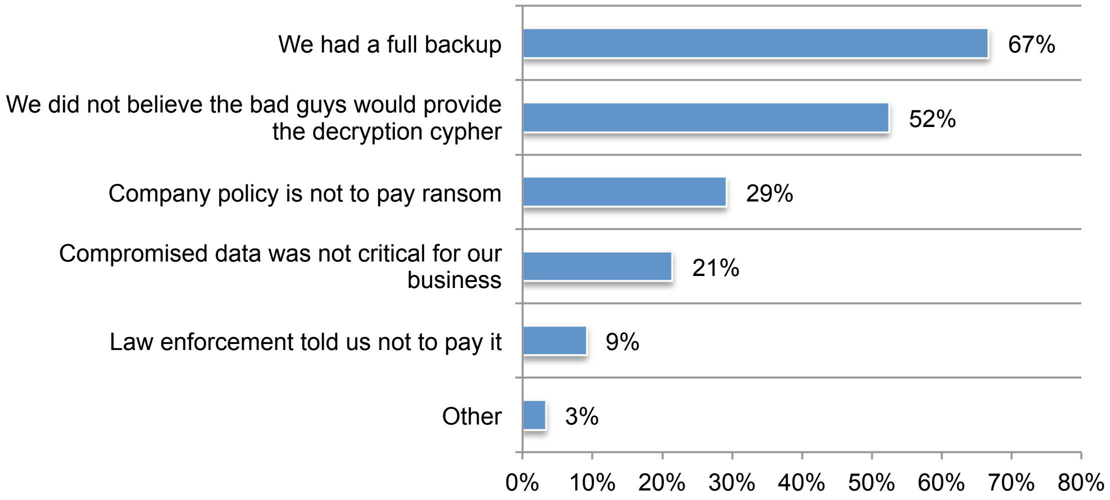
The device most often compromised by ransomware was a desktop/laptop (78 percent) and mobile device (37 percent), as shown in Figure 9.

Figure 9. What type of device(s) was compromised by ransomware?
More than one choice allowed



If successful, most companies paid the ransom. The average ransom was $2,157 and 60 percent of respondents say their companies paid the ransom. However, if they did not pay it was because they had a full backup (67 percent of respondents) or they did not trust the criminals to provide the decryption cypher (52 percent of respondents), as shown in Figure 10.

Figure 10. Why did your company not pay the ransom?
More than one choice allowed

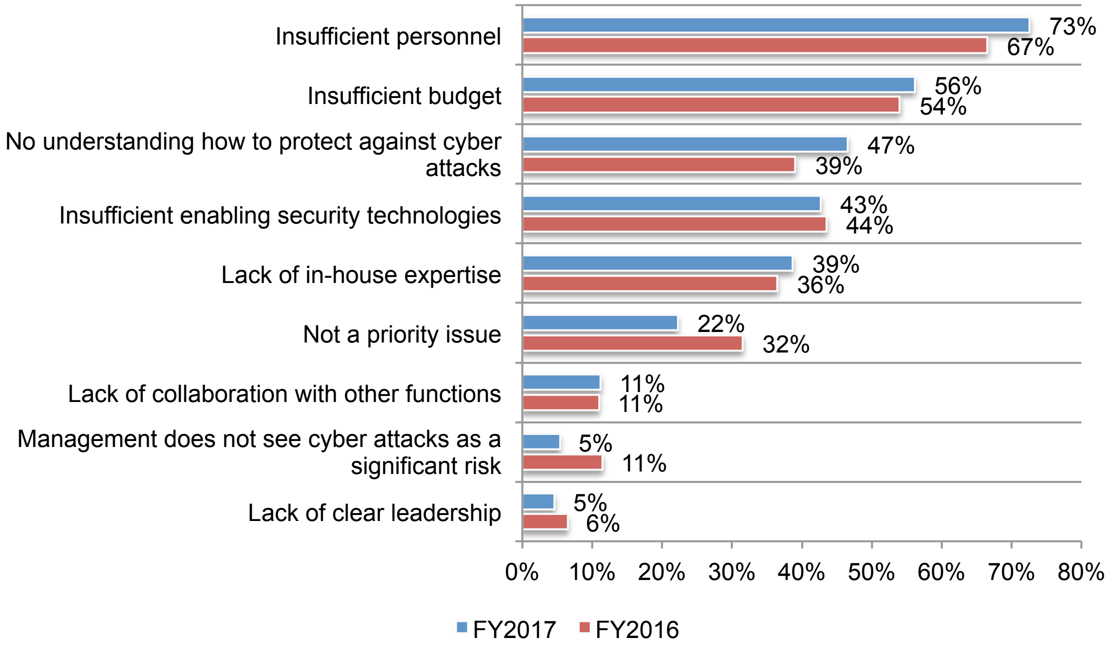


Cybersecurity posture and governance

A growing problem for SMBs is the inability to staff their IT functions. Figure 11 lists the challenges companies face when trying to create a stronger security posture.

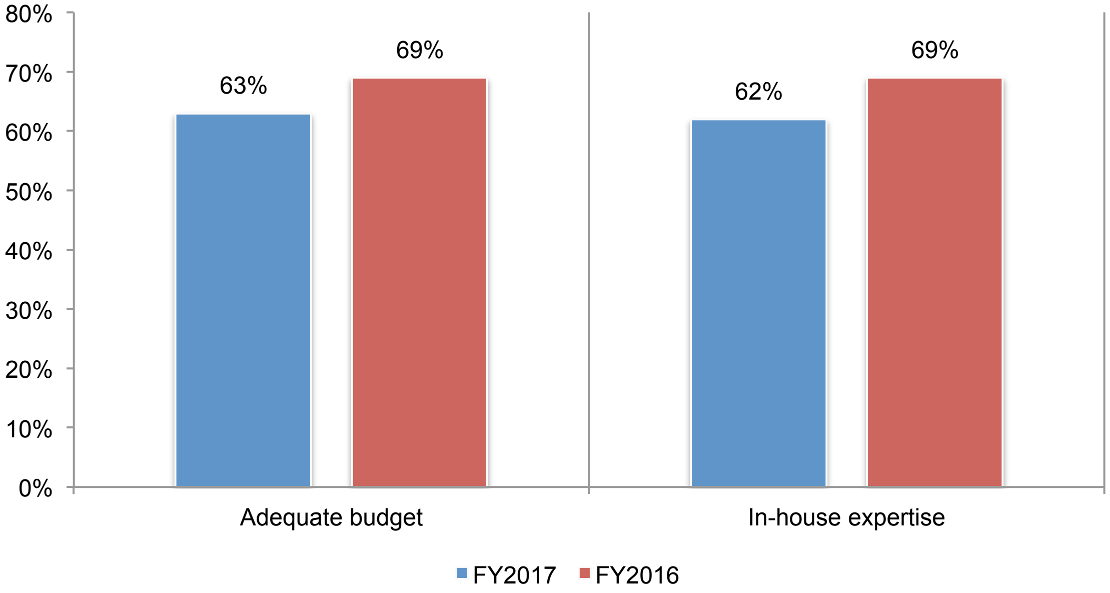
The biggest problem is not having the personnel to mitigate cyber risks, vulnerabilities and attacks, an increase from 67 percent of respondents to 73 percent. Insufficient budget (56 percent of respondents) and no understanding how to protect against cyber attacks, a significant increase from 39 percent to 47 percent of respondents. The challenge of not viewing cybersecurity as a priority decreased from 32 percent to 22 percent of respondents.

Figure 11. What challenges keep your IT security posture from being fully effective?
Three choices allowed



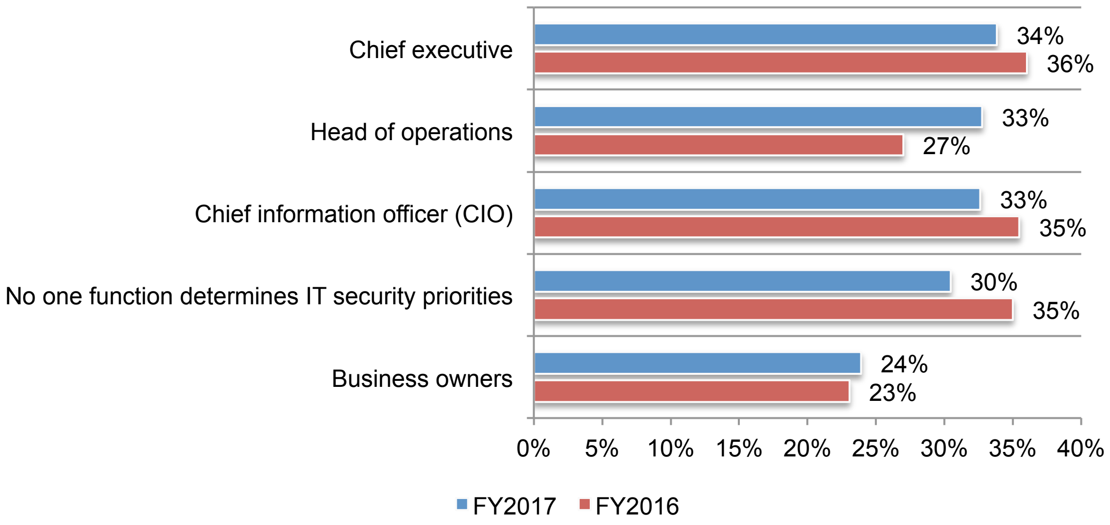
As shown in Figure 12, percent of respondents say their organizations do not have the budget (52 percent or are unsure (11 percent). Another 62 percent of respondents say they do not have the in-house expertise (52 percent) or are unsure (10 percent) adequate to achieve a strong cybersecurity posture.

Figure 12. Does your organization have an adequate budget and in-house expertise to achieve a strong cybersecurity posture?
No and Unsure responses combined



There is a significant shift in who determines IT security priorities. As shown in Figure 13, head of operations as the person determining IT security priorities, a significant increase from 27 percent to 33 percent of respondents. There also was a decrease in not having one function accountable for IT security priorities.

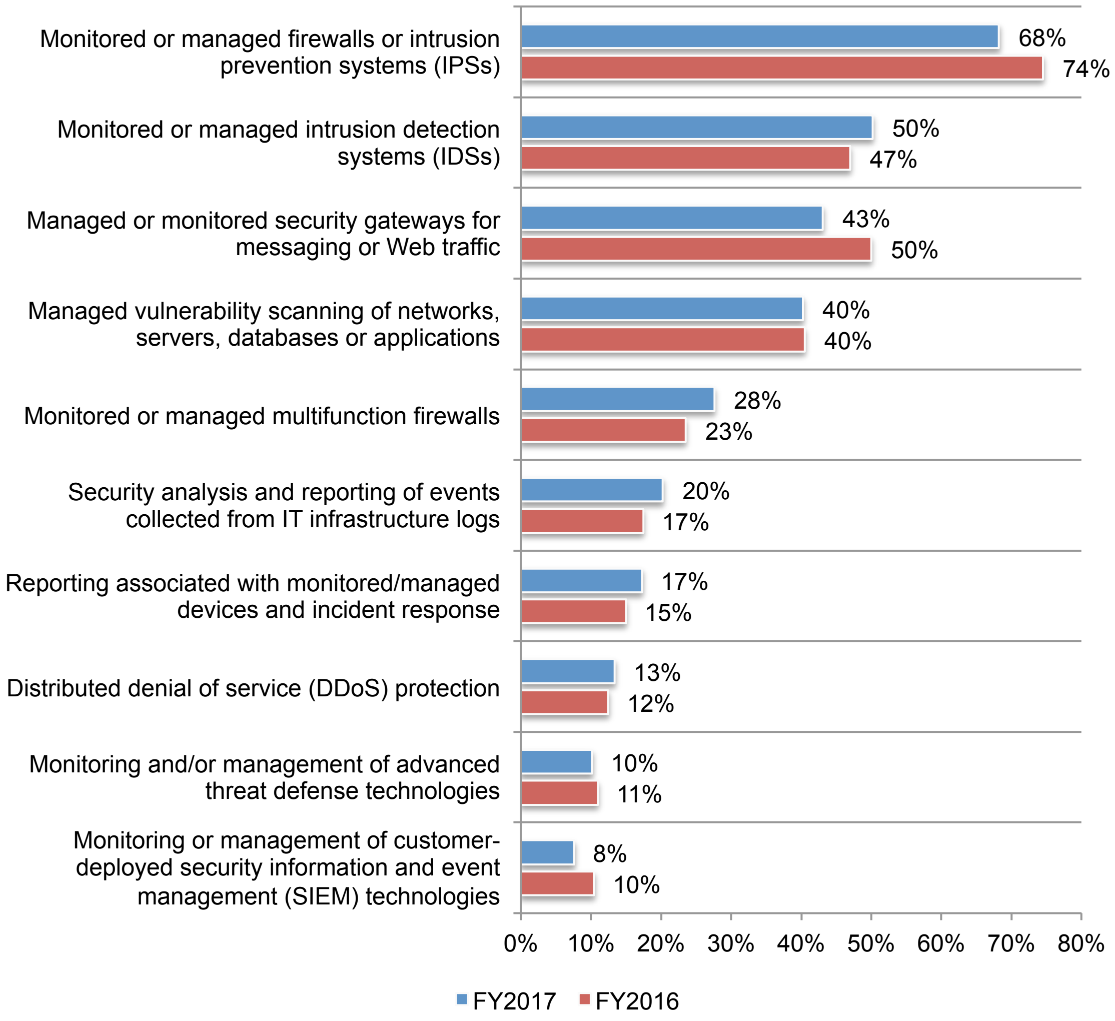
Figure 13. Who determines IT security priorities?
Two choices allowed



Managed security services providers (MSSPs) are engaged to support the IT security function. On average, 21 percent of a company's IT security operations are supported by MSSPs.

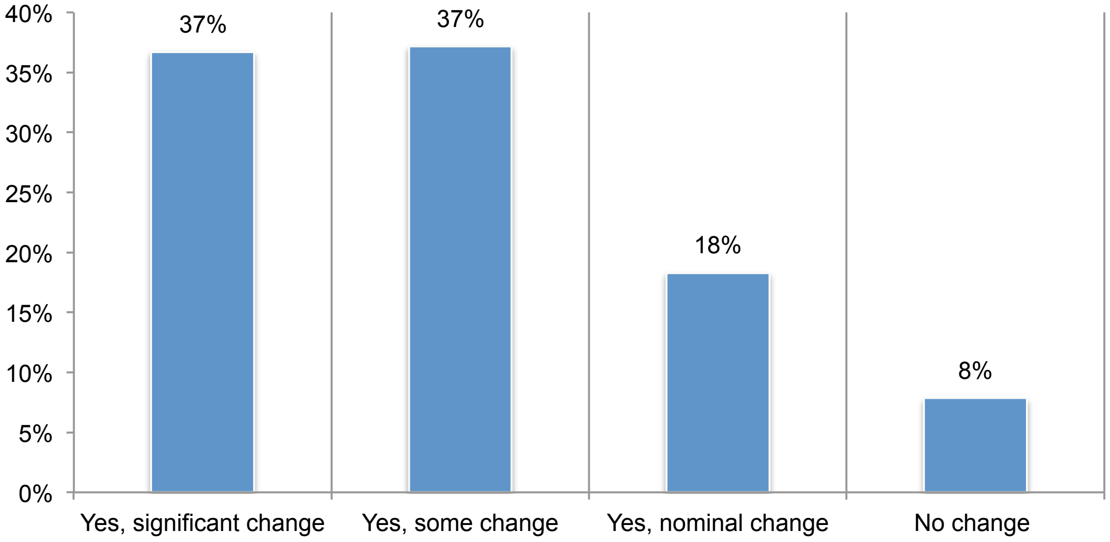
According to Figure 14, 68 percent of respondents say their MSSP monitors or manages firewalls or intrusion prevention systems (IPS). Fifty percent say they use MSSPs to monitor or manage intrusion detection systems (IDSs). Fewer companies are outsourcing the management or monitoring security gateways for messaging or web traffic (a decrease from 50 percent to 43 percent).

Figure 14. What services are provided by MSSPs to support your IT security posture?
More than one choice allowed



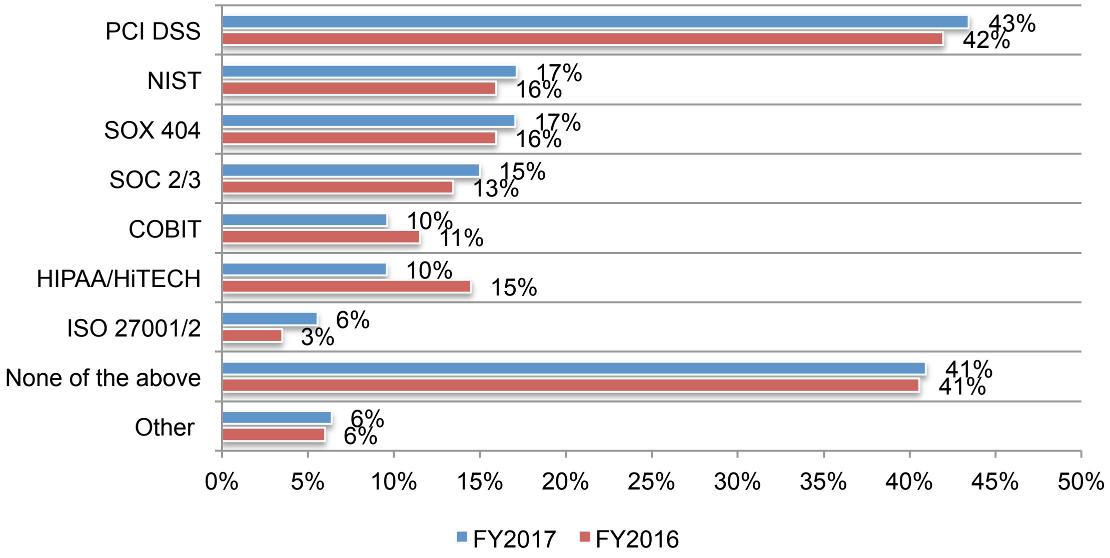
The new General Data Protection Regulation (GDPR) is a concern for SMBs. The GDPR will go in effect May 25, 2018 and establishes new requirements related to the export of personal data outside the European Union. As shown in Figure 15, 74 percent of respondents believe the new regulations will require changes to their security strategy. Only 20 percent of respondents say their organizations are prepared to comply with GDPR.

Figure 15. Will the GDPR require significant changes in your security strategy?



Companies mostly comply with PCI DSS. Figure 16 presents the leading IT security guidelines and standards. Forty-three percent of respondents say they comply with PCI DSS, but 41 percent say they do not comply with any of the standards.

Figure 16. Which IT security guidelines or standards does your company comply with?
More than one choice allowed

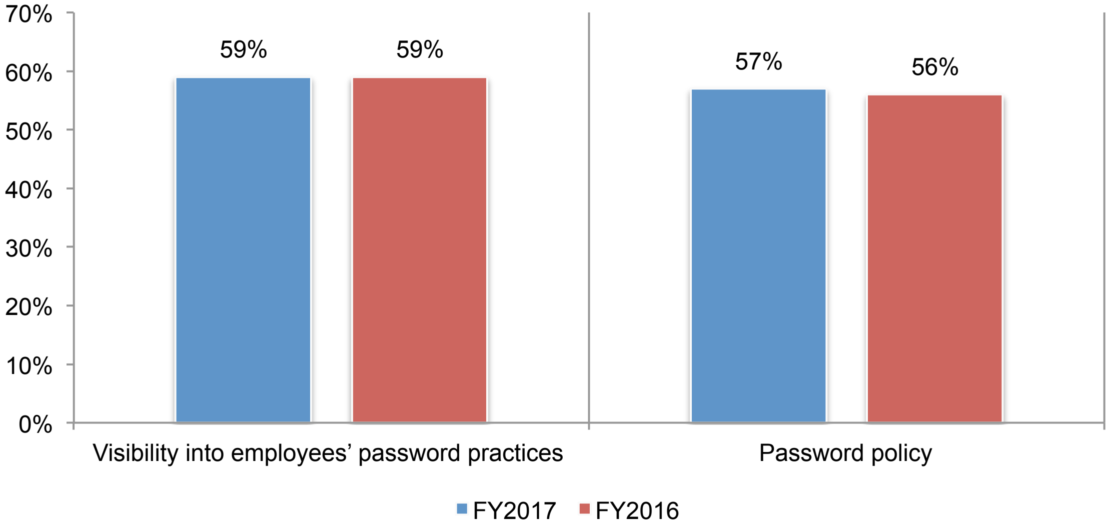


Technologies in place to address the threat

Strong passwords and biometrics are an essential part of the security defense. Similar to last year 60 percent of respondents say they rely upon strong passwords and/or biometrics to reduce the risk of attack.

However, as shown in Figure 15, 59 percent of respondents say they do not have or are unsure they have visibility into employees' password practices such as the use of unique or strong passwords and sharing passwords with others. Fifty-seven 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.

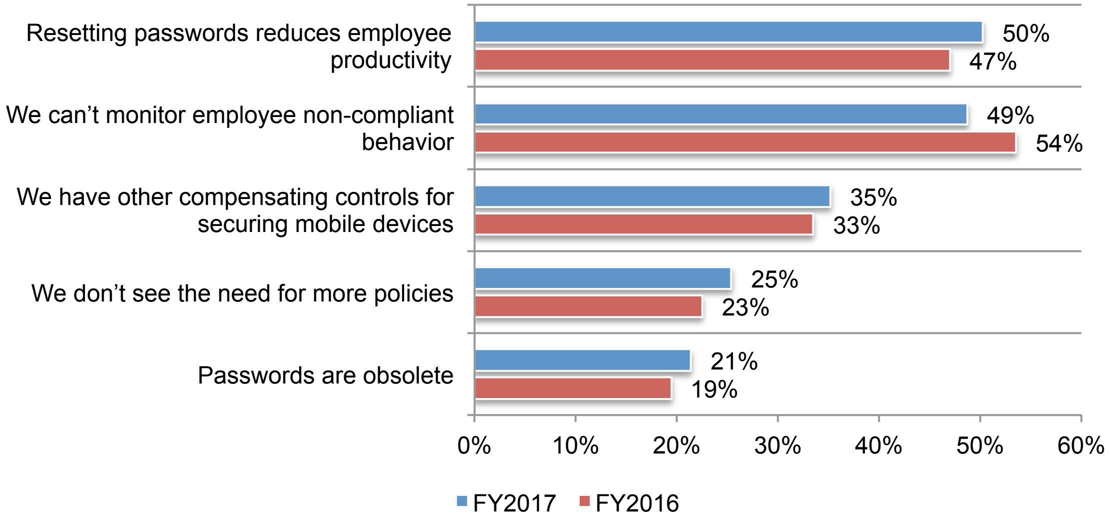
Figure 17. Does your organization have visibility into employees' password practices and a password policy?
No and Unsure responses combined



Password policies are not strictly enforced. Forty-three percent of respondents say their company has a policy pertaining to employees' use of passwords and/or biometrics (such as a fingerprint). If their company has a password policy, only 32 percent of respondents say they strictly enforce it. Almost half of these respondents (49 percent) say the policy does not require employees to use a password or biometric to secure access to mobile devices.

As shown in Figure 18, if companies do not require passwords or biometric protections on mobile devices, the primary reasons are the loss of productivity when employees are required to reset passwords (50 percent). However, it appears that companies are improving their ability to monitor employees' non-compliant behavior, a decrease from 54 percent to 49 percent.

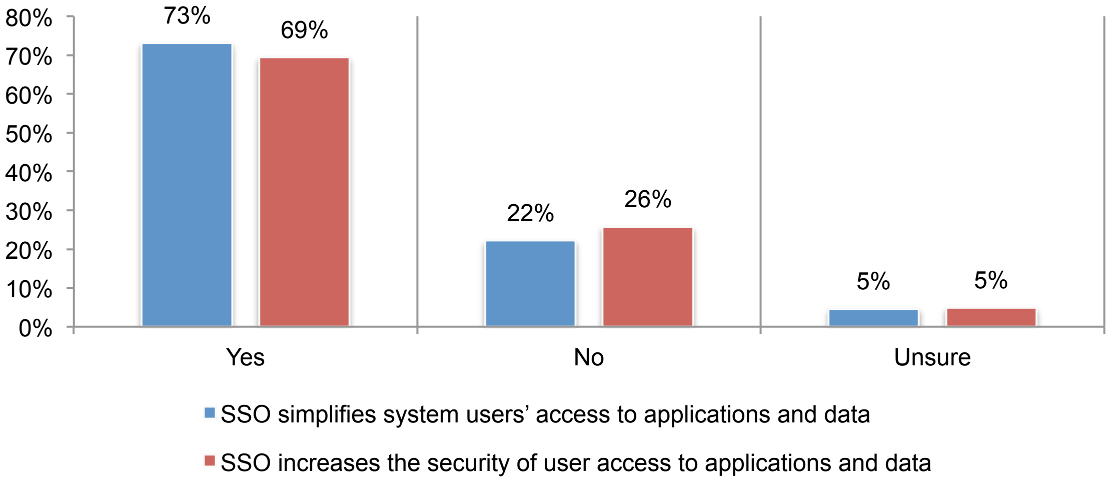
Figure 18. Why doesn't your organization require password or biometric protections on mobile devices?
More than one choice allowed



In this research, Single Sign-On (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.

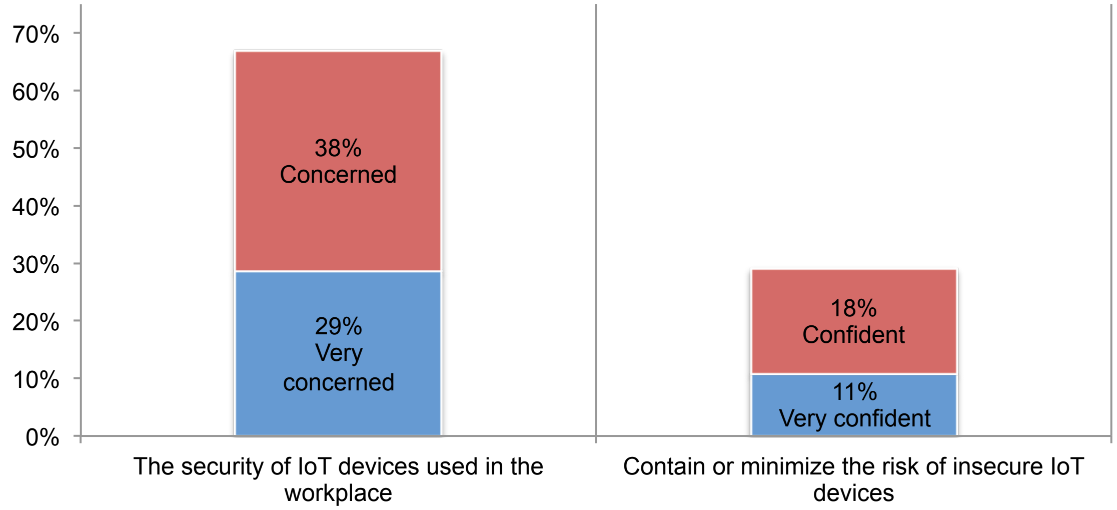
Respondents believe SSOs are effective. Fifty-one percent of respondents have fully implemented SSO across their enterprises (27 percent) or partially implemented across the enterprise (24 percent). These respondents believe SSO simplifies system users' access to applications and data in their organizations (73 percent) and increase the security of user access to their companies' applications and data (69 percent).

Figure 19. Does SSO simplify and increase the security of user access to your organization's applications and data?



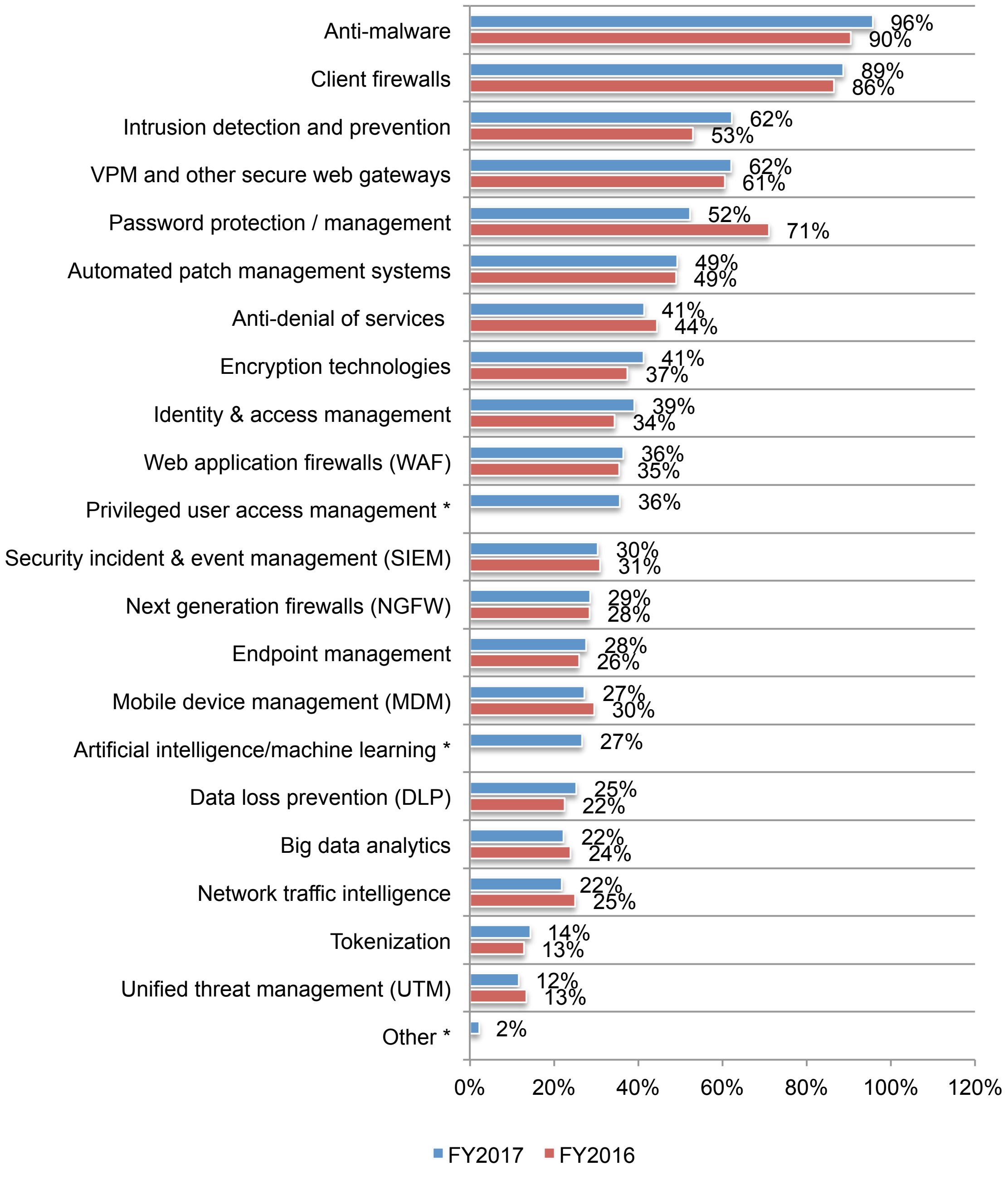
Confidence is low in companies' ability to minimize the risk of IoT devices. While only 23 percent of respondents say they experienced a data breach due to the use of IoT devices in the workplace, as shown in Figure 20 there is concern about their security (67 percent of respondents). There is also very low confidence (29 percent of respondents) in their ability to contain or minimize the risk of insecure IoT devices.

Figure 20. How concerned is your company about the security of IoT devices and how confident is your organization that it can contain or minimize the risk of insecure IoT devices?



Anti-malware and client firewalls continue to be the most important security technologies. According to Figure 21, 96 percent of respondents believe anti-malware is critical. Almost as many say the same of client firewalls (89 percent of respondents). Intrusion detection and prevention increased from 53 percent to 62 percent of respondents. Fifty-two percent of respondents say password protection and management are important (a significant decline from 71 percent last year).

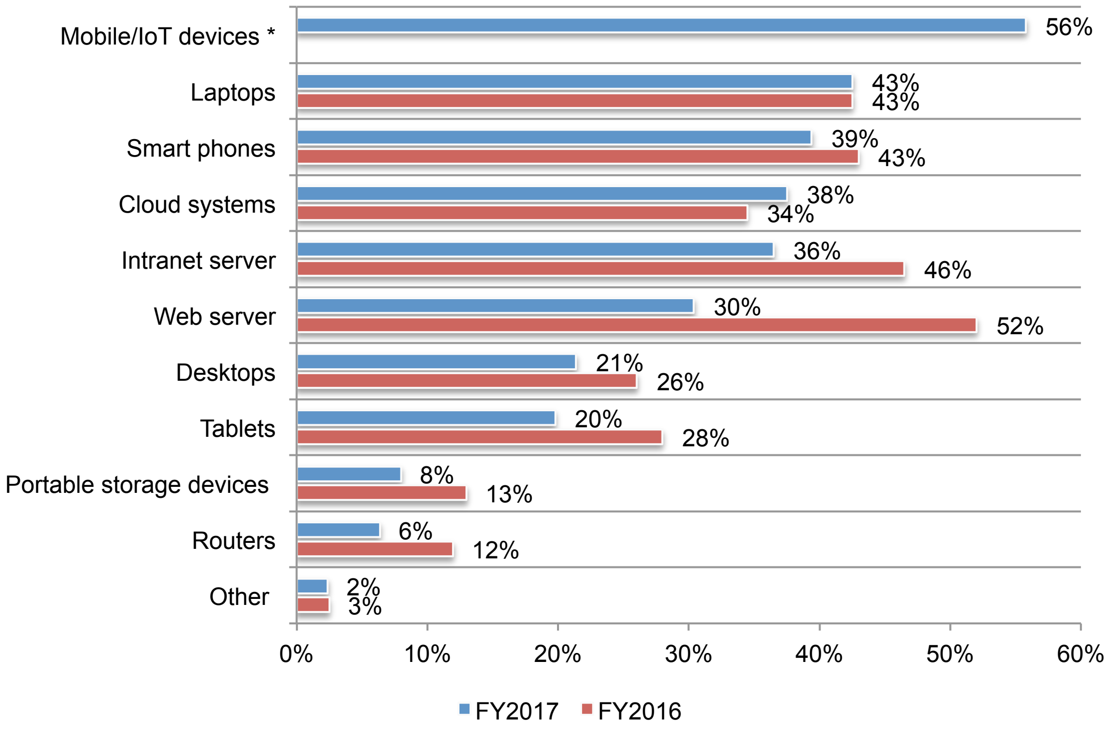
Figure 21. Security technologies considered essential and very important
More than one choice allowed



* Not a choice in FY2016

Mobile/IoT devices are the most vulnerable endpoints or entry points to networks and enterprise systems. For the first time, mobile/IoT devices was included in the research and is by far considered the most vulnerable endpoint or entry point to their companies' networks and enterprise systems. Web servers decreased from 52 percent to 30 percent of respondents.

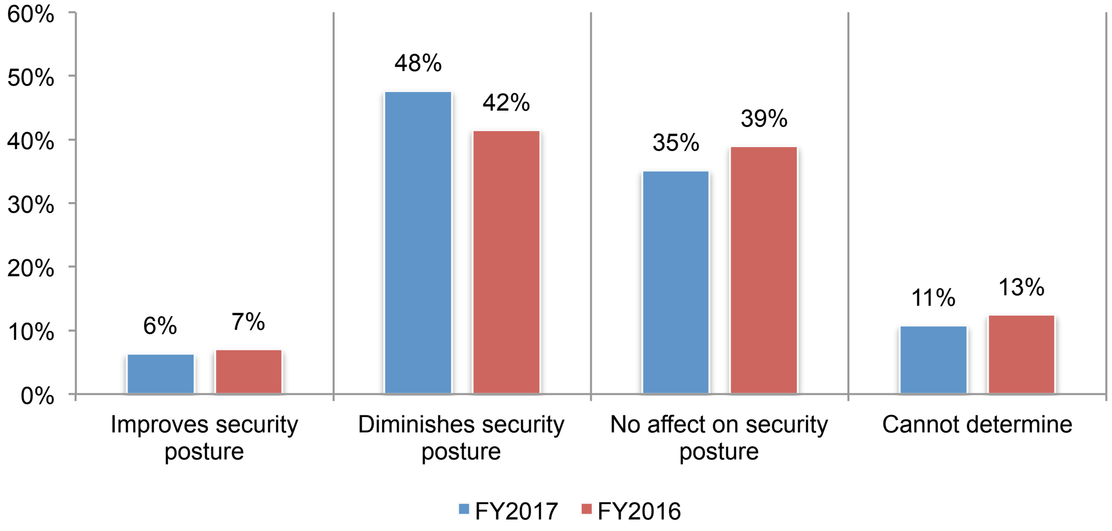
Figure 22. What are the most vulnerable endpoints or entry points to your organization's networks and enterprise systems?
Three choices allowed



* Not a choice in FY2016

More mobile devices will be used to access business-critical applications and IT infrastructure. Currently, on average, 49 percent of business critical applications are accessed from mobile devices such as smartphones and tablets. As shown in Figure 19, 48 percent of respondents say they diminish security posture, a significant increase from last year's research.

Figure 23. How does the use of mobile devices to access business-critical applications and IT infrastructure affect your organization's security posture?



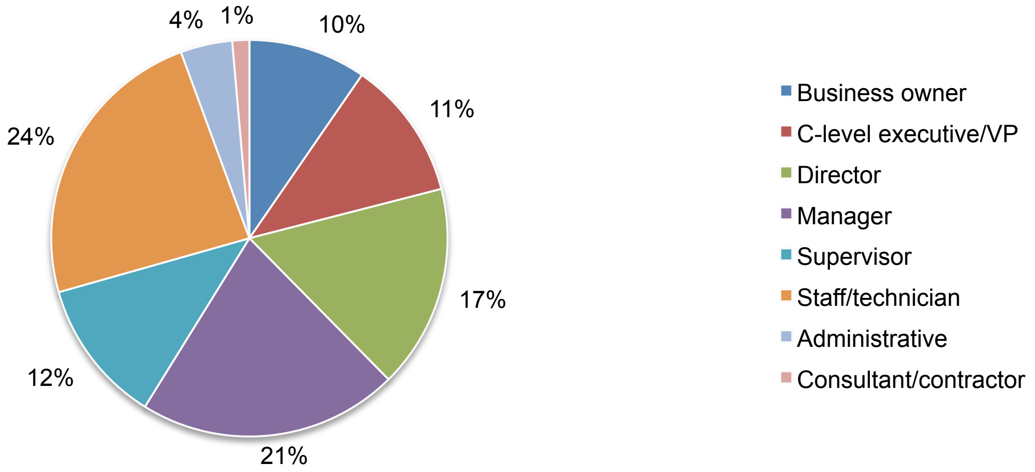
Part 3. Methods

A sampling frame of 29,988 IT and IT security practitioners in companies in the United States and United Kingdom with a headcount from less than 100 to 1,000 were selected as participants in the research. Table 1 shows 1,152 total returns. Screening and reliability checks required the removal of 112 surveys. Our final sample consisted of 1,040 surveys or a 3.5 percent response.

Table 1. Sample response	Freq	Pct%
Sampling frame	29,988	100.0%
Total returns	1,152	3.8%
Rejected or screened surveys	112	0.4%
Final sample	1,040	3.5%

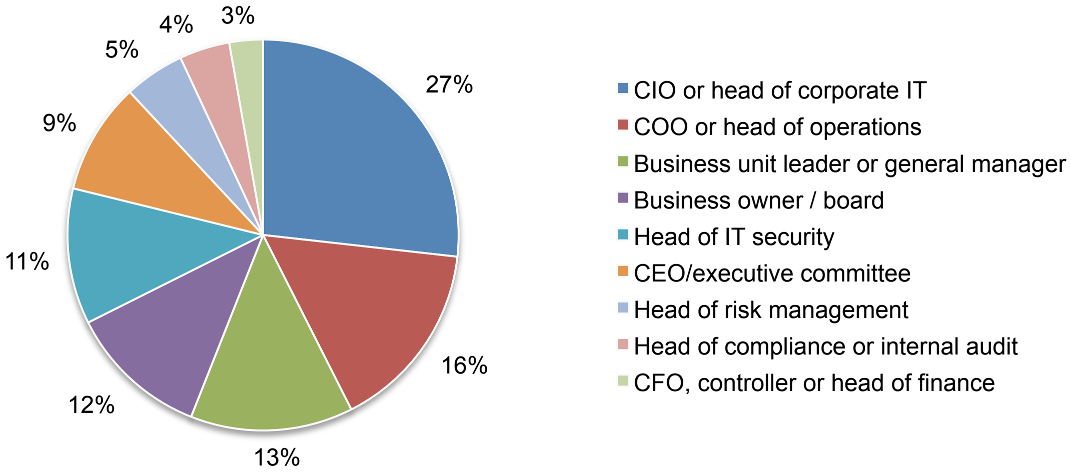
Pie Chart 1 reports the respondents' organizational level within participating organizations. By design, 71 percent of respondents are at or above the supervisory levels.

Pie Chart 1. Position level within the organization



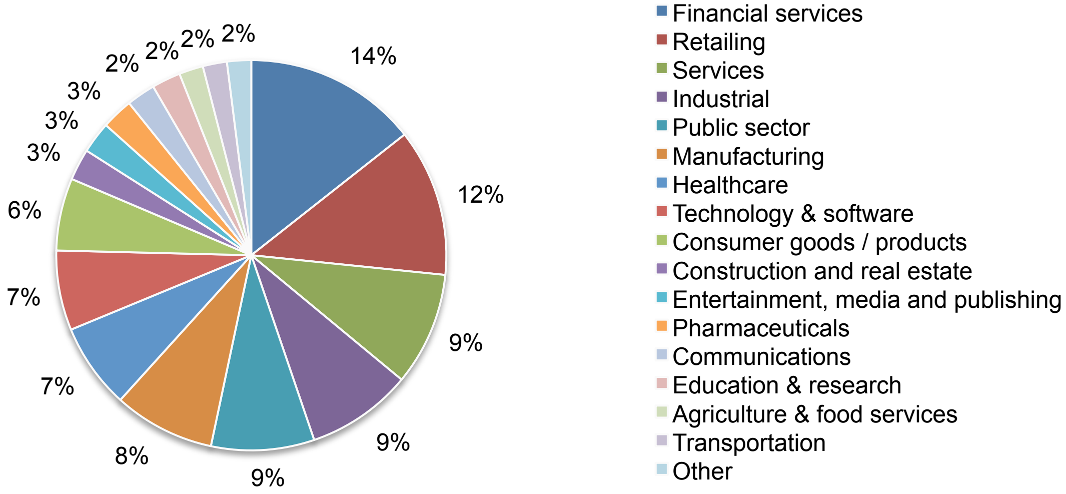
As shown in Pie Chart 2, 27 percent of respondents report directly to the CIO or head of corporate IT, 16 percent report to the COO or head of operations and 13 percent report to the business unit leader or general manager.

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



Pie Chart 3 reports the industry focus of respondents' organizations. This chart identifies financial services (14 percent) as the largest segment, followed by retailing (12 percent), services, industrial and public sector, all three industries are at 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 in June 2017.

Survey response	**FY2017**	**FY2016**
Total sampling frame	29,988.00	16,401
Total returns	1,152.00	665
Rejected surveys	112.00	67
Final sample	1,040.00	598
Response rate	3.5%	3.6%

Part 1. Screening Questions

S1. What range best describes the full-time employee headcount of your organization?	**FY2017**	**FY2016**
Less than 100	168	81
100 to 250	172	104
251 to 500	209	116
501 to 750	252	157
751 to 1,000	239	140
More than 1,000 [STOP]	-	-
Total	1,040	598

S2. What best describes your role in managing the IT security function or activities within your organization? Check all that apply.	**FY2017**	**FY2016**
Setting IT security priorities	62%	61%
Managing IT security budgets	57%	56%
Selecting vendors and contractors	49%	49%
Determining IT security strategy	46%	50%
Evaluating program performance	44%	50%
None of the above [STOP]	0%	0%
Total	257%	265%

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?	**FY2017**	**FY2016**
Very high level of involvement	34%	33%
High level of involvement	43%	43%
Moderate level of involvement	19%	22%
Low level of involvement	5%	2%
Not involved [STOP]	0%	0%
Total	100%	100%

Part 2: Your Organization's 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	FY2017	FY2016
1 or 2	11%	16%
3 or 4	38%	46%
5 or 6	30%	24%
7 or 8	14%	10%
9 or 10	7%	4%
Total	100%	100%
Extrapolated value	4.87	4.25

Q2. What challenges keep your organization's IT security posture from being fully effective? Top three choices.	FY2017	FY2016
Insufficient budget (money)	56%	54%
Insufficient personnel	73%	67%
Lack of in-house expertise	39%	36%
Lack of clear leadership	5%	6%
Insufficient enabling security technologies	43%	44%
No understanding how to protect against cyber attacks	47%	39%
Management does not see cyber attacks as a significant risk	5%	11%
Lack of collaboration with other functions	11%	11%
Not a priority issue	22%	32%
Total	300%	300%

Q3. What types of information are you most concerned about protecting from cyber attackers? Top two choices.	FY2017	FY2016
Customer credit or debit card information	37%	46%
Financial information	26%	26%
Intellectual property	48%	49%
Customer records	63%	66%
Employee records	16%	8%
Business correspondence	8%	5%
Other (please specify)	1%	1%
Total	200%	200%

Q4. Who determines IT security priorities in your organization? Top two choices.	FY2017	FY2016
Business owners	24%	23%
Board of directors	9%	11%
Chief executive	34%	36%
Head of operations	33%	27%
Chief information officer (CIO)	33%	35%
Chief technology officer (CTO)	8%	7%
Chief information security officer (CISO)	11%	7%
Compliance officer	6%	3%
General counsel	4%	5%
Lines of business	9%	8%
No one function determines IT security priorities	30%	35%
Other (please specify)	0%	1%
Total	200%	200%

Q5. Is your organization's budget adequate for achieving a strong IT security posture?	FY2017	FY2016
Yes	37%	31%
No	52%	54%
Unsure	11%	15%
Total	100%	100%

Q6. What percentage of your organization's IT budget is dedicated to IT security activities?	FY2017	FY2016*
Less than 5%	19%	22%
5 to 10%	27%	31%
11 to 15%	25%	30%
16 to 20%	19%	12%
21 to 25%	6%	4%
26 to 30%	3%	1%
31 to 40%	1%	0%
41 to 50%	0%	0%
More than 50%	0%	0%
Total	100%	100%
Extrapolated value	11.6%	10.6%

Q7. Does your organization have the in-house expertise necessary for achieving a strong IT security posture?	FY2017	FY2016
Yes	38%	31%
No	52%	56%
Unsure	10%	13%
Total	100%	100%

Q8. What percentage of your organization's IT personnel support IT security operations? *Scale was different in FY2016	FY2017	FY2016
Less than 5%	0%	
5 to 10%	5%	4%
11 to 15%	8%	
16 to 20%	12%	
21 to 25%	15%	19%
26 to 30%	11%	
31 to 40%	8%	22%
41 to 50%	8%	
More than 50%	33%	54%
Total	100%	100%
Extrapolated value	0.36	54%

Q9a. What percentage of your organization's IT security operations are supported by managed security services providers (MSSPs)?	FY2017	FY2016
None [Skip Q10]	47%	54%
Less than 10%	10%	11%
10% to 25%	12%	13%
26% to 50%	11%	9%
51% to 75%	9%	9%
76% to 100%	10%	4%
Total	100%	100%
Extrapolated value	21%	16%

Q9b. Following are core services typically provided by MSSPs. Please check all services provided by MSSPs to support your organization's IT security posture.	FY2017	FY2016
Monitored or managed firewalls or intrusion prevention systems (IPSs)	68%	74%
Monitored or managed intrusion detection systems (IDSs)	50%	47%
Monitored or managed multifunction firewalls	28%	23%
Managed or monitored security gateways for messaging or Web traffic	43%	50%
Security analysis and reporting of events collected from IT infrastructure logs	20%	17%
Reporting associated with monitored/managed devices and incident response	17%	15%
Managed vulnerability scanning of networks, servers, databases or applications	40%	40%
Distributed denial of service (DDoS) protection	13%	12%
Monitoring or management of customer-deployed security information and event management (SIEM) technologies	8%	10%
Monitoring and/or management of advanced threat defense technologies	10%	11%
Total	298%	302%

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.	FY2017	FY2016
PCI DSS	43%	42%
ISO 27001/2	6%	3%
SOC 2/3	15%	13%
COBIT	10%	11%
SOX 404	17%	16%
NIST	17%	16%
HIPAA/HiTECH	10%	15%
None of the above	41%	41%
Other (please specify)	6%	6%
Total	165%	163%

Part 3: Cyber Attacks

Q11a. Has your organization experienced a cyber attack in the past 12 months?	FY2017	FY2016
Yes	61%	55%
No	24%	29%
Unsure	14%	16%
Total	100%	100%

Q11b. If yes, what best describes the type of attacks experienced by your organization? Please select all that apply.	FY2017	FY2016
Advanced malware / zero day attacks	16%	14%
Phishing / social engineering	48%	43%
SQL injection	24%	26%
Cross-site scripting	10%	11%
Denial of services	26%	21%
Compromised / stolen devices	30%	25%
Malicious insider	11%	13%
General malware	36%	35%
Web-based attack	43%	49%
Other (please specify)	3%	1%
Ransomware		2%
Total	248%	241%

Q12a. My company believes it is too small to be the target of ransomware.	FY2017
Strongly agree	20%
Agree	31%
Unsure	15%
Disagree	23%
Strongly disagree	11%
Total	100%

Q12b. My company would never pay ransom even if we lost the data.	FY2017
Strongly agree	22%
Agree	27%
Unsure	26%
Disagree	17%
Strongly disagree	8%
Total	100%

Q12c. Negligent employees put our company at risk for a ransomware attack.	FY2017
Strongly agree	24%
Agree	34%
Unsure	15%
Disagree	18%
Strongly disagree	8%
Total	100%

Q12d. A ransomware attack would have serious financial consequences for our company.	FY2017
Strongly agree	23%
Agree	35%
Unsure	21%
Disagree	16%
Strongly disagree	6%
Total	100%

Q12e. Prevention of ransomware attacks is a high priority for our company.	FY2017
Strongly agree	20%
Agree	30%
Unsure	17%
Disagree	25%
Strongly disagree	9%
Total	100%

Q12f. We are confident our current anti-virus software will protect our company from ransomware.	FY2017
Strongly agree	22%
Agree	26%
Unsure	19%
Disagree	24%
Strongly disagree	9%
Total	100%

Q13. Have you or your company experienced ransomware? (This includes both unsuccessful and successful ransomware attacks)	FY2017
Yes, within the past 3 months	10%
Yes, within the past 6 months	14%
Yes, within the past 12 months	18%
Yes, more than 12 months ago	9%
No (Go to Q20a)	48%
Total	100%

Q14. How many ransomware incidents have you or your company experienced?	FY2017
1	47%
2 to 5	31%
6 to 10	17%
Greater than 10	5%
Total	100%

Q15. What type of ransomware did you experience?	FY2017
Encrypting ransomware, which incorporates advanced encryption algorithms. It's designed to block system files and demand payment to provide the victim with the key that can decrypt the blocked content. Examples include CryptoLocker, CrytpoWall and more.	39%
Locker ransomware, which locks the victim out of the operating system making it impossible to access the desktop and any apps or files. The files are not encrypted in this case, but the attackers still ask for a ransom to unlock the infected computer. An example includes Winlocker.	30%
Both encrypting and locker ransomware was experienced	31%
Total	100%

Q16. How was the ransomware unleashed? Please select all that apply.	FY2017
Phishing/social engineering	79%
Insecure or spoofed website	27%
Social media	14%
Malvertisements	14%
Other	4%
Total	139%

Q17. What type of device(s) was compromised by ransomware? Please select all that apply.	FY2017
Desktop/laptop	78%
Mobile device	37%
Server	34%
Other	4%
Total	152%

Q18. If the attack was successful, how much was the ransom? If you experienced two or more ransomware attacks, please select one choice that represented the highest ransom amount.	FY2017
Less than $100	13%
$100 to $500	30%
$501 to $1,000	30%
$1,001 to $5,000	13%
$5,001 to $10,000	7%
More than $10,000	8%
Total	100%
Extrapolated value	$2,157

**UK amount was converted from GBP to dollars*

Q19a. If the attack was successful, did your company pay the ransom?	FY2017
Yes	60%
No	40%
Total	100%

Q19b. If you did not pay a ransom, why not? Please select all that apply.	FY2017
We had a full backup	67%
Company policy is not to pay ransom	29%
Law enforcement told us not to pay it	9%
We did not believe the bad guys would provide the decryption cypher	52%
Compromised data was not critical for our business	21%
Other	3%
Total	182%

Q20a. 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?	FY2017	FY2016
Yes	54%	50%
No [skip to Q21]	46%	38%
Unsure		12%
Total	100%	100%

Q20b. If yes, with respect to your organization’s largest breach over the past 12 months, how many individual records were lost or stolen?	FY2017	FY2016
Less than 100	33%	35%
100 to 500	26%	29%
501 to 1,000	15%	19%
1,001 to 10,000	14%	8%
10,001 to 50,000	7%	5%
50,001 to 100,000	4%	4%
100,001 to 1,000,000	1%	0%
More than 1,000,000	0%	0%
Total	100%	100%
Extrapolated value	9,350	5,079

Q20c. If yes, what were the root causes of the data breaches experienced by your organization? Please select that apply.	FY2017	FY2016
Malicious insider	7%	5%
External (hacker) attacks	33%	27%
Negligent employee or contractor	54%	48%
Error in system or operating process	34%	35%
Third party mistakes	43%	41%
Other (please specify)	2%	2%
Don’t know	32%	32%
Total	206%	189%

Q21. Does your organization have an incident response plan for responding to cyber attacks and data breaches?	FY2017	FY2016
Yes	55%	48%
No	44%	48%
Unsure	1%	3%
Total	100%	100%

Q22a. Has your organization ever experienced situations when exploits and malware have evaded your intrusion detection system?	FY2017	FY2016
Yes	66%	57%
No	22%	21%
Unsure	12%	
Don't have IDS		22%
Total	100%	100%

Q22b. Has your organization ever experienced situations when exploits and malware have evaded your anti-virus solutions?	FY2017	FY2016
Yes	81%	76%
No	13%	21%
Unsure	5%	
Don't have anti-virus		3%
Total	100%	100%

Please rate the following statements using the five-point scale provided below each item. % Strongly Agree and Agree responses combined

Q23a. Cyber attacks experienced by my organization are becoming more **targeted**.	FY2017	FY2016
Strongly agree	27%	25%
Agree	33%	27%
Unsure	19%	29%
Disagree	13%	12%
Strongly disagree	9%	7%
Total	100%	100%

Q23b. Cyber attacks experienced by my organization are becoming more **sophisticated**.	FY2017	FY2016
Strongly agree	26%	23%
Agree	33%	28%
Unsure	21%	28%
Disagree	12%	13%
Strongly disagree	8%	8%
Total	100%	100%

Q23c. Cyber attacks experienced by my organization are becoming more **severe** in terms of negative consequences (such as financial impact).	FY2017	FY2016
Strongly agree	27%	21%
Agree	32%	30%
Unsure	24%	27%
Disagree	12%	17%
Strongly disagree	5%	5%
Total	100%	100%

Q23d. The use of strong passwords and/or biometrics is an essential part of my organization's security defense.	FY2017	FY2016
Strongly agree	28%	30%
Agree	32%	30%
Unsure	19%	21%
Disagree	13%	12%
Strongly disagree	7%	7%
Total	100%	100%

Part 4. Disruptive Technology Trends

Q24. 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.	FY2017	FY2016
Zero	3%	4%
Less than 10%	4%	5%
11 to 25%	10%	15%
26 to 50%	42%	38%
51 to 75%	21%	25%
76 to 100%	20%	13%
Total	100%	100%
Extrapolated value	49%	44%

Q25. Does your organization have **visibility in**to employees' password practices (e.g., password hygiene) – such as the use of unique or strong passwords, periodic change to passwords, sharing passwords with others, and so forth?	**FY2017**	**FY2016**
Yes	41%	41%
No	52%	54%
Unsure	7%	5%
Total	100%	100%

Q26. Does your organization use SSO?	**FY2017**
Yes, fully implemented across the enterprise	27%
Yes, partially implemented across the enterprise	24%
No (skip to Q33a)	50%
Total	100%

Q27. Do you believe that SSO simplifies system users' access to applications and data in your organization?	**FY2017**
Yes	73%
No	22%
Unsure	5%
Total	100%

Q28. Do you believe that SSO increases the security of user access to your organization's applications and data?	**FY2017**
Yes	69%
No	26%
Unsure	5%
Total	100%

Q29a. Does your organization have a policy pertaining to employees' use of passwords and/or biometrics (such as a fingerprint)?	**FY2017**	**FY2016**
Yes	43%	44%
No	52%	51%
Unsure	5%	5%
Total	100%	100%

Q29b. If yes, does your organization strictly enforce this policy?	**FY2017**	**FY2016**
Yes	32%	31%
No	63%	65%
Unsure	5%	4%
Total	100%	100%

Q30b-1. If Q29a=yes, does this policy require employees to use a password or biometric to secure access to mobile devices?	**FY2017**	**FY2016**
Yes	51%	42%
No	46%	54%
Unsure	3%	4%
Total	100%	100%

Q30b-2. If no, why doesn't your organization require password or biometric protections on mobile devices?	FY2017	FY2016
We have other compensating controls for securing mobile devices	35%	33%
We don't see the need for more policies	25%	23%
Passwords are obsolete	21%	19%
Resetting passwords reduces employee productivity	50%	47%
We can't monitor employee non-compliant behavior	49%	54%
Other	1%	
Total	182%	176%

Q31. 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?	FY2017	FY2016
Improves security posture	6%	7%
Diminishes security posture	48%	42%
No affect on security posture	35%	39%
Cannot determine	11%	13%
Total	100%	100%

Q32. Has your organization experienced a data breach or security incident due to the use of Internet of Things (IoT)?	FY2017
Yes	23%
No	77%
Total	100%

Q33. How concerned is your company about the security of IoT devices used in the workplace?	FY2017
Very concerned	29%
Concerned	38%
Somewhat concerned	21%
Not concerned	12%
Total	100%

Q34. How confident is your company that it can contain or minimize the risk of insecure IoT devices?	FY2017
Very confident	11%
Confident	18%
Somewhat confident	22%
Not confident	49%
Total	100%

Part 5. Enabling Security Technologies

Q35. Do the security technologies currently used by your organization detect and block most cyber attacks?	FY2017	FY2016
Yes	39%	33%
No	61%	67%
Total	100%	100%

Q36. 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.	**FY2017**	**FY2016**
Anti-malware	96%	90%
Anti-denial of services	41%	44%
Artificial intelligence/machine learning	27%	
Privileged user access management	36%	
Automated patch management systems	49%	49%
Password protection / management	52%	71%
Big data analytics	22%	24%
Data loss prevention (DLP)	25%	22%
Encryption technologies	41%	37%
Tokenization	14%	13%
Endpoint management	28%	26%
Mobile device management (MDM)	27%	30%
Client firewalls	89%	86%
Identity & access management	39%	34%
Intrusion detection and prevention	62%	53%
Network traffic intelligence	22%	25%
Next generation firewalls (NGFW)	29%	28%
VPM and other secure web gateways	62%	61%
Security incident & event management (SIEM)	30%	31%
Unified threat management (UTM)	12%	13%
Web application firewalls (WAF)	36%	35%
Other	2%	
Total	842%	775%

Q37. In your opinion, what are the most vulnerable endpoints or entry points to your organization's networks and enterprise systems? Select the top 3 choices.	**FY2017**	**FY2016**
Desktops	21%	26%
Laptops	43%	43%
Tablets	20%	28%
Smart phones	39%	43%
Web server	30%	52%
Intranet server	36%	46%
Routers	6%	12%
Portable storage devices (including USBs)	8%	13%
Cloud systems	38%	34%
Mobile/IoT devices	56%	
Other (please specify)	2%	3%
Total	300%	300%

Q38. Please rate the importance of passwords or biometric authentication for securing endpoints and/or entry points to your organization's networks and enterprise systems.	FY2017	FY2016
Essential	41%	40%
Very important	39%	36%
Important	11%	12%
Not important	7%	8%
Irrelevant	1%	3%
Total	100%	100%

Part 6. Cost Estimation

Q39a. Approximately, how much did damage or theft of IT assets and infrastructure cost your organization over the past 12 months?	FY2017	FY2016
None	34%	39%
Less than $5,000	8%	9%
$5,001 to $10,000	2%	6%
$10,001 to $50,000	6%	5%
$50,001 to $100,000	6%	7%
$100,001 to $250,000	8%	6%
$250,001 to $500,000	8%	4%
$500,001 to $999,999	9%	10%
$1 million to $5 million	10%	8%
$5 million to $10 million	6%	5%
More than $10 million	1%	1%
Total	99%	100%
Extrapolated value	$1,027,053	$879,582

**UK amount was converted from GBP to dollars*

Q39b. Approximately, how much did disruption to normal operations cost your organization over the past 12 months?	FY2017	FY2016
None	33%	39%
Less than $5,000	8%	2%
$5,001 to $10,000	2%	3%
$10,001 to $50,000	6%	5%
$50,001 to $100,000	4%	9%
$100,001 to $250,000	10%	10%
$250,001 to $500,000	9%	5%
$500,001 to $999,999	9%	10%
$1 million to $5 million	9%	10%
$5 million to $10 million	6%	5%
More than $10 million	3%	1%
Total	100%	100%
Extrapolated value	$1,207,965	$955,429

Part 7. General Data Protection Regulation (GDPR)

Q40. Will the GDPR require significant changes in your security strategy?	FY2017
Yes, significant change	37%
Yes, some change	37%
Yes, nominal change	18%
No change (skip to Part 8)	8%
Total	100%

Q41. Using the following 10-point scale, please rate your organization's level of readiness to comply with the GDPR. 1 = not ready to 10 = ready.	FY2017
1 or 2	11%
3 or 4	31%
5 or 6	37%
7 or 8	13%
9 or 10	7%
Total	100%
Extrapolated value	5.24

Part 8. Role & Organizational Characteristics

D1. What best describes your position level within the organization?	FY2017	FY2016
Business owner	10%	9%
C-level executive/VP	11%	10%
Director	17%	18%
Manager	21%	21%
Supervisor	12%	12%
Staff/technician	24%	24%
Administrative	4%	4%
Consultant/contractor	1%	2%
Total	100%	100%

D2. Which of the following commands do you report to in your current role?	FY2017	FY2016
Business owner / board	12%	14%
CEO/executive committee	9%	9%
COO or head of operations	16%	15%
CFO, controller or head of finance	3%	3%
CIO or head of corporate IT	27%	28%
Business unit leader or general manager	13%	12%
Head of compliance or internal audit	4%	4%
Head of risk management	5%	4%
Head of IT security	11%	11%
Total	100%	100%

D3. What best describes your organization's primary industry classification?	FY2017	FY2016
Aerospace & defense	1%	0%
Agriculture & food services	2%	4%
Communications	2%	2%
Construction and real estate	3%	4%
Consumer goods / products	6%	7%
Education & research	2%	3%
Entertainment, media and publishing	3%	1%
Financial services	14%	15%
Healthcare	7%	9%
Industrial	9%	8%
Logistics and distribution	1%	2%
Manufacturing	8%	6%
Pharmaceuticals	3%	3%
Public sector	9%	6%
Retailing	12%	12%
Services	9%	9%
Technology & software	7%	8%
Transportation	2%	3%
Total	100%	100%

Please contact research@ponemon.org or call us at 800.877.3118 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 organizations.

As a member of the **Council of American Survey Research Organizations (CASRO)**, 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

Keeper Security is transforming the way businesses and individuals protect their passwords and sensitive digital assets to significantly reduce cyber theft. As the leading password manager and digital vault, Keeper helps millions of people and thousands of businesses substantially mitigate the risk of a data breach. Keeper is SOC 2 Certified and utilizes best-in-class encryption to safeguard its customers. Keeper protects industry-leading companies including Chase, Sony, Siemens, Chipotle, Philips and The University of Alabama at Birmingham. Keeper partners with global OEMs and mobile operators to preload Keeper on smartphones and tablets. Learn more at https://keepersecurity.com.