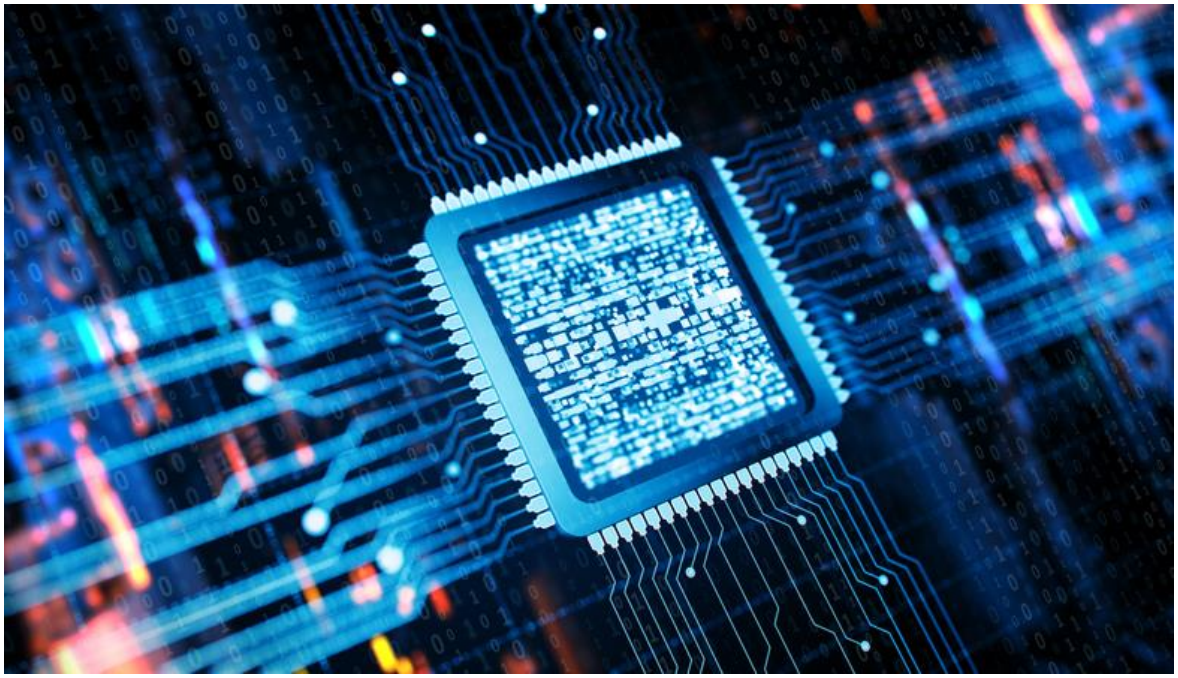


2019 Global State of Cybersecurity in Small and Medium-Sized Businesses (SMB)

Sponsored by Keeper Security

Independently conducted by Ponemon Institute LLC

Publication Date: October 1, 2019

2019 Global State of Cybersecurity in Small and Medium-Sized Businesses

Ponemon Institute, October 2019

Part 1. Executive summary

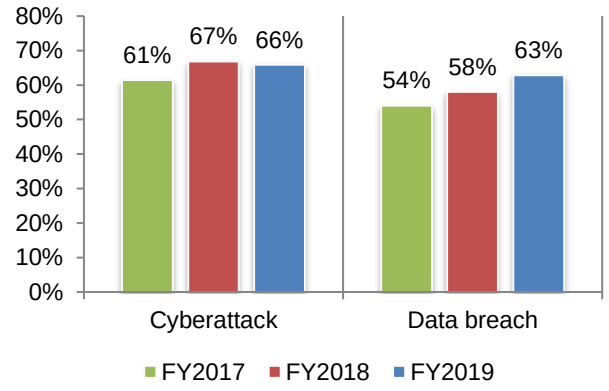
Ponemon Institute is pleased to present the results of the *2019 Global State of Cybersecurity in Small and Medium-Sized Businesses* sponsored by Keeper Security. This is the third annual study that focuses exclusively on organizations with a headcount of less than 100 to 1,000.

We surveyed 2,176 individuals in companies in the United States, the United Kingdom and for the first time DACH (Germany, Austria, Switzerland), Benelux (Belgium, Netherlands, Luxemburg) and Scandinavia (Denmark, Norway and Sweden).

In addition to tracking trends in cyberattacks and data breaches, this year's study reveals how SMBs are unprepared to deal with risks created by third parties and the Internet of Things (IoT).

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

Yes responses



A key takeaway from this research is that over the past three years there has been a significant increase in SMBs experiencing a data breach as shown in Figure 1. In addition, 66 percent of respondents said their organization experienced a cyberattack in the past 12 months.

In the aftermath of these incidents, these companies spent an average of $1.2 million -- an increase from $1.03 million in 2017 -- because of damage or theft of IT assets and infrastructure. In addition, disruption to normal operations cost an average of $1.9 million, an increase from $1.21 million in 2017.

Following are the most salient findings from this research.

Part 2. Key findings

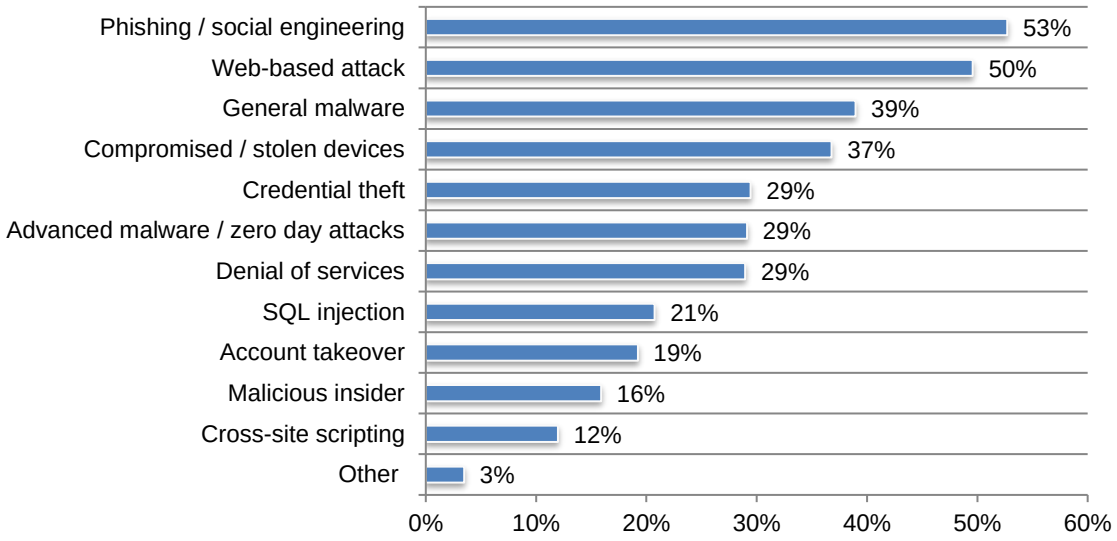
In this section we present a deeper dive into the findings. The complete audited findings are presented in the Appendix of this report. We have organized the report according to the following themes:

- Most SMBs have experienced cyberattacks and data breaches
- Cybersecurity posture and governance
- Trends in password practices and other authentication methods
- Third party and IoT risks
- Regional and country differences

Most SMBs have experienced cyberattacks and data breaches

Phishing and web-based attacks are the top two cyberattacks. Seventy-two percent of respondents said that they have experienced at least one cyberattack. As shown in Figure 2, phishing/social engineering is the number one attack SMBs experience (53 percent of respondents). Other frequent attacks are web-based attacks and general malware (50 percent and 39 percent of respondents, respectively).

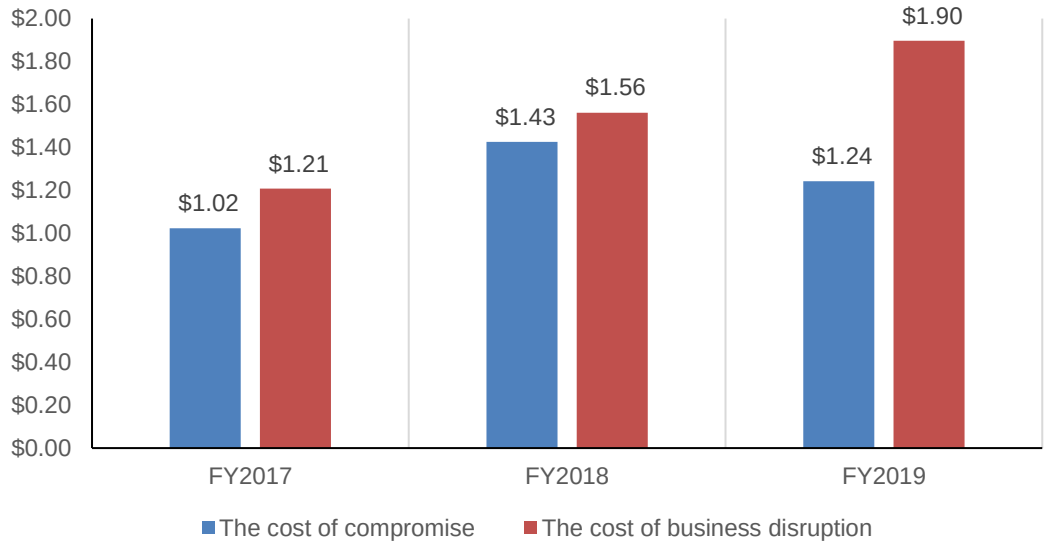
Figure 2. What types of attacks did your business ever experience?
More than one choice allowed



The financial consequences of security compromises and business disruptions to SMBs are severe. According to Figure 3, the average cost of recovering from business disruption has increased significantly since 2017. However, the average cost of dealing with damage or theft of IT assets and infrastructure declined from $1.43 million in 2018 to $1.24 million in 2019.

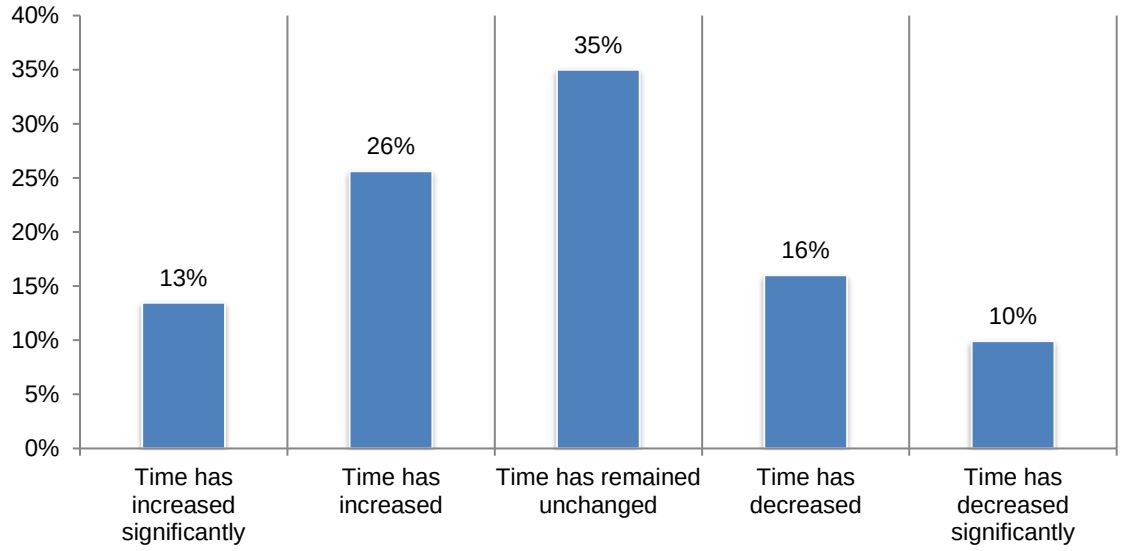
Figure 3. The average cost of compromise and business disruption over a 12-month period

US$ millions



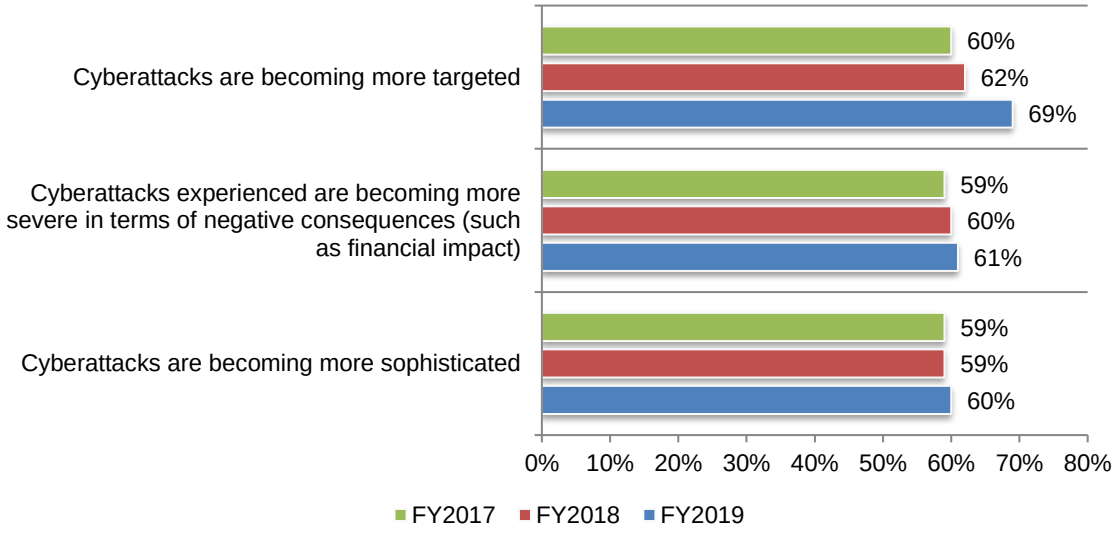
The time to respond to a cyberattack has increased or not improved. According to Figure 4, only 26 percent of respondents (16 percent + 10 percent) said their organizations have been able to decrease the time it takes to respond to a cyberattack.

Figure 4. In the past 12 months, how has the time to respond to a cyberattack changed?



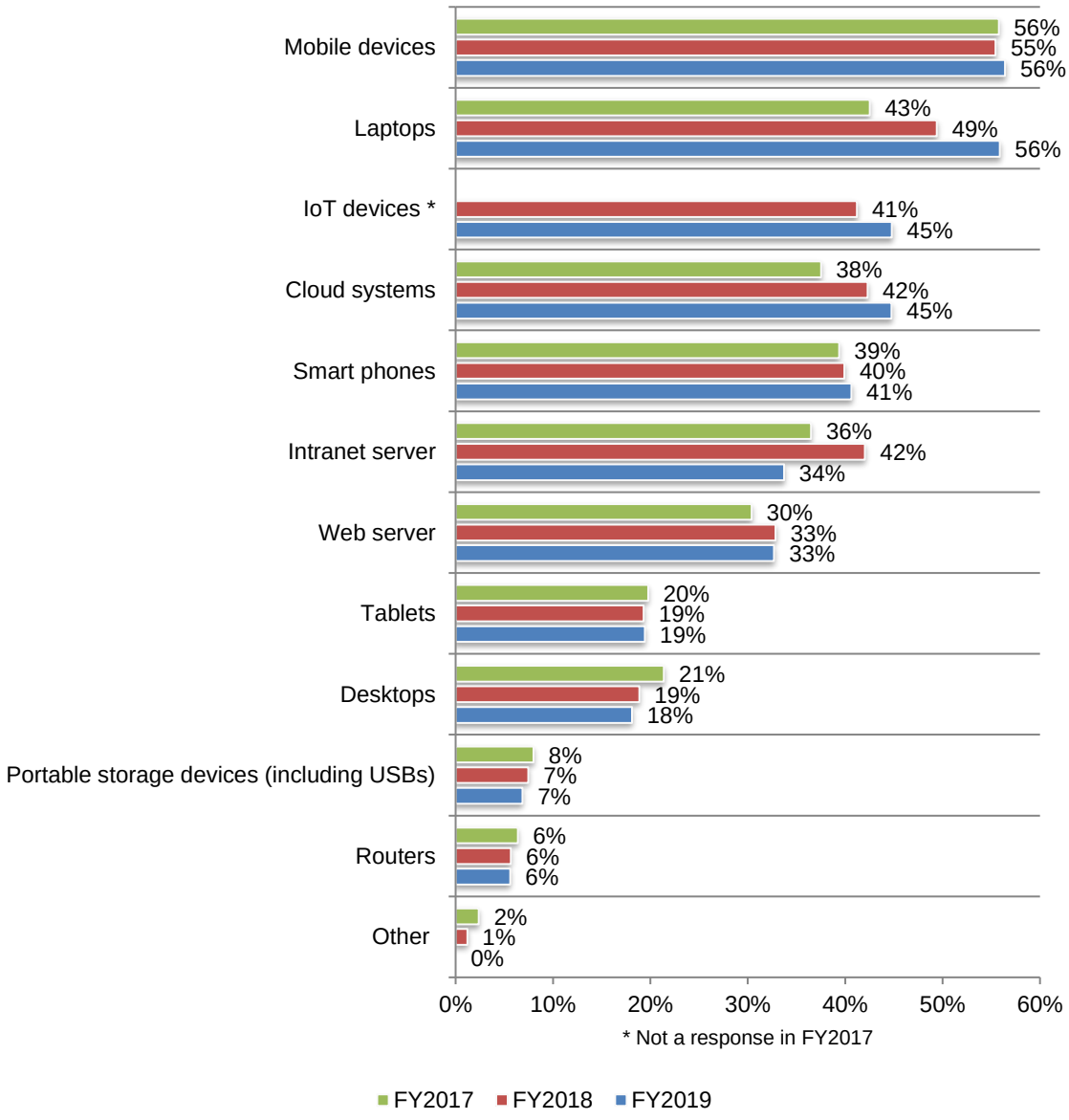
Cyber threats against SMBs are becoming more targeted. Since 2017, SMBs report that cyber threats are more targeted, an increase from 60 percent to 69 percent of respondents in 2019. Most respondents said cyberattacks against their companies are severe and sophisticated (61 percent and 60 percent, respectively) and this has not changed since 2017 as shown in Figure 5.

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



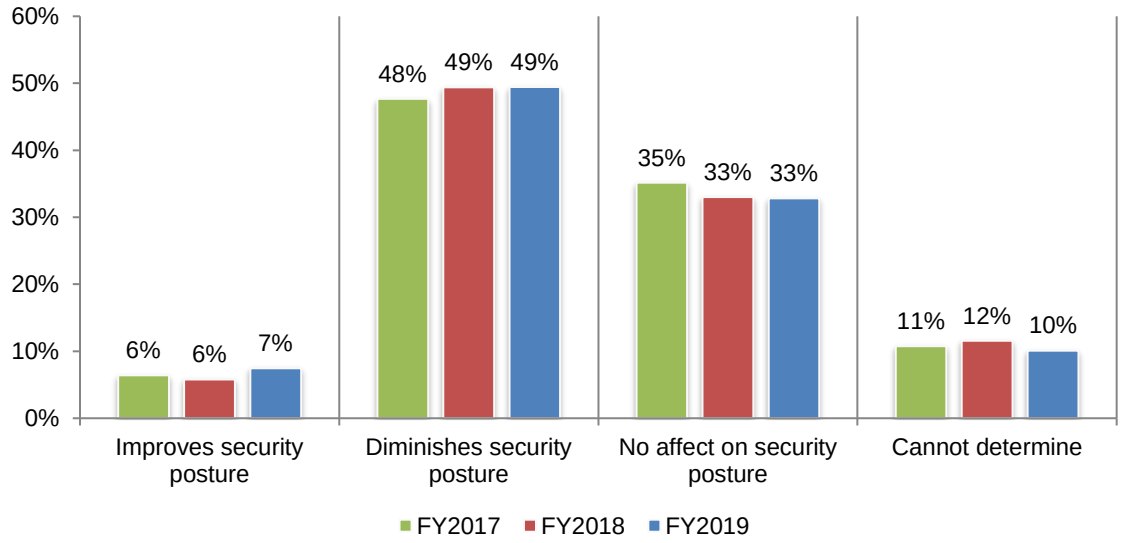
More SMBs said the laptop is the most vulnerable endpoint or entry point to networks and enterprise systems. As shown in Figure 6, mobile devices and laptops are considered, by far, the most vulnerable endpoint or entry point to respondents' companies' networks and enterprise systems. Since 2017, respondents who believe laptops are vulnerable increased from 43 percent of respondents to 56 percent of respondents.

Figure 6. 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. On average, companies represented in this research have 120 business-critical applications and an average of 48 percent of these business-critical applications are accessed from mobile devices such as smartphones and tablets. This is an increase from 45 percent in last year's research. As shown in Figure 7, nearly half (49 percent) of respondents said these devices diminish their companies' security posture.

Figure 7. How does the use of mobile devices to access business-critical applications and IT infrastructure affect your organization's security posture?

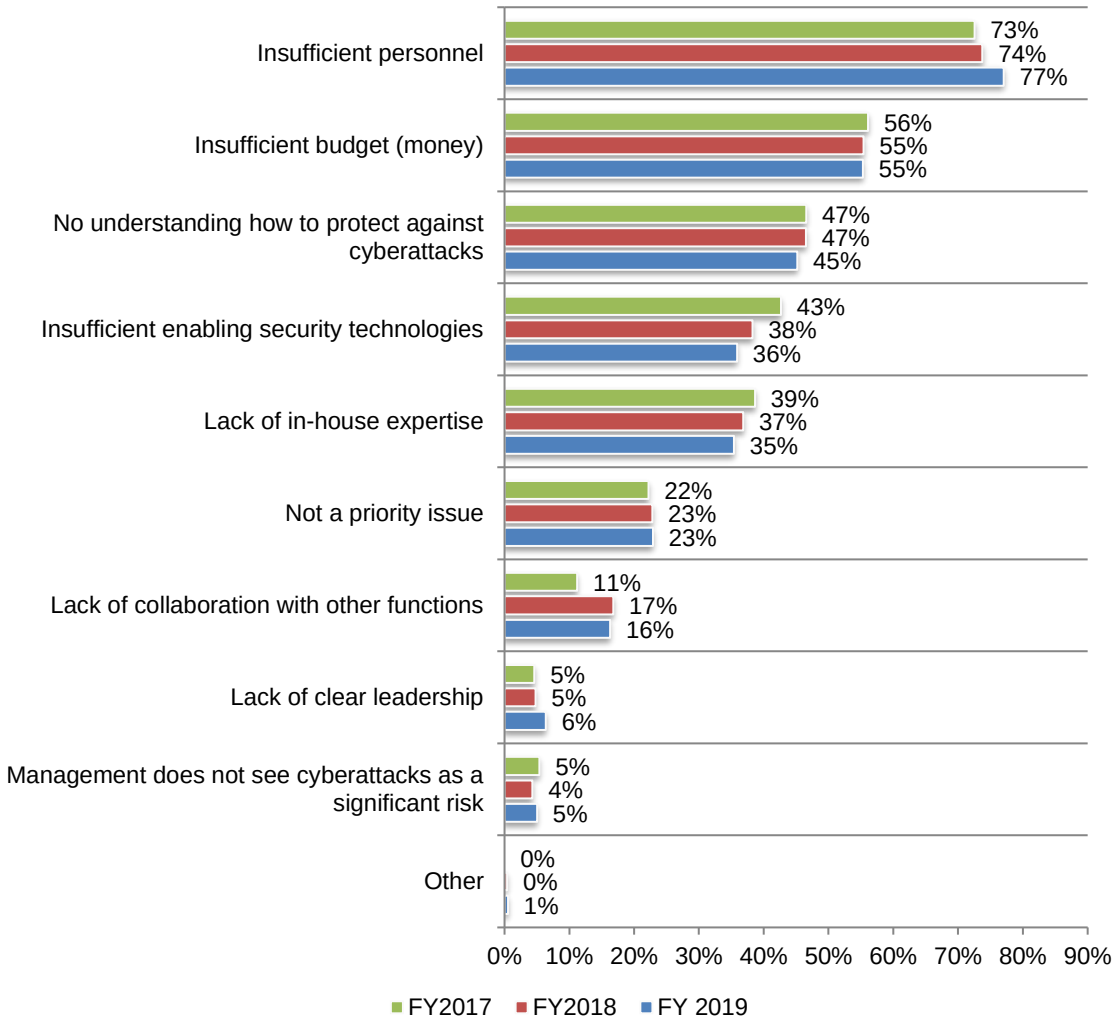


Cybersecurity posture and governance

SMBs continue to struggle with insufficient personnel and money. Only 30 percent of respondents rate their organization's IT security posture in terms of its effectiveness at mitigating risks, vulnerabilities and attacks across the enterprise as very high. Figure 8 lists the challenges companies face when trying to create a stronger security posture.

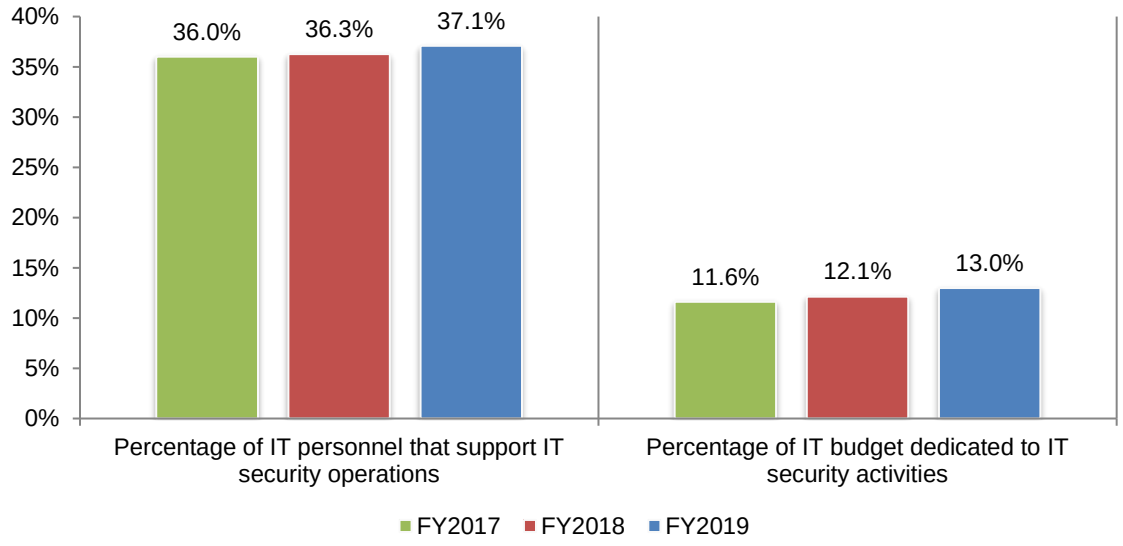
The biggest problem is not having the personnel to mitigate cyber risks, vulnerabilities and attacks (77 percent of respondents). The next biggest challenges are insufficient budget (55 percent of respondents) and no understanding of how to protect against cyberattacks (45 percent of respondents). Since 2017, the challenge of not having sufficient enabling security technologies has decreased from 43 percent of respondents to 36 percent of respondents.

Figure 8. What challenges keep your IT security posture from being fully effective?
Three choices allowed



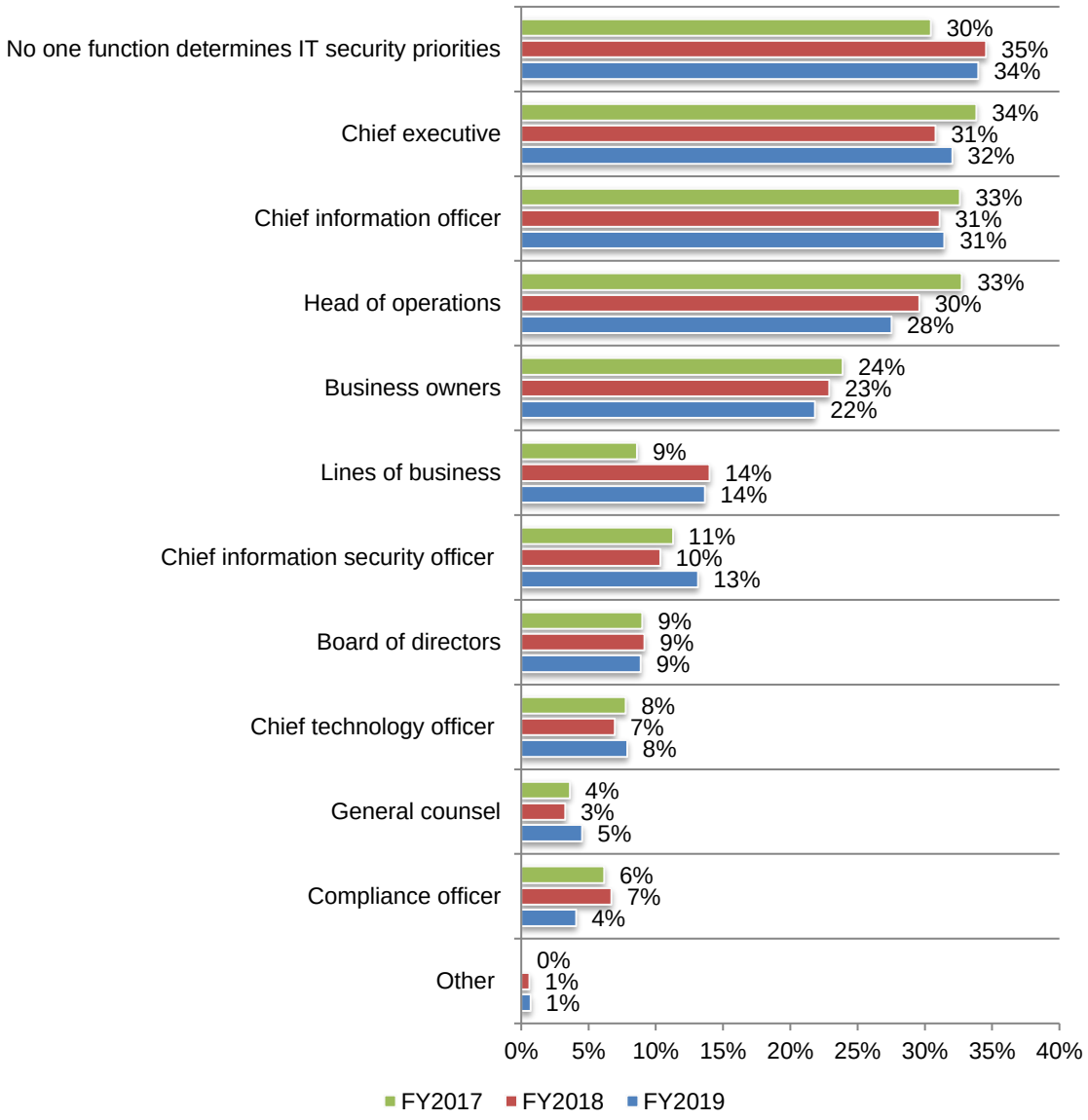
Sixty-five percent of respondents said their budget for achieving a strong security posture is inadequate or unsure and 42 percent of respondents said they have an appropriate level of in-house expertise. As Figure 9 shows, only an average of 13 percent of the IT budget is dedicated to IT security activities and an average of 37 percent of the IT personnel support IT security operations.

Figure 9. The percentage of IT budget and personnel support IT security operations
Extrapolated value



Leadership in determining IT security priorities is lacking. As shown in Figure 10, 34 percent of respondents said no one person is responsible for determining IT security priorities, an increase from 30 percent of respondents in 2017. According to the findings, responsibility for companies' IT security strategy is dispersed throughout the company.

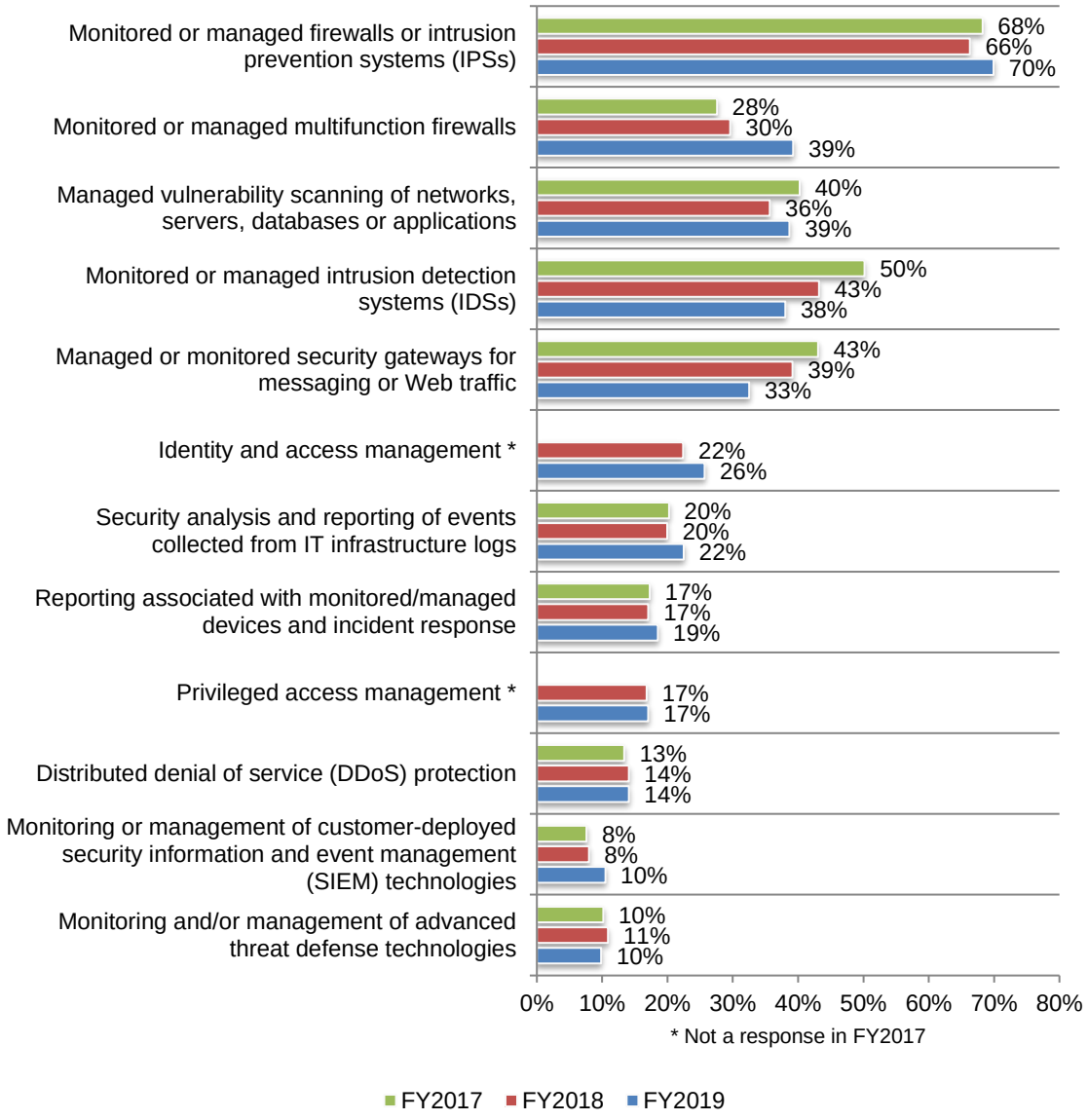
Figure 10. Who determines IT security priorities?
Two choices allowed



More SMBs are engaging managed security services providers (MSSPs) to support the IT security function. On average, 32 percent of a company's IT security operations are supported by MSSPs, this is an increase from 29 percent in last year's study.

According to Figure 11, 70 percent of respondents said their MSSP monitors or manages firewalls or intrusion prevention systems (IPS). Since 2017, more SMBs are engaging MSSPs to monitor or manage multifunction firewalls (an increase from 28 percent in 2017 to 39 percent in this year's research). Fewer respondents said they use MSSPs to monitor or manage intrusion detection systems security gateways for messaging or web traffic.

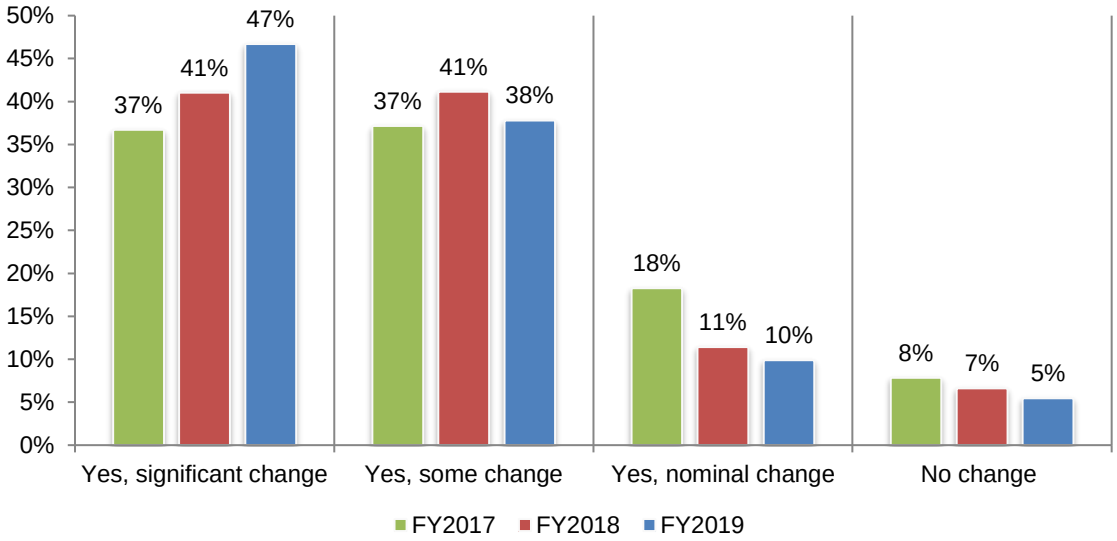
Figure 11. What services are provided by MSSPs to support your IT security posture?
More than one choice permitted



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

Eighty-three percent of respondents said their organizations are required to comply with GDPR. As Figure 12 shows, 95 percent of respondents said the new regulations required changes to their privacy and security strategy. In 2018, 93 percent of respondent said the new regulation did require significant changes.

Figure 12. Will the GDPR require significant changes in your privacy and security strategy?



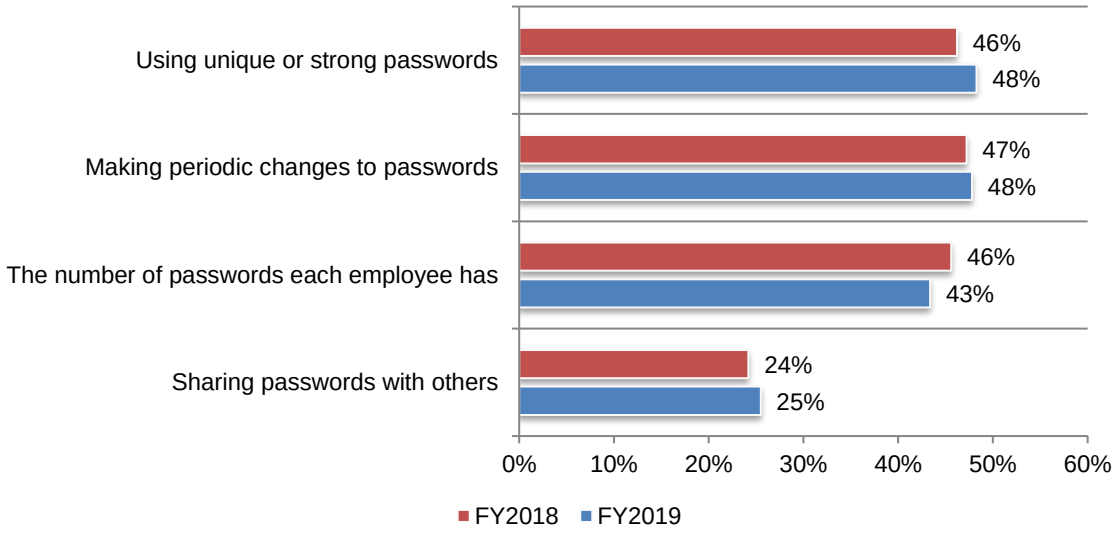
Trends in password practices and authentication methods

Almost half of SMBs have suffered an attack involving the compromise of employees' passwords. Forty-seven percent of respondents said their companies had an attack involving the compromise of employees' passwords in the past year, and the average cost of each attack was $384,598. To mitigate the risk of such attacks, policies pertaining to employees' use of passwords and/or biometrics, such as a fingerprint are helpful. According to the research, 55 percent of respondents said their companies do not have or are unsure of such a policy.

Sixty-four percent of respondents said the use of strong passwords is an essential part of their organization's security strategy. Despite the importance of strong passwords, most SMBs are not improving their ability to know employees' password practices. In fact, 58 percent of respondents said they do not have, or are unsure if they have, visibility into employees' password practices.

According to Figure 13, if they do have visibility less than half (48 percent of respondents) require the use of unique or strong passwords and only 25 percent of respondents said their organizations can determine if employees are sharing passwords.

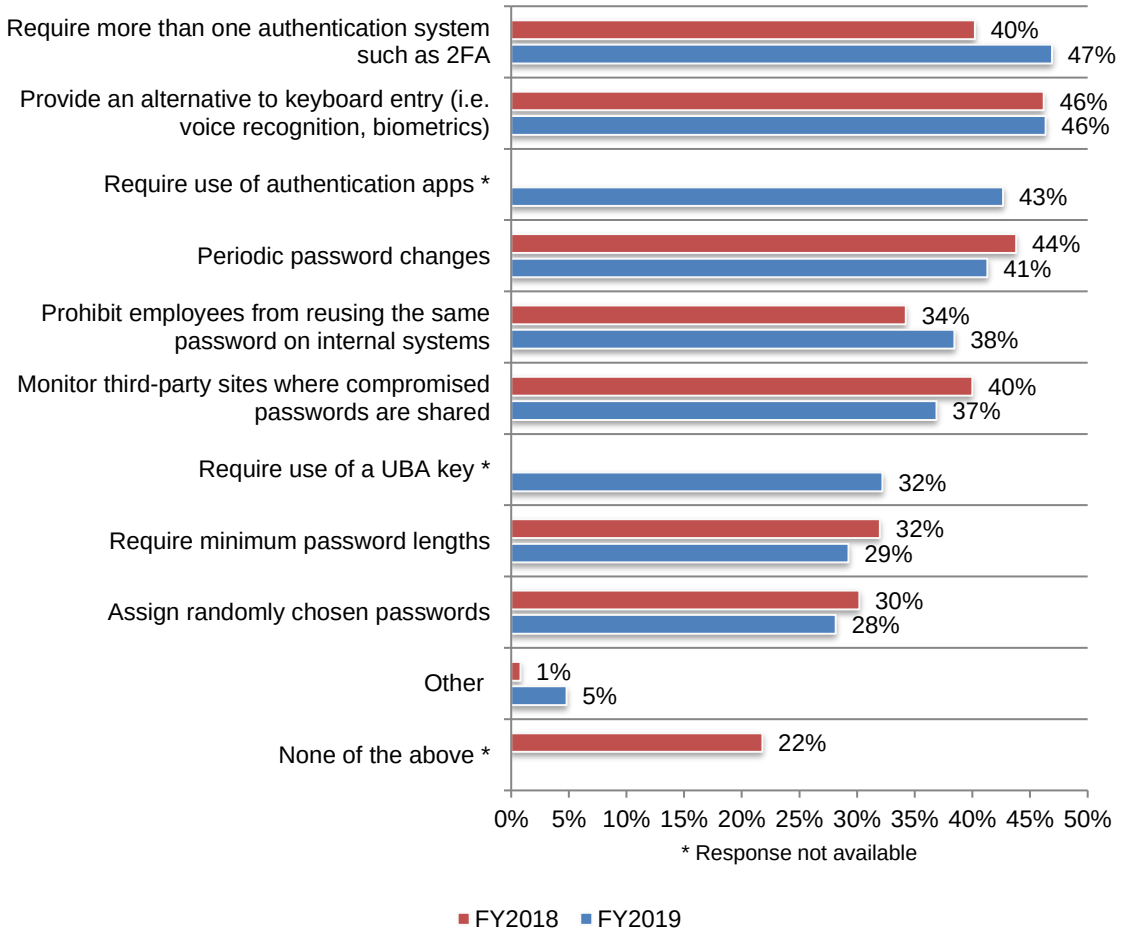
Figure 13. Is your company able to determine employees' password practices?
More than one choice allowed



SMBs require more than one authentication system. According to Figure 14, almost half (47 percent of respondents) said their companies require two-factor authentication or other multi-authentication systems. This practice is followed by providing an alternative to keyboard entry such as voice recognition and biometrics.

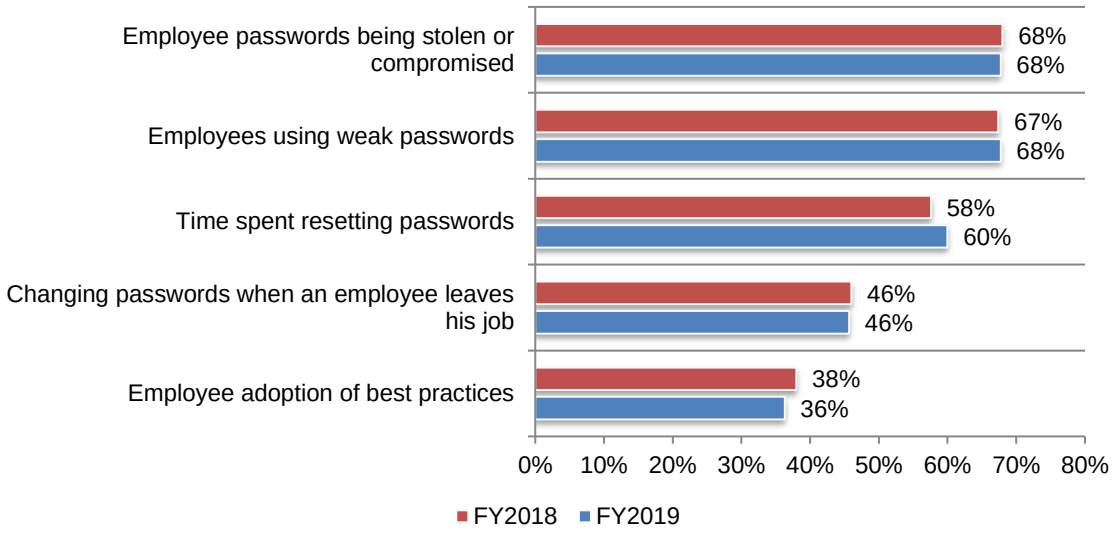
However, most companies are not requiring employees to improve their password practices. Only 38 percent of respondents said their companies prohibit employees from reusing the same password on internal systems and only 29 percent of respondents said they require minimum password lengths.

Figure 14. Does your organization take any of the following steps?
More than one choice allowed



Employees' use of weak passwords leads to theft or passwords being compromised. Figure 15 lists what respondents think are the biggest pain points in managing employees' passwords. As shown, 68 percent of respondents said having to deal with passwords being stolen or compromised and employees using weak passwords are the biggest pain points.

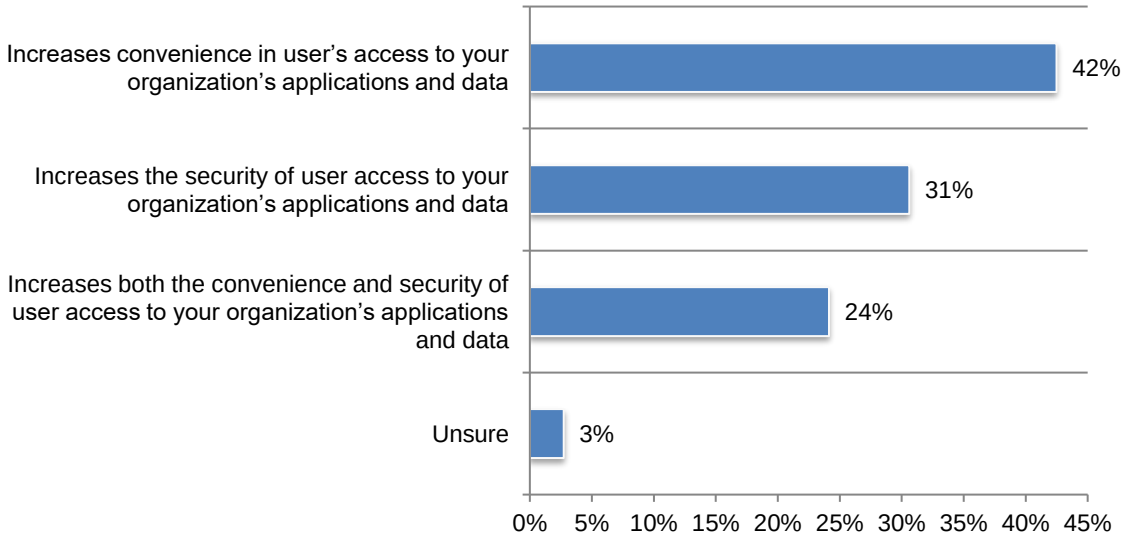
Figure 15. What is your biggest pain point about employees and their passwords?
Two choices allowed



Convenience and security are the two top benefits of single sign-on (SSO). In the context of this research, SSO enables a user to log 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.

Sixty-four percent of respondents said their companies have SSO either fully (34 percent) or partially implemented (30 percent). According to these respondents, the primary benefits are convenience (42 percent) and increased security (31 percent), as shown in Figure 16.

Figure 16. What are the benefits of SSO?



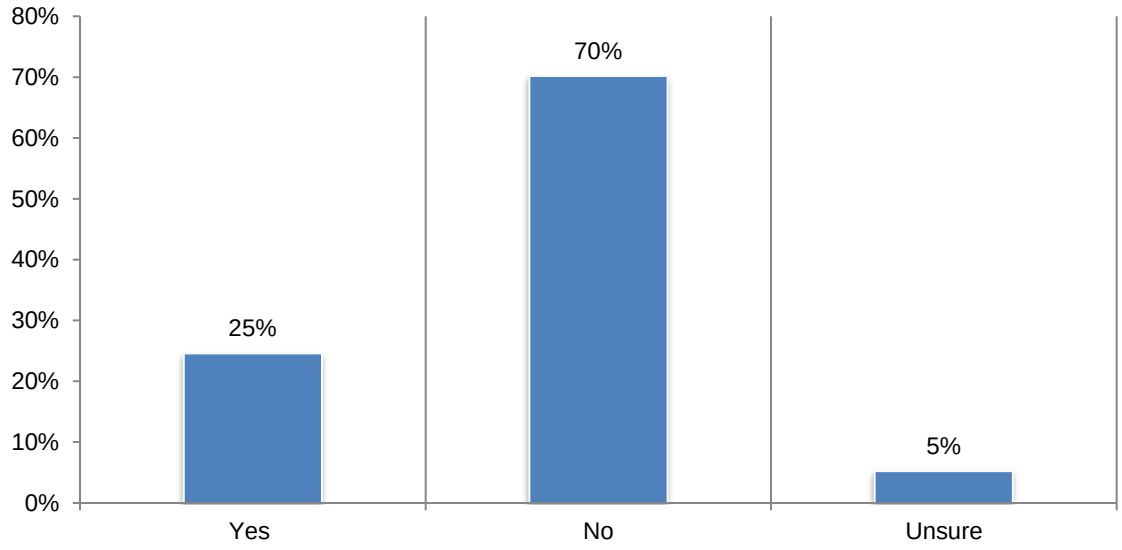
Third-party and IoT risks

For the first time, SMBs were surveyed about their vulnerability to a data breach caused by third-party and IoT risks. In the context of this research, IoT is defined as the network of physical objects or "things" embedded with electronics, software, sensors and network connectivity, which enables these objects to collect, monitor and exchange data. Examples of IoT devices in the workplace include network-connected printers and building automation solutions. It is projected there will be a total of 22.5 billion IoT devices in 2021, up from 6.6 billion in 2016. Between 2016 and 2021 there will be $4.8 trillion in aggregate IoT investment.[1]

The majority of SMBs consider third-party risk a serious threat to sensitive and confidential information. Fifty-seven percent of respondents said third parties put their companies at risk for a data breach and 58 percent of respondents said they are not confident that their primary third party would notify them if it had a data breach involving sensitive and confidential information.

SMBs are also at risk because most of them (70 percent of respondents) do not have a comprehensive inventory of all third parties with whom they share sensitive and confidential information, as shown in Figure 17. Without this information, they are unable to conduct assessments to ensure their third parties are taking steps to safeguard their sensitive and confidential information.

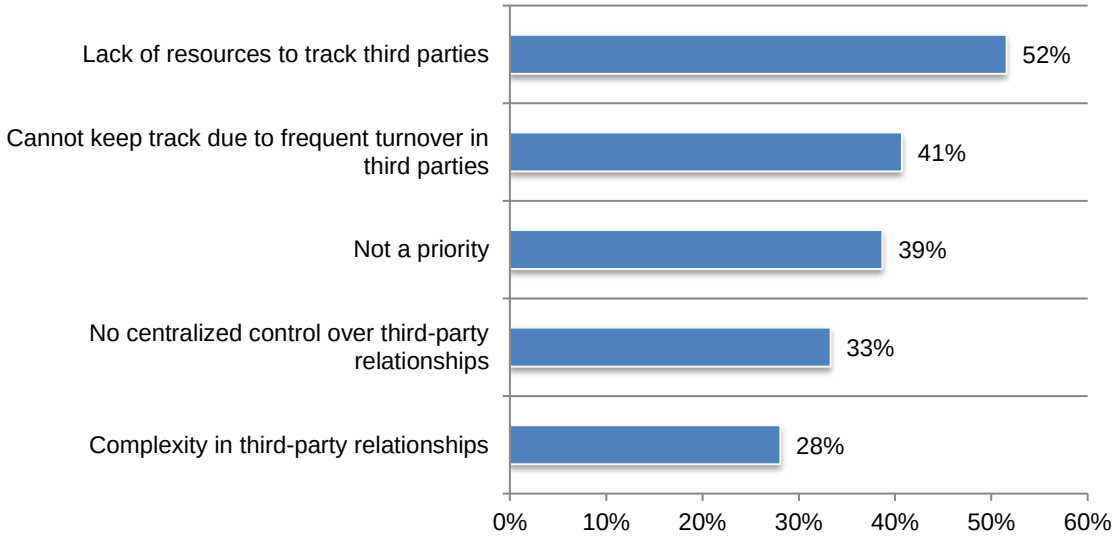
Figure 17. Does your company have a comprehensive inventory of all third parties with whom it shares sensitive and confidential information?



[1] "The Internet of Things 2017 Report: How the IoT Is Improving Lives to Transform the World," by Peter Newman, Business Insider, January 12, 2017

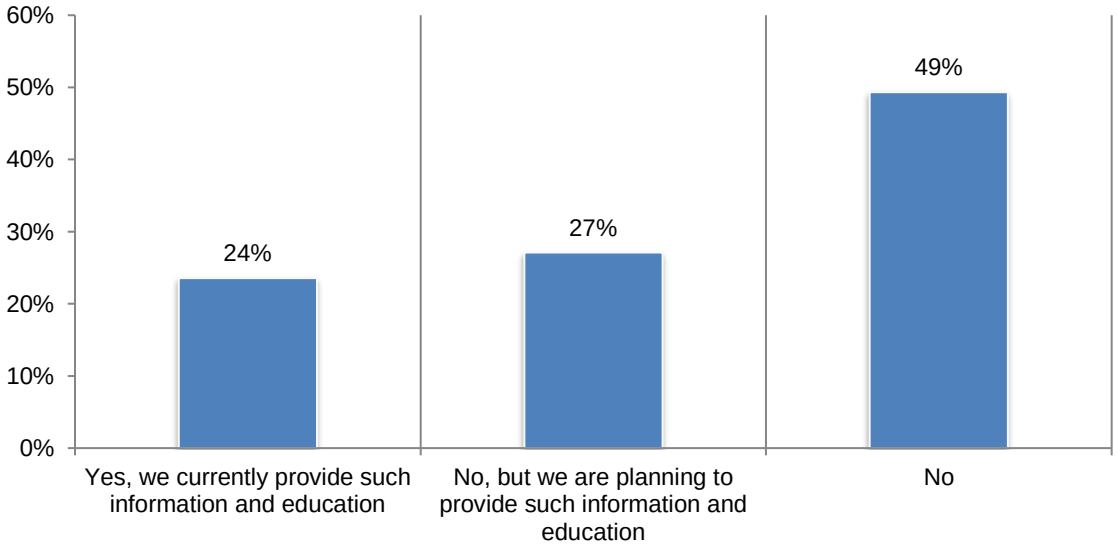
SMBs are unable to track third parties with whom they share their sensitive data. As shown above, 70 percent of respondents said they do not have an inventory with whom they share sensitive data. The two primary reasons are a lack of resources (52 percent of respondents) and the inability to track third parties because of frequent turnover (41 percent of respondents), according to Figure 18.

Figure 18. If no or unsure, why?
More than one response permitted



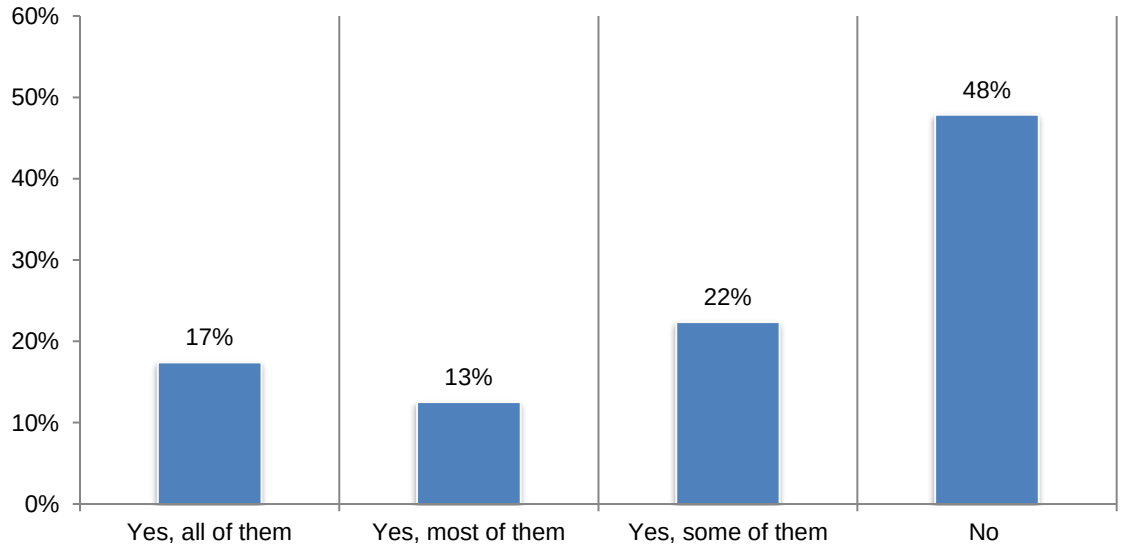
SMBs recognize the risks created by IoT devices. Eighty percent of respondents said it is likely a security incident related to unsecured IoT devices or applications could be catastrophic to their companies. However, very few SMBs are informing and educating employees and third parties about the IoT risk in the workplace

Figure 19. Does your organization inform and educate employees and third parties about the risks created by IoT devices in the workplace?



Only 21 percent of respondents said their companies are monitoring the risk of IoT devices in the workplace. Similar to not understanding what third parties have their sensitive and confidential information, almost half of respondents (48 percent) said they are not aware of the network of physical objects connected to the internet.

Figure 20. Are you aware of the network of physical objects in your company that are connected to the internet?

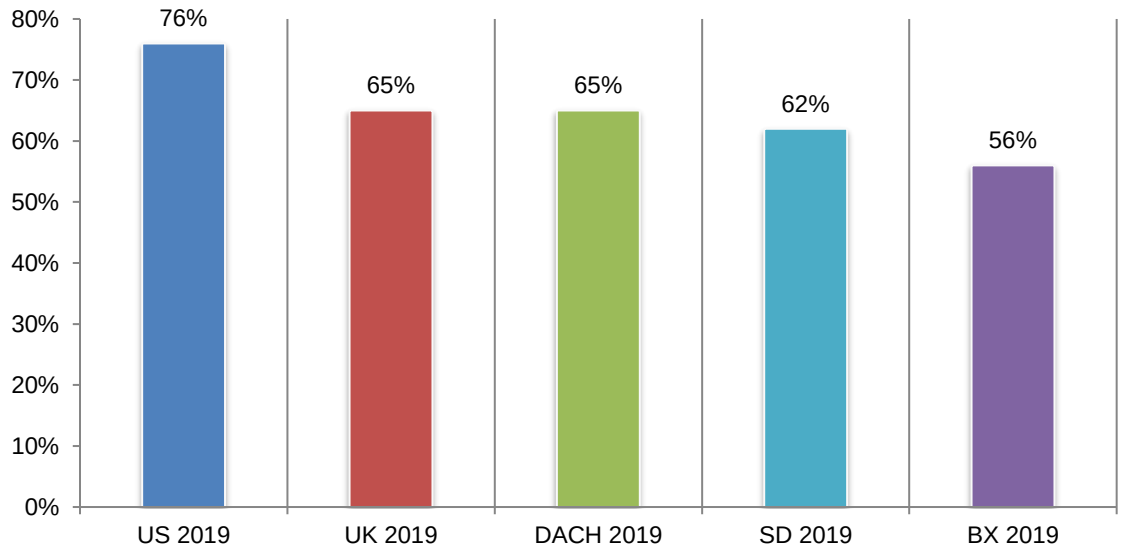


Country and regional differences

In this section, we present the most salient differences among the countries and regions represented in this study. These include: the US (592 respondents), the UK (378 respondents); Germany, Austria, Switzerland (DACH, 449 respondents); Belgium, Netherlands and Luxembourg (BX, 395 respondents); and Denmark Norway and Sweden (SD, 362 respondents).

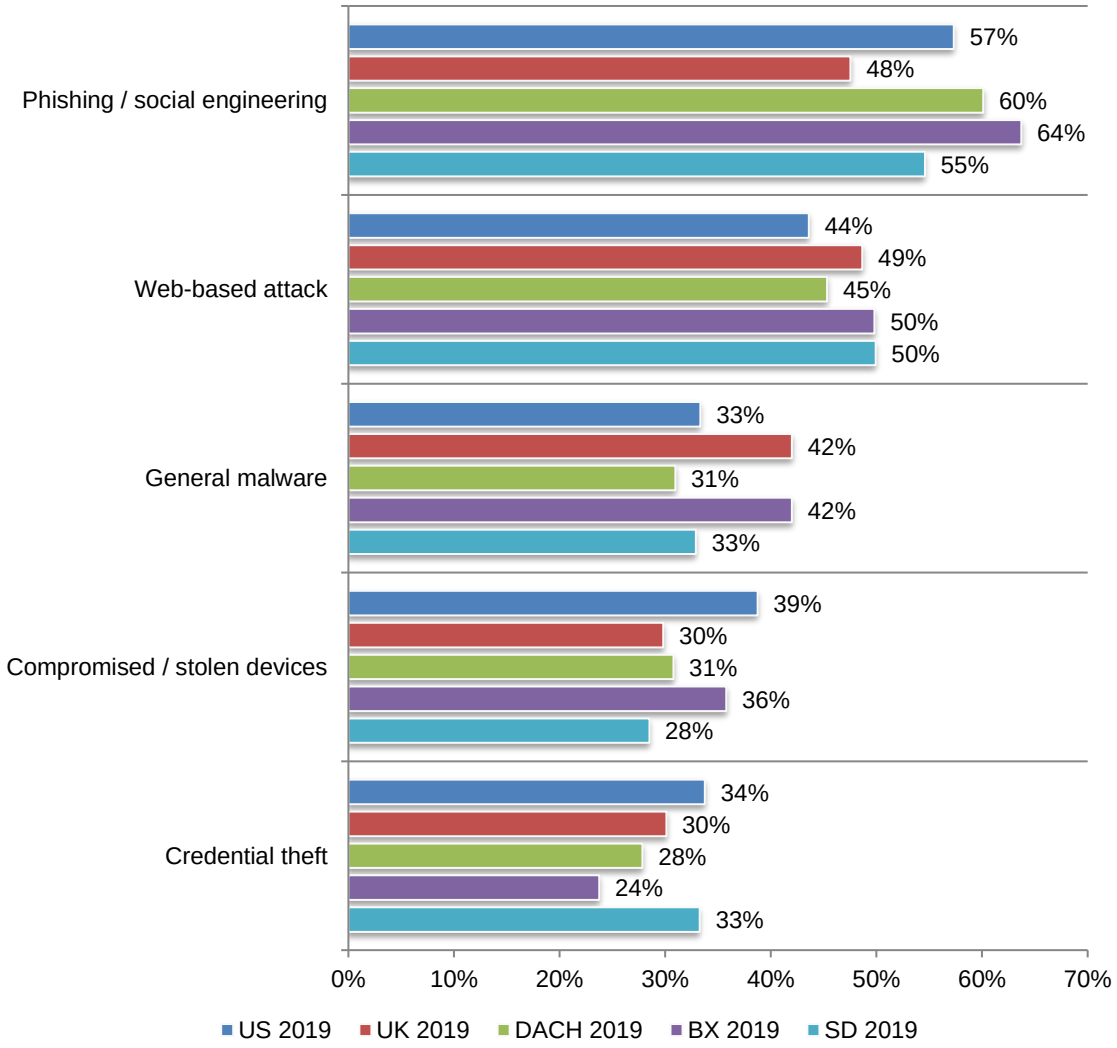
US companies have the most cyberattacks. According to Figure 21, 76 percent of respondents in the US said their companies had a cyberattack in the past year. The countries with the lowest occurrence of cyberattacks are Belgium, Netherlands and Luxembourg (56 percent of respondents).

Figure 21. Has your organization experienced a cyberattack in the past 12 months?



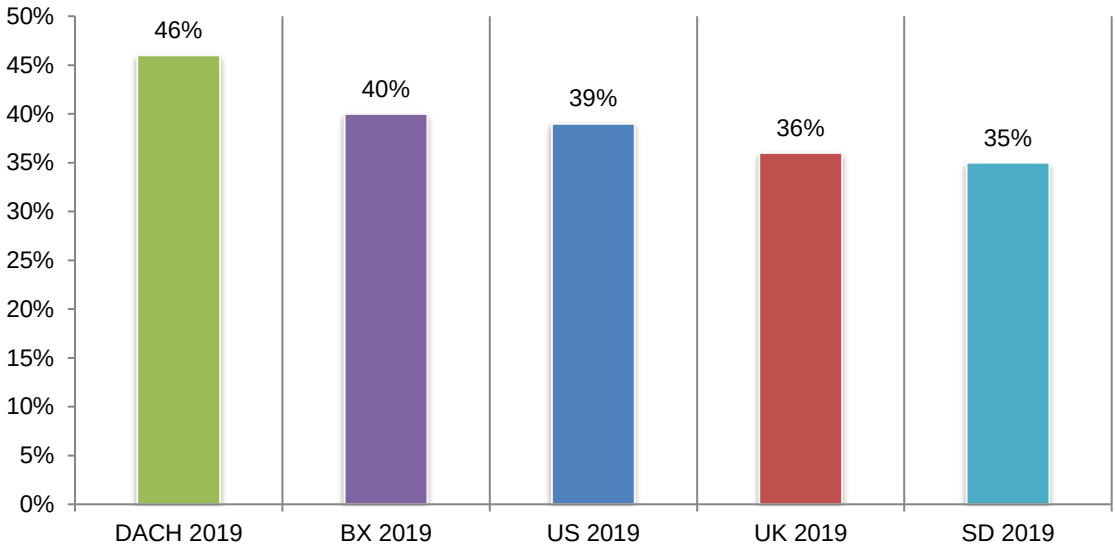
Phishing and social engineering are the most common types of cyberattacks experienced by SMBs in all countries. DACH and BX countries were more likely to have phishing/social engineering attacks (60 percent and 64 percent of respondents, respectively). UK and BX were more likely to have general malware attacks (both 42 percent of respondents).

Figure 22. What best describes the type of cyberattacks your company experienced in the past 12 months?



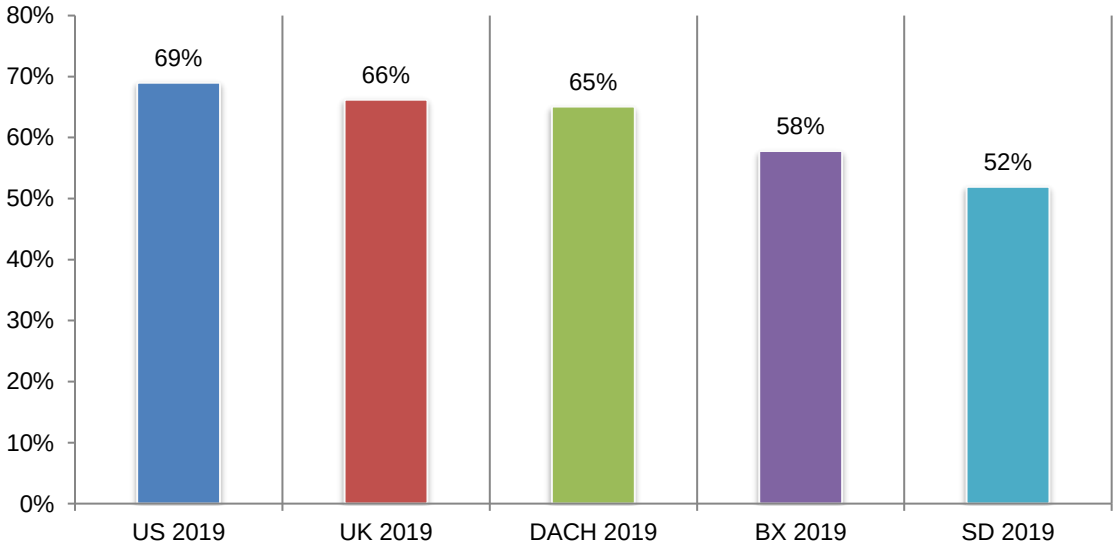
DACH and BX respondents said it is taking longer to respond to a cyberattack (46 and 40 percent of respondents, respectively). In contrast, only 35 percent of respondents in SD countries said the time has increased.

Figure 23. In the past 12 months, how has the time to respond to a cyberattack?
Increased significantly and Increased responses combined



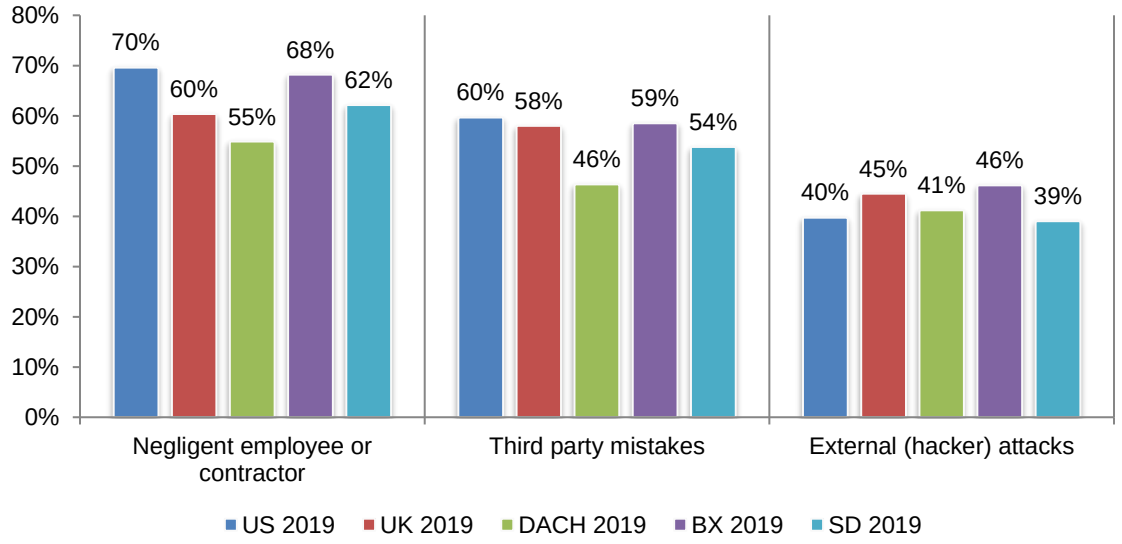
The US, UK and DACH had the most data breaches in the past 12 months. As shown in Figure 24, the majority of all countries had a data breach in the past 12 months. The US (69 percent of respondents), UK (66 percent of respondents) and DACH (65 percent of respondents) had the most data breaches.

Figure 24. Has your organization experienced a data breach in the past 12 months?



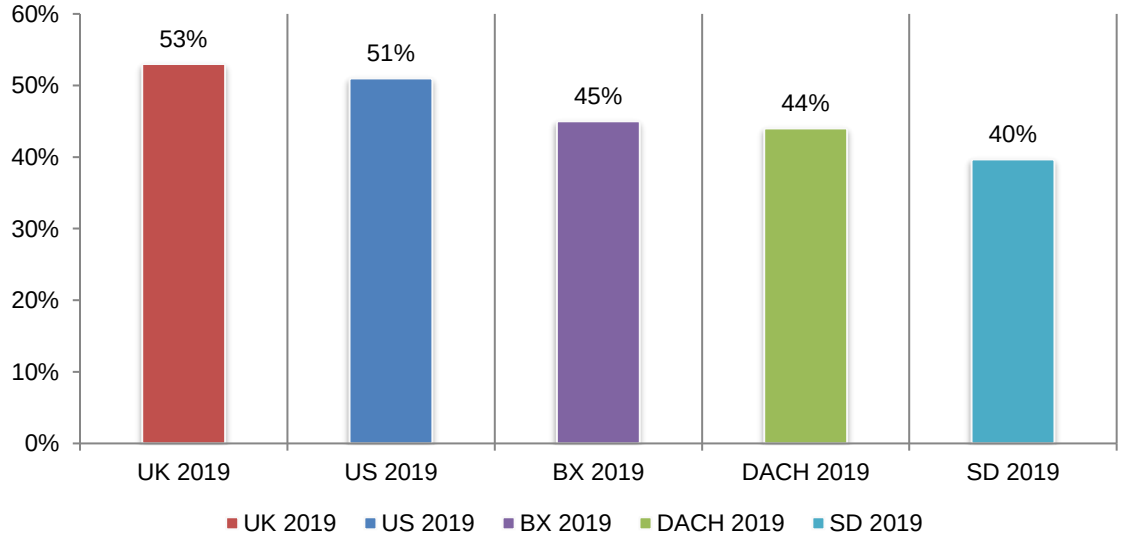
The root cause of most data breaches is the negligent employee or contractor. Figure 25 presents the three root causes of the data breaches experienced by SMBs. The US and BX were most likely to have data breaches caused by negligent employee or contractor and third-party mistakes. The UK and BX were more likely to have a data breach caused by a hacker.

Figure 25. What were the root causes of the data breach?



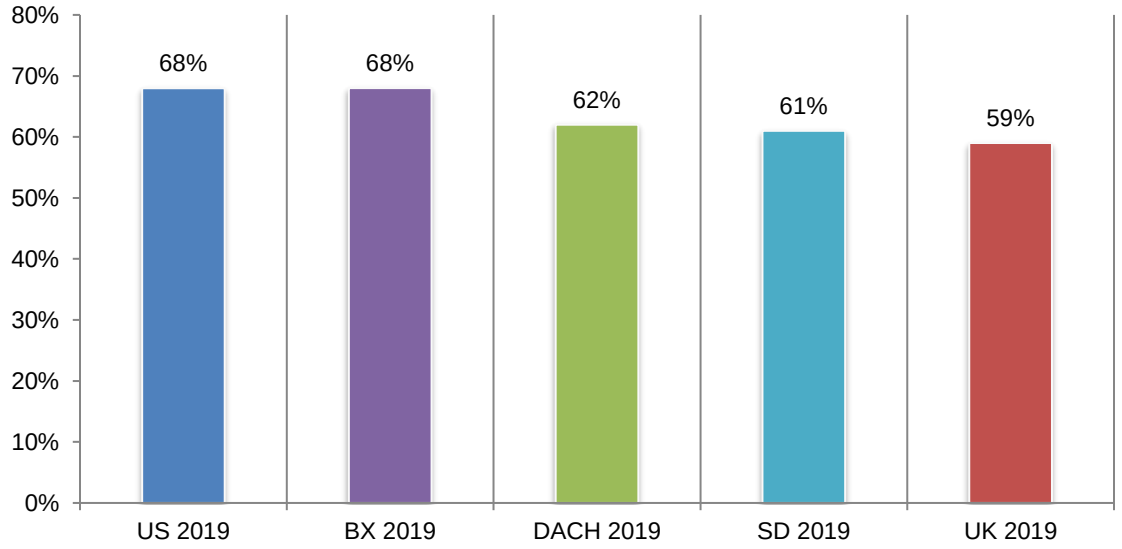
SMBs in the UK and US are more likely to have an attack involving the compromise of employees' passwords, according to 53 percent and 51 percent of respondents, respectively.

Figure 26. Have you had an attack involving the compromise of employees' passwords in the past 12 months?
Yes responses presented



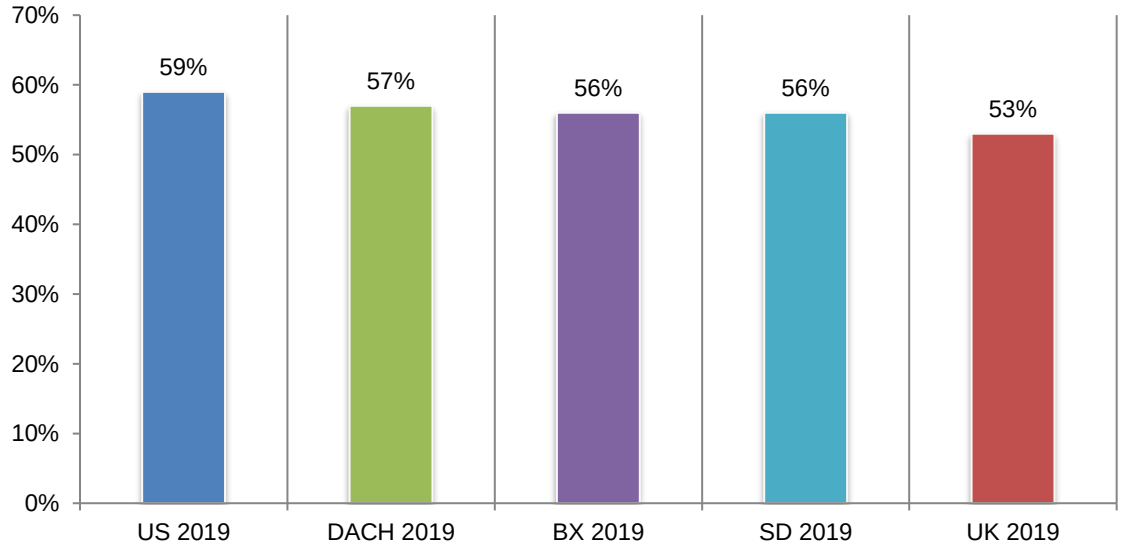
Most, but not all, SMBs are making the strong use of passwords a security priority. The countries most likely to make the use of strong passwords an essential part of their security defense are the US and BX, according to Figure 27.

Figure 27. The use of strong passwords is an essential part of my organization's security defense
Strongly agree and Agree responses combined



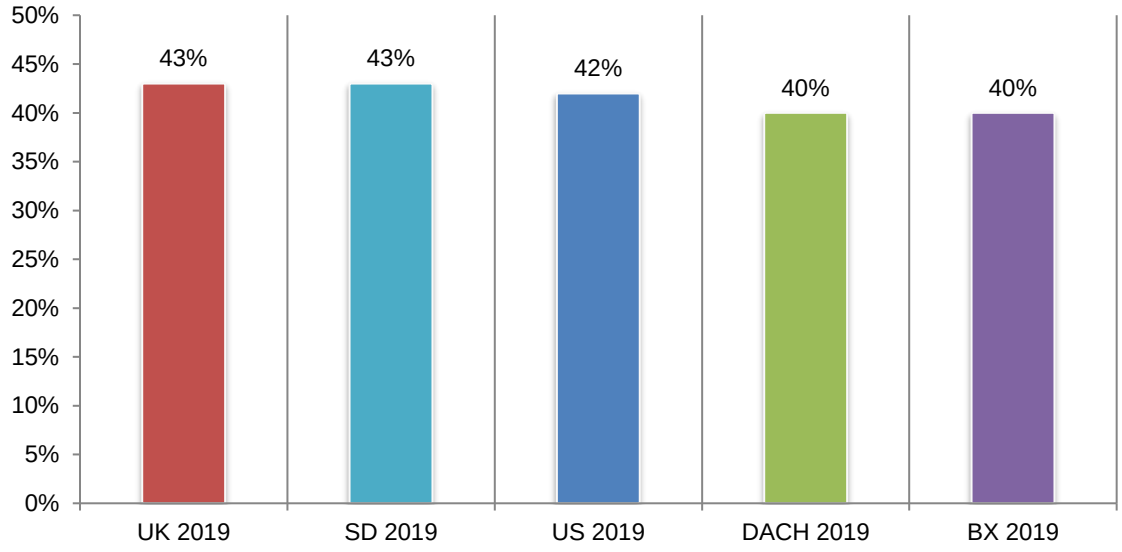
The majority of SMBs recognize the risks created by third parties. As shown in Figure 28, the US and DACH are most likely to recognize the risk to their sensitive and confidential information.

Figure 28. Our organization considers third-party risk a serious threat to sensitive and confidential information
Strongly agree and Agree responses combined



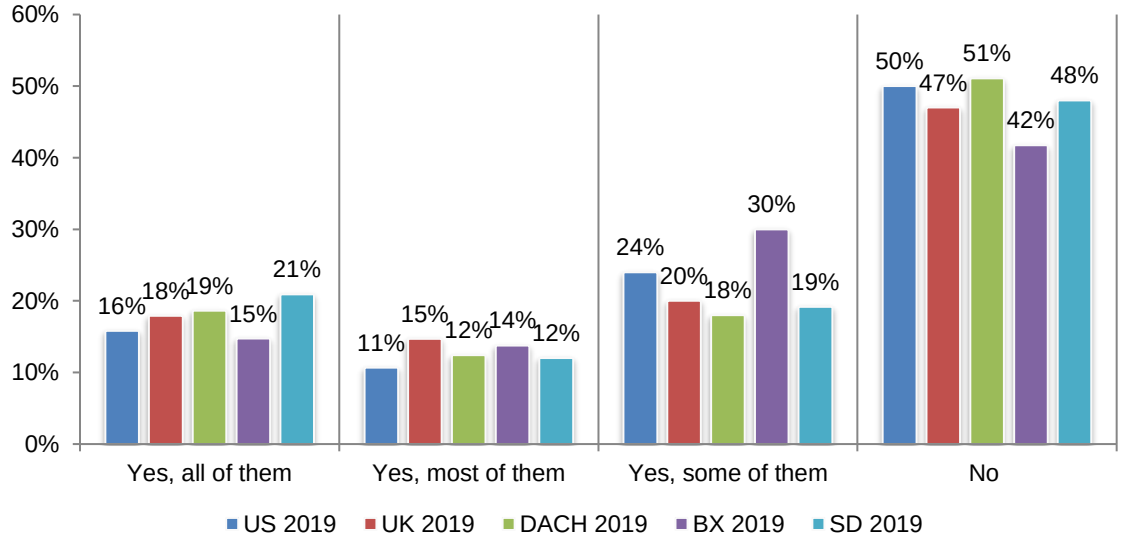
The majority of all SMBs recognizes that third-party risk is a serious threat to sensitive and confidential information. Respondents were asked to rate how confident they are that a third party would notify them if they had a data breach involving their sensitive and confidential information. Figure 29 presents the highly confident (7+) responses. Only 40 percent of respondents in DACH and BX were highly confident they would receive such notification.

Figure 29. How confident are you that your primary third party would notify your organization if it had a data breach involving your sensitive and confidential information?
On a scale of 1 = not confident to 10 = highly confident, 7+ responses combined



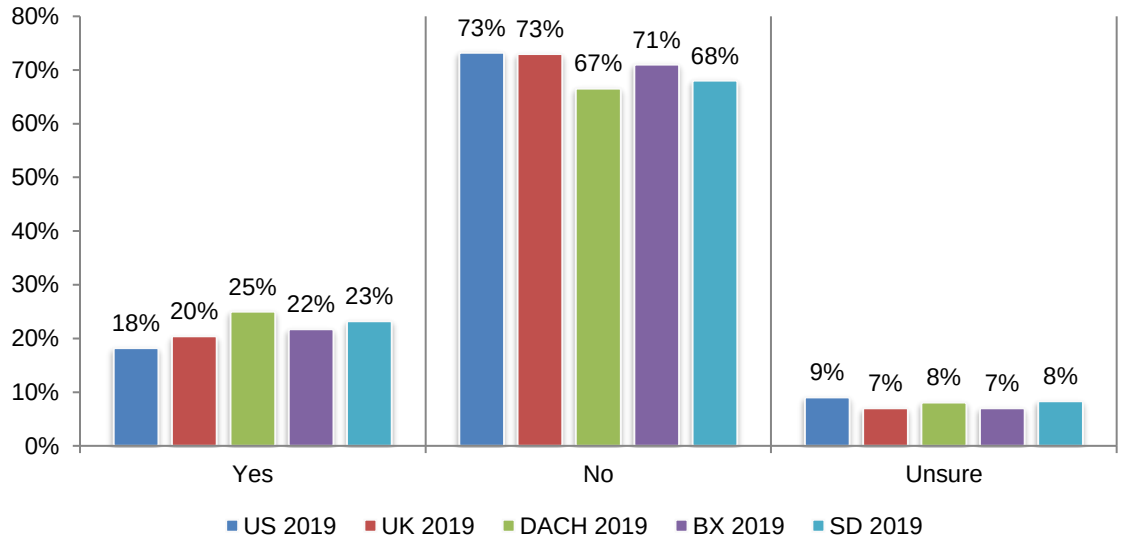
While SMBs in all countries and regions recognize that a security incident related to unsecured IoT devices or applications could be catastrophic to their organizations, most are not aware of the physical objects in their companies that are connected to the internet.

Figure 30. Are you aware of the network of physical objects in your company that are connected to the internet?



Furthermore, SMBs are not monitoring the risk of IoT devices used in the workplace.

Figure 31. Does your organization monitor the risk of IoT devices used in the workplace?



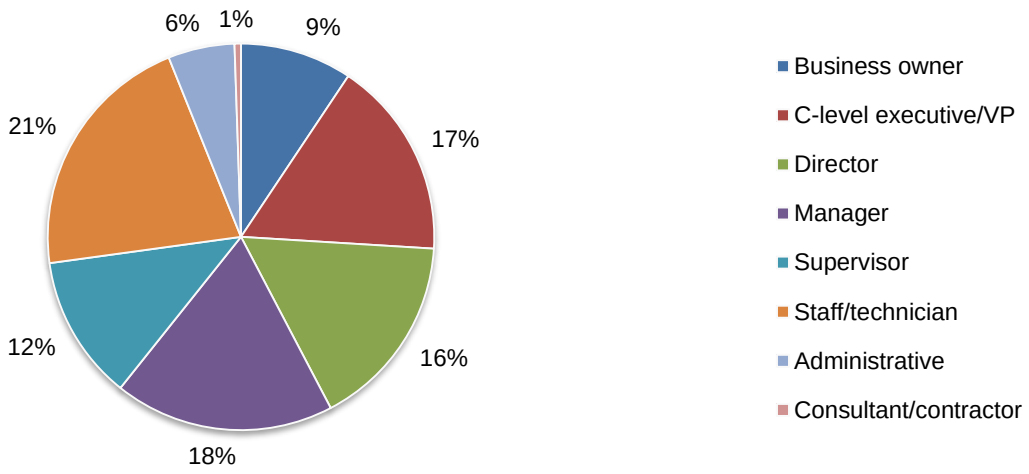
Part 3. Methods

A sampling frame of 60,223 individuals in companies in the United States, the United Kingdom and for the first time DACH (Germany, Austria, Switzerland), Benelux (Belgium, Netherlands, Luxemburg) and Scandinavia (Denmark, Norway and Sweden) were selected as participants in this survey. Table 1 shows 2,391 total returns. Screening and reliability checks required the removal of 215 surveys. Our final sample consisted of 2,176 surveys or a 3.6 percent response.

Table 1. Sample response	FY2019	FY2018	FY2017
Sampling frame	60,223	28,919	29,988
Total returns	2,391	1,149	1,152
Rejected or screened surveys	215	104	112
Final sample	2,176	1,045	1,040
Response rate	3.6%	3.6%	3.5%

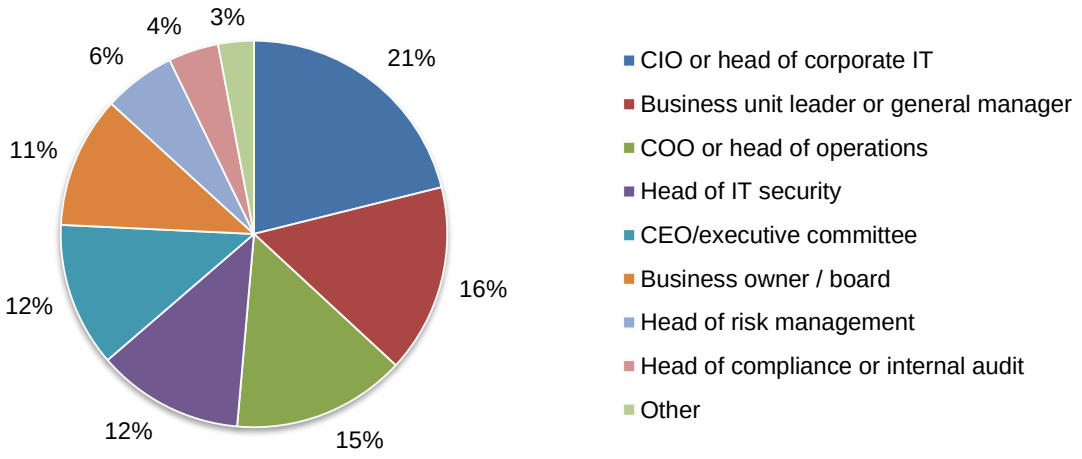
Pie Chart 1 reports the respondents' position within the participating organizations. More than half of the respondents (72 percent) are at or above the supervisory levels and 21 percent of respondents are at the staff/technician level.

Pie Chart 1. Current position within the organization



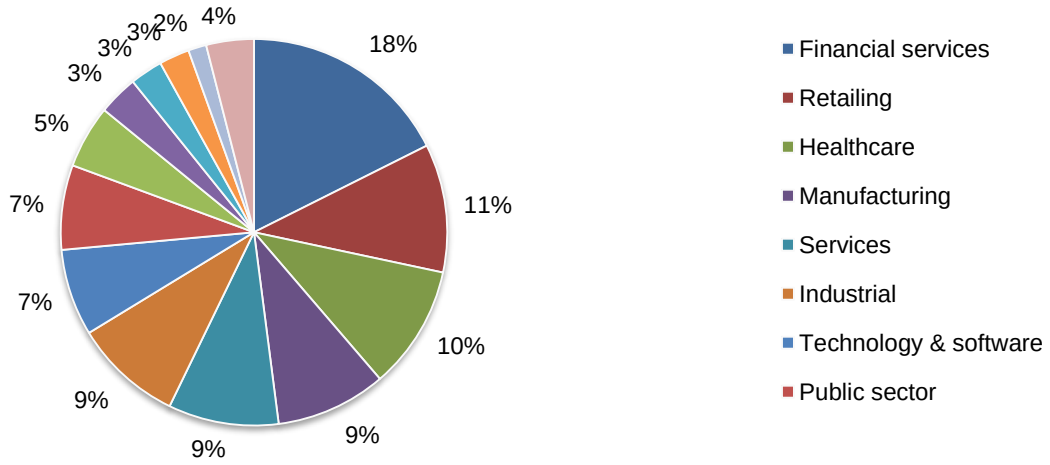
As shown in Pie Chart 2, 21 percent of respondents report directly to the CIO or head of corporate IT, 16 percent of respondents report to the business unit leader or general manager, 15 percent of respondents report to the COO or head of operations, 12 percent of respondents report to the head of IT security and 12 percent of respondents report to the CEO/executive committee.

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 (18 percent) as the largest segment, which includes banking, investment management, insurance, brokerage, payments and credit cards. This is followed by retailing (11 percent of respondents), healthcare (10 percent of respondents) and manufacturing, services, and industrial, each of which accounts for 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 in companies with a headcount from less than 100 to 1,000. 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 August 2019.

Survey response	FY 2019	FY2018	FY2017
Total sampling frame	60,223	28,919	29,988
Total returns	2,391	1,149	1,152
Rejected surveys	215	104	112
Final sample	2,176	1,045	1,040
Response rate	3.6%	3.6%	3.5%

Part 1. Screening Questions

S1. What range best describes the full-time employee headcount of your organization?	FY 2019	FY2018	FY2017
Less than 100	22%	15%	16%
100 to 250	22%	15%	17%
251 to 500	20%	22%	20%
501 to 750	25%	23%	24%
751 to 1,000	11%	24%	23%
More than 1,000 [STOP]	0%	0%	0%
Total	100%	100%	100%

S2. What best describes your role in managing the IT security function or activities within your organization? Check all that apply.	FY 2019	FY2018	FY2017
Setting IT security priorities	69%	66%	62%
Managing IT security budgets	54%	57%	57%
Selecting vendors and contractors	48%	46%	49%
Determining IT security strategy	40%	45%	46%
Evaluating program performance	49%	44%	44%
Administrating systems	45%		
None of the above [STOP]	0%	0%	0%
Total	305%	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 2019	FY2018	FY2017
Very high level of involvement	37%	33%	34%
High level of involvement	39%	43%	43%
Moderate level of involvement	19%	19%	19%
Low level of involvement	5%	5%	5%
Not involved [STOP]	0%	0%	0%
Total	100%	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 2019	FY2018	FY2017
1 or 2	11%	9%	11%
3 or 4	34%	34%	38%
5 or 6	25%	28%	30%
7 or 8	18%	17%	14%
9 or 10	12%	11%	7%
Total	100%	100%	100%
Extrapolated value	5.22	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 2019	FY2018	FY2017
Insufficient budget (money)	55%	55%	56%
Insufficient personnel	77%	74%	73%
Lack of in-house expertise	35%	37%	39%
Lack of clear leadership	6%	5%	5%
Insufficient enabling security technologies	36%	38%	43%
Not understanding how to protect against cyberattacks	45%	47%	47%
Management does not see cyberattacks as a significant risk	5%	4%	5%
Lack of collaboration with other functions	16%	17%	11%
Not a priority issue	23%	23%	22%
Other	1%	0%	0%
Total	300%	300%	300%

Q3. What types of information are you most concerned about protecting from cyberattackers? Please choose **two** top choices.	FY 2019	FY2018	FY2017
Customer credit or debit card information	42%	40%	37%
Financial information	31%	28%	26%
Intellectual property	50%	51%	48%
Customer records	57%	57%	63%
Employee records	13%	15%	16%
Business correspondence	7%	8%	8%
Other	0%	1%	1%
Total	200%	200%	200%

Q4. Who determines IT security priorities in your organization? Please select your top **two** choices.	FY2019	FY2018	FY2017
Business owners	22%	23%	24%
Board of directors	9%	9%	9%
Chief executive	32%	31%	34%
Head of operations	28%	30%	33%
Chief information officer (CIO)	31%	31%	33%
Chief technology officer (CTO)	8%	7%	8%
Chief information security officer (CISO)	13%	10%	11%
Compliance officer	4%	7%	6%
General counsel	5%	3%	4%
Lines of business	14%	14%	9%
No one function determines IT security priorities	34%	35%	30%
Other	1%	1%	0%
Total	200%	200%	200%

Q5. Is your organization's budget adequate for achieving a strong IT security posture?	FY2019	FY2018	FY2017
Yes	36%	37%	37%
No	54%	52%	52%
Unsure	11%	11%	11%
Total	100%	100%	100%

Q6. What percentage of your organization's IT budget is dedicated to IT security activities?	FY2019	FY2018	FY2017
Less than 5%	14%	16%	19%
5 to 10%	30%	31%	27%
11 to 15%	21%	23%	25%
16 to 20%	21%	18%	19%
21 to 25%	7%	6%	6%
26 to 30%	4%	3%	3%
31 to 40%	3%	3%	1%
41 to 50%	0%	0%	0%
More than 50%	0%	0%	0%
Total	100%	100%	100%
Extrapolated value	13.0%	12.1%	11.6%

Q7. Does your organization have the in-house expertise necessary for achieving a strong IT security posture?	FY2019	FY2018	FY2017
Yes	42%	41%	38%
No	42%	48%	52%
Unsure	16%	11%	10%
Total	100%	100%	100%

Q8. What percentage of your organization's IT personnel support IT security operations?	FY2019	FY2018	FY2017
Less than 5%	0%	0%	0%
5 to 10%	3%	4%	5%
11 to 15%	7%	7%	8%
16 to 20%	8%	10%	12%
21 to 25%	15%	14%	15%
26 to 30%	11%	10%	11%
31 to 40%	8%	8%	8%
41 to 50%	11%	11%	8%
More than 50%	37%	35%	33%
Total	100%	100%	100%
Extrapolated value	37%	36%	36%

Q9a. What percentage of your organization's IT security operations are supported by managed security service providers (MSSPs)?	FY2019	FY2018	FY2017
None [Skip Q10]	37%	41%	47%
Less than 10%	7%	9%	10%
10% to 25%	10%	8%	12%
26% to 50%	12%	11%	11%
51% to 75%	19%	18%	9%
76% to 100%	15%	14%	10%
Total	100%	100%	100%
Extrapolated value	32%	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.	FY2019	FY2018	FY2017
Monitored or managed firewalls or intrusion prevention systems (IPSs)	70%	66%	68%
Monitored or managed intrusion detection systems (IDSs)	38%	43%	50%
Monitored or managed multifunction firewalls	39%	30%	28%
Managed or monitored security gateways for messaging or web traffic	33%	39%	43%
Security analysis and reporting of events collected from IT infrastructure logs	22%	20%	20%
Reporting associated with monitored/managed devices and incident response	19%	17%	17%
Managed vulnerability scanning of networks, servers, databases or applications	39%	36%	40%
Distributed denial of service (DDoS) protection	14%	14%	13%
Monitoring or management of customer-deployed security information and event management (SIEM) technologies	10%	8%	8%
Monitoring and/or management of advanced threat defense technologies	10%	11%	10%
Identity and access management *	26%	22%	
Privileged access management *	17%	17%	
Other *	0%		
Total	337%	323%	298%

*not a response in 2016 & 2017

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.	FY2019	FY2018	FY2017
PCI DSS	43%	46%	43%
ISO 27001/2	5%	6%	6%
CCPA *	4%		
SOC 2/3	19%	17%	15%
COBIT	8%	9%	10%
SOX 404	11%	18%	17%
NIST	15%	17%	17%
GDPR *	69%		
NYDFS *	7%		
PIPEDA	5%		
HIPAA/HiTECH	6%	8%	10%
Other healthcare regulations and standards *	3%		
EMEA guidelines and standards *	10%		
None of the above *		31%	41%
Other	6%	6%	6%
Total	213%	158%	165%

*Response not available in all years

Q11. What percent of your organization's business-critical applications are accessed from mobile devices such as smart phones, tablets and others?	FY2019	FY2018
Zero	1%	0%
Less than 10%	5%	5%
11 to 25%	15%	17%
36 to 50%	32%	37%
51 to 75%	34%	30%
76 to 100%	14%	11%
Total	100%	100%
Extrapolated value	48%	45%

Q12. How many business-critical applications does your organization have?	FY2019
Less than 10	3%
10 to 25	10%
26 to 50	20%
51 to 100	28%
101 to 250	24%
More than 250	16%
Total	100%
Extrapolated value	120

Part 3: Cyberattacks

Q13a. Has your organization experienced a cyberattack in the past 12 months?	FY2019	FY2018	FY2017
Yes	66%	67%	61%
No	26%	22%	24%
Unsure	8%	11%	14%
Total	100%	100%	100%

Q13b. If yes, what best describes the type of attacks experienced by your organization in the past 12 months? Please select all that apply.	FY2019	FY2018	FY2017
Advanced malware / zero day attacks	26%	24%	16%
Phishing / social engineering	57%	52%	48%
Denial of services	28%	26%	26%
Account takeover *	19%		
Credential theft *	30%		
SQL injection	19%	20%	24%
Cross-site scripting	10%	9%	10%
Compromised / stolen devices	33%	34%	30%
Malicious insider	13%	12%	11%
General malware	36%	37%	36%
Web-based attack	47%	47%	43%
Other	4%	4%	3%
Total	322%	266%	248%

*Response not available in all years

Q14a. In the past 12 months, has your organization experienced situations when exploits and malware have evaded your intrusion detection system?	FY2019	FY2018	FY2017
Yes	69%	72%	66%
No	19%	20%	22%
Unsure	12%	8%	12%
Total	100%	100%	100%

Q14b. In the past 12 months, has your organization ever experienced situations when exploits and malware have evaded your anti-virus solutions?	FY2019	FY2018	FY2017
Yes	82%	82%	81%
No	14%	12%	13%
Unsure	4%	6%	5%
Total	100%	100%	100%

Q15. In the past 12 months, how has the time to **respond to** a cyberattack changed?	FY2019
Time has increased significantly	13%
Time has increased	26%
Time has remained unchanged	35%
Time has decreased	16%
Time has decreased significantly	10%
Total	100%

Please rate the following statements using the five-point scale provided below each item.			
Q16a. In the past 12 months, cyberattacks experienced by my organization are becoming more **targeted**.	**FY2019**	**FY2018**	**FY2017**
Strongly agree	33%	28%	27%
Agree	36%	34%	33%
Unsure	15%	16%	19%
Disagree	11%	13%	13%
Strongly disagree	5%	9%	9%
Total	100%	100%	100%

Q16b. In the past 12 months, cyberattacks experienced by my organization are becoming more **sophisticated**.	**FY2019**	**FY2018**	**FY2017**
Strongly agree	26%	23%	26%
Agree	34%	36%	33%
Unsure	24%	21%	21%
Disagree	11%	13%	12%
Strongly disagree	6%	8%	8%
Total	100%	100%	100%

Q16c. In the past 12 months, cyberattacks experienced by my organization are becoming more **severe** in terms of negative consequences (such as financial impact).	**FY2019**	**FY2018**	**FY2017**
Strongly agree	28%	26%	27%
Agree	33%	34%	32%
Unsure	23%	22%	24%
Disagree	12%	12%	12%
Strongly disagree	4%	5%	5%
Total	100%	100%	100%

Q17a. Has your organization **ever** experienced a cyberattack?	**FY2019**
Yes	72%
No	20%
Unsure	8%
Total	100%

Q17b. If yes, what best describes the type of attacks experienced by your organization? Please select all that apply.	FY2019
Advanced malware / zero day attacks	29%
Phishing / social engineering	53%
Denial of services	29%
Account takeover	19%
Credential theft	29%
SQL injection	21%
Cross-site scripting	12%
Compromised / stolen devices	37%
Malicious insider	16%
General malware	39%
Web-based attack	50%
Other	3%
Total	337%

Q18. 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?	FY2019	FY2018	FY2017
Improves security posture	7%	6%	6%
Diminishes security posture	49%	49%	48%
No effect on security posture	33%	33%	35%
Cannot determine	10%	12%	11%
Total	100%	100%	100%

Q19. In your opinion, what are the most vulnerable endpoints or entry points to your organization's networks and enterprise systems? Please select all that apply.	FY2019	FY2018	FY2017
Desktops	18%	19%	21%
Laptops	56%	49%	43%
Tablets	19%	19%	20%
Smartphones	41%	40%	39%
Web server	33%	33%	30%
Intranet server	34%	42%	36%
Routers	6%	6%	6%
Portable storage devices (including USBs)	7%	7%	8%
Cloud systems	45%	42%	38%
Mobile devices	56%	55%	56%
Other	0%	1%	2%
IoT devices	45%	41%	
Total	359%	356%	300%

Part 4. Data breach experience

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?	FY2019	FY2018	FY2017
Yes	63%	58%	54%
No	37%	42%	46%
Total	100%	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?	FY2019	FY2018	FY2017
Less than 100	28%	33%	33%
100 to 500	26%	23%	26%
501 to 1,000	15%	15%	15%
1,001 to 10,000	18%	14%	14%
10,001 to 50,000	7%	8%	7%
50,001 to 100,000	5%	6%	4%
100,001 to 1,000,000	0%	1%	1%
More than 1,000,000	0%	0%	0%
Total	100%	100%	100%
Extrapolated value	8,719	10,848	9,350

Q20c. If yes, what were the root causes of the data breaches experienced by your organization in the past 12 months? Please select that apply.	FY2019	FY2018	FY2017
Malicious insider	8%	7%	7%
External (hacker) attacks	42%	37%	33%
Negligent employee or contractor	63%	60%	54%
Error in system or operating process	32%	30%	34%
Third party mistakes	55%	43%	43%
Other	1%	1%	2%
Don't know	32%	31%	32%
Total	233%	209%	206%

Q21. Does your organization have an incident response plan for responding to cyberattacks and data breaches?	FY2019	FY2018	FY2017
Yes	60%	60%	55%
No	39%	39%	44%
Unsure	1%	1%	1%
Total	100%	100%	100%

Part 5. Password practices and policies

Q22. The use of strong passwords is an essential part of my organization's security defense.	FY2019
Strongly agree	29%
Agree	35%
Unsure	23%
Disagree	11%
Strongly disagree	2%
Total	100%

Q23a. Does your organization have visibility into employees' password practices?	FY2019	FY2018	FY2017
Yes	42%	45%	41%
No [Please skip to Q24]	54%	50%	52%
Unsure [Please skip to Q24]	4%	4%	7%
Total	100%	100%	100%

Q23b. If yes, are you able to determine the following steps taken by employees? Please select all that apply.	FY2019	FY2018
Using unique or strong passwords	48%	46%
Making periodic changes to passwords	48%	47%
Sharing passwords with others	25%	24%
The number of passwords each employee has	43%	46%
Total	165%	163%

Q24. Does your organization have a policy pertaining to employees' use of passwords?	FY2019	FY2018	FY2017
Yes	45%	47%	43%
No [Please skip to Q26]	50%	49%	52%
Unsure [Please skip to Q26]	5%	5%	5%
Total	100%	100%	100%

Q25a. Does your organization strictly enforce this policy and require employees to use a password manager?	FY2019	FY2018	FY2017
Yes	32%	32%	32%
No	65%	64%	63%
Unsure	3%	4%	5%
Total	100%	100%	100%

Q25b. If yes, what brand of password manager does your company use?	FY2019
LastPass	12%
Dashlane	10%
OneLogin	15%
Keeper	13%
Sticky Password	9%
1Password	11%
True Key	13%
Other	18%
Total	100%

Q26. What are your **two** biggest pain points about employees and their passwords? Please select your top **two** choices.	FY2019	FY2018
Time spent resetting passwords	60%	58%
Changing passwords when an employee leaves his job	46%	46%
Employees using weak passwords	68%	67%
Employee passwords being stolen or compromised	68%	68%
Employee adoption of best practices	36%	38%
Total	277%	277%

Q27. Does your organization take any of the following steps? Please select all that apply.	FY2019	FY2018
Periodic password changes	41%	44%
Assign randomly chosen passwords	28%	30%
Require minimum password lengths	29%	32%
Prohibit employees from reusing the same password on internal systems	38%	34%
Provide an alternative to keyboard entry (i.e. voice recognition, biometrics)	46%	46%
Require more than one authentication system such as 2FA	47%	40%
Monitor third-party sites where compromised passwords are shared	37%	40%
Require use of authentication apps *	43%	
Require use of a UBA key *	32%	
Other	5%	1%
None of the above *		22%
Total	347%	289%

*Response not available in all years

Q28a. Does your organization use biometrics to identify and authenticate?	FY2019
Yes, we currently use [Please skip to Q29a]	45%
We plan to implement in the near future [Please skip to Q29a]	30%
No, we do not use	24%
Total	100%

Q28b. If no, why does your organization not use biometrics to identify and authenticate?	FY2019	FY2018
Too costly	46%	43%
Difficult to enforce	51%	48%
Too risky if biometric information was lost	39%	43%
Still need passwords as backup	41%	39%
Total	177%	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.			
Q29a. Does your organization use SSO?	**FY2019**	**FY2018**	**FY2017**
Yes, fully implemented across the enterprise	34%	31%	27%
Yes, partially implemented across the enterprise	30%	27%	24%
No (skip to Q30)	36%	42%	50%
Total	100%	100%	100%

Q29b. If yes, what do you believe are the benefits of SSO?	**FY2019**
Increases convenience in user's access to your organization's applications and data	42%
Increases the security of user access to your organization's applications and data	31%
Increases both the convenience and security of user access to your organization's applications and data	24%
Unsure	3%
Total	100%

Part 6. Third-party risk vulnerabilities

Q30. Our organization considers third-party risk a serious threat to sensitive and confidential information.	**FY2019**
Strongly agree	27%
Agree	30%
Unsure	26%
Disagree	13%
Strongly disagree	5%
Total	100%

Q31. How confident are you that your primary third party would notify you if it had a data breach involving your company's sensitive and confidential information? (1 = not confident to 10 = highly confident)	**FY2019**
1 or 2	12%
3 or 4	17%
5 or 6	30%
7 or 8	25%
9 or 10	17%
Total	100%
Extrapolated value	5.86

Q32a Does your company have a comprehensive inventory of all third parties with whom it shares sensitive and confidential information?	FY2019
Yes [Please skip to Q33]	25%
No	70%
Unsure	5%
Total	100%

Q32b. If no or unsure, why? Please check all that apply	FY2019
Lack of resources to track third parties	52%
No centralized control over third-party relationships	33%
Complexity in third-party relationships	28%
Cannot keep track due to frequent turnover in third parties	41%
Not a priority	39%
Total	192%

Part 7. IoT risks in the workplace

Q33. Does your organization inform and educate employees and third parties about the risks created by IoT devices in the workplace and what steps they need to take to minimize the risk?	FY2019
Yes, we currently provide such information and education	24%
No, but we are planning to provide such information and education	27%
No	49%
Total	100%

Q34. Are you aware of the network of physical objects in your company that are connected to the internet (i.e. printers or building automation solutions)?	FY2019
Yes, all of them	17%
Yes, most of them	13%
Yes, some of them	22%
No	48%
Total	100%

Q35. What is the likelihood a security incident related to unsecured IoT devices or applications could be catastrophic to your organization?	FY2019
Very likely	31%
Somewhat likely	31%
Likely	18%
Not likely	11%
Not possible	9%
Total	100%

Q36. Does your organization monitor the risk of IoT devices used in the workplace?	FY2019
Yes	21%
No	71%
Unsure	8%
Total	100%

Part 8. The cost of compromises

Q37a. Approximately, how much did damage or theft of IT assets and infrastructure cost your organization over the past 12 months?	FY2019	FY2018	FY2017
We had no compromises	29%	32%	34%
Less than $5,000	8%	8%	8%
$5,001 to $10,000	4%	2%	2%
$10,001 to $50,000	6%	5%	6%
$50,001 to $100,000	5%	5%	6%
$100,001 to $250,000	8%	7%	8%
$250,001 to $500,000	10%	9%	8%
$500,001 to $999,999	8%	8%	9%
$1 million to $5 million	13%	11%	10%
$5 million to $10 million	8%	11%	6%
More than $10 million	1%	2%	1%
Total	100%	100%	99%
Extrapolated value (US$)	$1,242,678	$1,426,422	$ 1,027,053

**UK amount was converted from GBP to dollars*

Q37b. Approximately, how much did disruption to normal operations cost your organization over the past 12 months?	FY2019	FY2018	FY2017
Less than $5,000	9%	8%	8%
$5,001 to $10,000	3%	2%	2%
$10,001 to $50,000	6%	6%	6%
$50,001 to $100,000	4%	4%	4%
$100,001 to $250,000	6%	7%	10%
$250,001 to $500,000	6%	9%	9%
$500,001 to $999,999	8%	8%	9%
$1 million to $5 million	11%	10%	9%
$5 million to $10 million	8%	7%	6%
More than $10 million	7%	5%	3%
We had no compromises	33%	32%	33%
Total	100%	100%	100%
Extrapolated value (US$)	$1,896,996	$ 1,562,124	$1,207,965

Q38a. Have you had an attack involving the compromise of employees' passwords in the past year?	FY2019	FY2018
Yes	47%	40%
No	47%	52%
Unsure	6%	8%
Total	100%	100%

Q38b. If yes, on average how much did each attack cost your organization?	FY2019	FY2018
Less than $10,000	3%	3%
$10,001 to $50,000	9%	7%
$50,001 to $100,000	10%	14%
$100,001 to $250,000	30%	29%
$250,001 to $500,000	21%	22%
$500,001 to $1,000,000	17%	13%
More than $1,000,000	10%	12%
Total	100%	100%
Extrapolated value (US$)	$ 384,598	$ 383,365

Part 9. General Data Protection Regulation (GDPR)		
Q39. Is your organization required to comply with GDPR?	FY2019	FY2018
Yes	83%	72%
No [Skip to Part 10]	13%	19%
Unsure	5%	9%
Total	100%	100%

Q40. If yes, did compliance require significant changes in your privacy and security strategies?	FY2019	FY2018	FY2017
Yes, significant change	47%	41%	37%
Yes, some change	38%	41%	37%
Yes, nominal change	10%	11%	18%
No change	5%	7%	8%
Total	100%	100%	100%

Q41. Using the following 10-point scale, please rate your organization's level of compliance with the GDPR. 1 = not ready and 10 = ready.	FY2019	FY2018
1 or 2	11%	18%
3 or 4	28%	23%
5 or 6	21%	20%
7 or 8	18%	21%
9 or 10	22%	19%
Total	100%	100%
Extrapolated value	5.76	5.48

Part 10. Role & Organizational Characteristics

D1. What best describes your position level within the organization?	FY2019	FY2018	FY2017
Business owner	9%	10%	10%
C-level executive/VP	17%	12%	11%
Director	16%	17%	17%
Manager	18%	20%	21%
Supervisor	12%	13%	12%
Staff/technician	21%	23%	24%
Administrative	6%	5%	4%
Consultant/contractor	1%	1%	1%
Other	0%		
Total	100%	100%	100%

D2. Which of the following commands do you report to in your current role?	FY2019	FY2018	FY2017
Business owner / board	11%	12%	12%
CEO/executive committee	12%	10%	9%
COO or head of operations	15%	16%	16%
CFO, controller or head of finance	2%	3%	3%
CIO or head of corporate IT	21%	23%	27%
Business unit leader or general manager	16%	15%	13%
Head of compliance or internal audit	4%	4%	4%
Head of risk management	6%	5%	5%
Head of IT security	12%	11%	11%
Other	1%		
Total	100%	100%	100%

D3. What best describes your organization's primary industry classification?	FY2019	FY2018	FY2017
Aerospace & defense	1%	1%	1%
Agriculture & food services	1%	1%	2%
Communications	3%	2%	2%
Construction and real estate	3%	3%	3%
Consumer goods	5%	6%	6%
Education & research	2%	2%	2%
Entertainment, media and publishing	1%	1%	3%
Financial services	18%	16%	14%
Healthcare	10%	7%	7%
Industrial	9%	9%	9%
Logistics and distribution	0%	1%	1%
Manufacturing	9%	8%	8%
Pharmaceuticals	3%	2%	3%
Public sector	7%	9%	9%
Retailing	11%	12%	12%
Services	9%	10%	9%
Technology & software	7%	8%	7%
Transportation	1%	3%	2%
Other	0%		
Total	100%	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 companies.

As a member of the **Council of American Survey Research Companies (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.