2016 State of Cybersecurity in Small & Medium-Sized Businesses (SMB)

Sponsored by Keeper Security

Independently conducted by Ponemon Institute LLC

Publication Date: June 2016

2016 State of Cybersecurity in Small and Medium-Sized Businesses (SMB)

Ponemon Institute, June 2016

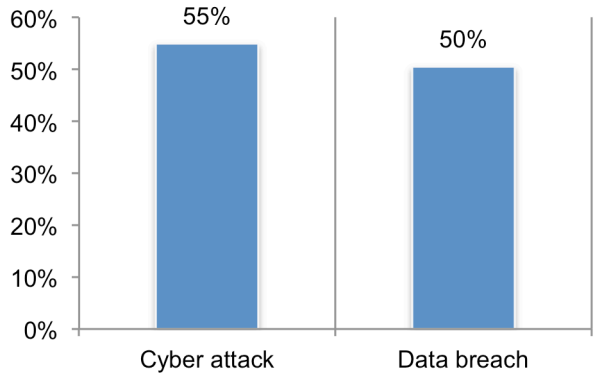
Part 1. Introduction

No business is too small to evade a cyber attack or data breach. Unfortunately, smaller organizations may not have the budget and in-house expertise to harden their systems and networks against potential threats. In fact, only 14 percent of the companies represented in this study rate their ability to mitigate cyber risks, vulnerabilities and attacks as highly effective. Moreover, the introduction of cloud applications and infrastructure and more mobile devices is creating more security risks that will stretch these companies' resources.

Ponemon Institute is pleased to present the results of the *2016 State of Cybersecurity in Small and Medium-Sized Business* sponsored by Keeper Security. We surveyed 598 individuals in companies with a headcount from less than 100 to 1,000.

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

Yes responses



As shown in Figure 1, 55 percent of these respondents say their companies have experienced a cyber attack in the past 12 months, and 50 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 $879,582 because of damage or theft of IT assets. In addition, disruption to normal operations cost an average of $955,429.

The following 10 findings reveal the state of cybersecurity in smaller businesses.

1. The most prevalent attacks against smaller businesses are Web-based and phishing/social engineering.

2. Negligent employees or contractors and third parties caused most data breaches. However, almost one-third of companies in this research could not determine the root cause.

3. Companies are most concerned about the loss or theft of their customers' information and their intellectual property.

4. Strong passwords and biometrics are believed 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.

5. Password policies are not strictly enforced. If a company has a password policy, 65 percent of respondents say they do not strictly enforce it. Moreover, the policy does not require employees to use a password or biometric to secure access to mobile devices.

6. Current technologies cannot detect and block many cyber attacks. Most exploits have evaded intrusion detection systems and anti-virus solutions.

7. Personnel, budget and technologies are insufficient to have a strong security posture. As a result, some companies engage managed security service providers to support an average of 34 percent of their IT security operations.

8. Determination of IT security priorities is not centralized. The two functions most responsible are chief executive and chief information office. However, 35 percent of respondents say no one function in their company determines IT security priorities.

9. Web and intranet servers are considered the most vulnerable endpoints or entry points to networks and enterprise systems. The challenge of not having adequate resources may prevent many companies from investing in the technologies to mitigate these risks. Web application firewalls, SIEM, endpoint management, network traffic intelligence are not considered very important in current security strategy. At a minimum anti-malware and client firewalls are considered the most important security technologies.

10. Cloud usage and mobile devices that access business-critical applications and IT infrastructure will increase and threaten the security posture of companies in this study. However, only 18 percent of respondents say their company uses cloud-based IT security services and most password policies do not require employees to use a password or biometric to secure access to their mobile devices.

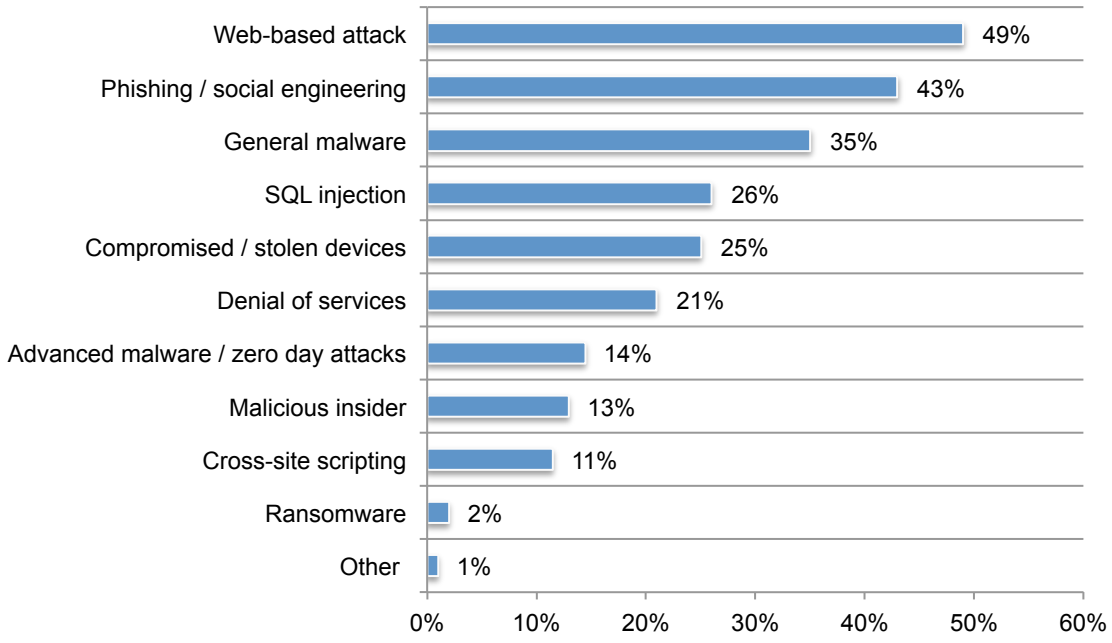
Part 2. Key findings

- The state of SMB cyber threats
- IT security posture and governance
- Technologies in place to address the threat
- The impact of the Cloud and mobile on IT security posture

The SMB cyber threat

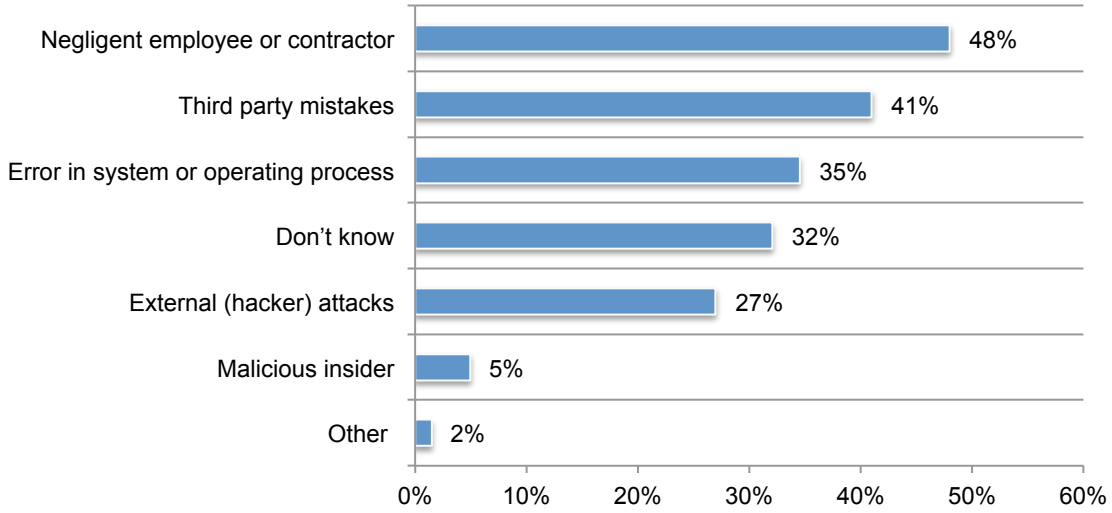
Cyber attacks and data breaches target SMBs. As discussed, the majority of businesses represented in this study experienced a cyber attack and data breach with severe financial consequences. Web-based attacks (49 percent of respondents) or phishing/social engineering (43 percent of respondents) were the most common type of cyber attacks, as shown in Figure 2.

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



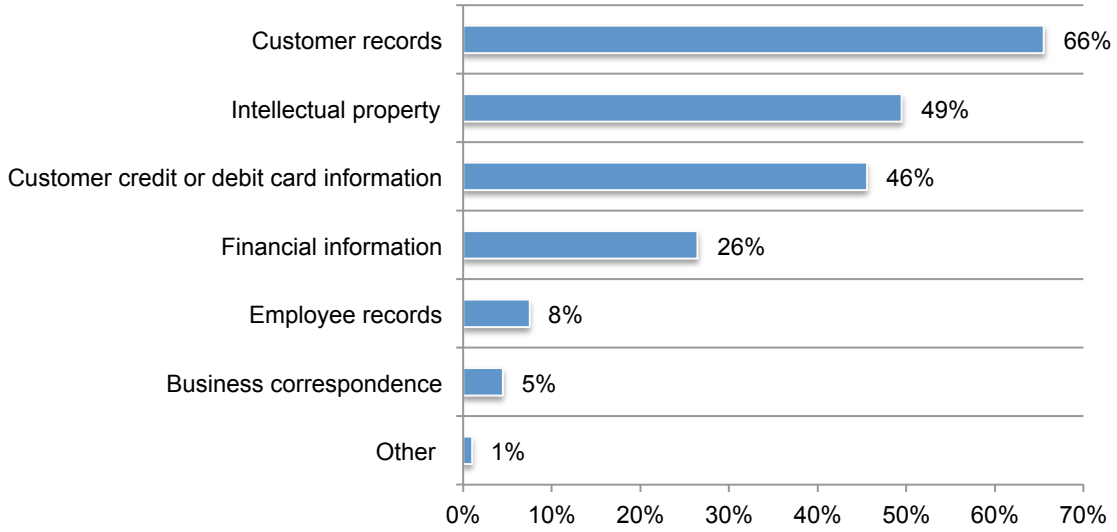
Many businesses cannot determine the root cause of a data breach. Companies represented in this research lost an average of more than 5,000 individual records as a result of the data breach. As shown in Figure 3, negligent employees or contractors (48 percent of respondents) and third party mistakes (41 percent of respondents) were the most common causes of these incidents. However, almost one-third of respondents say their companies could not determine what caused the incident.

Figure 3. What were the root causes of the data breaches your business experienced?
More than one choice permitted



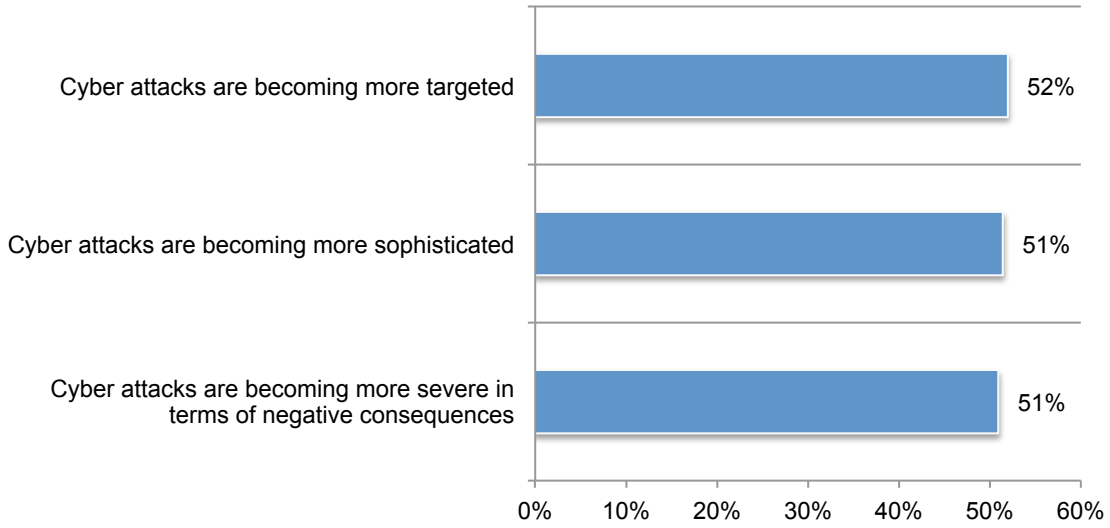
B**usinesses are most concerned about customer records and intellectual property.** When asked what information cyber attackers are most likely to target, 66 percent of respondents say customer records are their biggest concern. Possibly because this is the information smaller companies most often use. Almost half of respondents (49 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 permitted



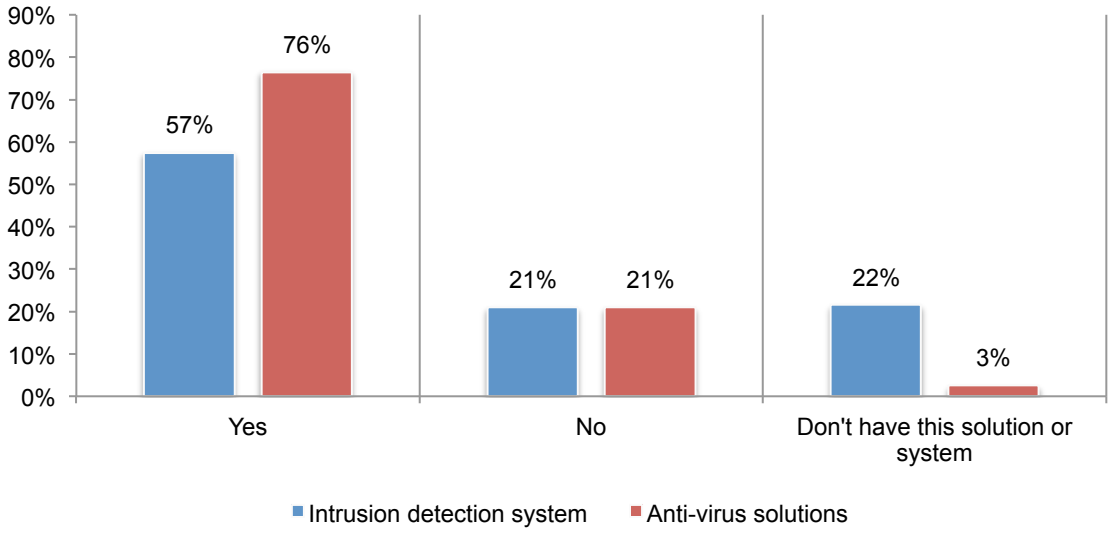
Cyber attacks are more targeted, sophisticated and severe. According to Figure 5, the majority of respondents are concerned that the cyber attacks against their companies are becoming more targeted, sophisticated and severe.

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



Businesses are vulnerable to exploits and malware. Only 33 percent of respondents say the technologies currently used by their organization can detect and block most cyber attacks. According to Figure 6, 57 percent of respondents say exploits and malware evaded intrusion detection systems and 76 percent of respondents say they have evaded their anti-virus solutions.

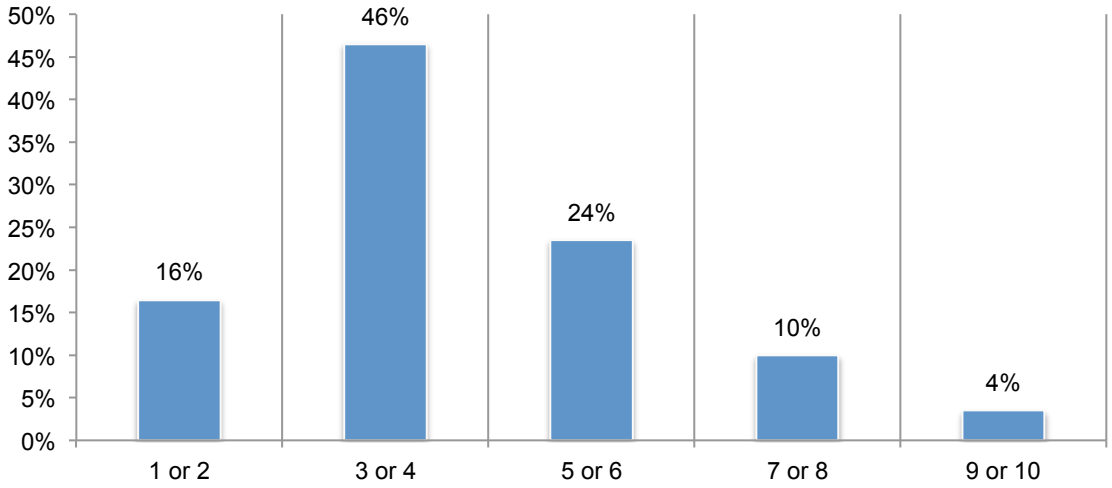
Figure 6. Has your business experienced situations when exploits and malware have evaded their intrusion detection system or anti-virus solutions?



Cybersecurity posture and governance

Businesses are not prepared to mitigate cyber risks, vulnerabilities and attacks. We asked respondents to rate the effectiveness of their IT security posture from 1 (not effective) to 10 (highly effective). As shown in Figure 7**,** only 14 percent of respondents rate their organizations effectiveness in their IT security posture at mitigating risks, vulnerabilities and attacks against their businesses above 6.

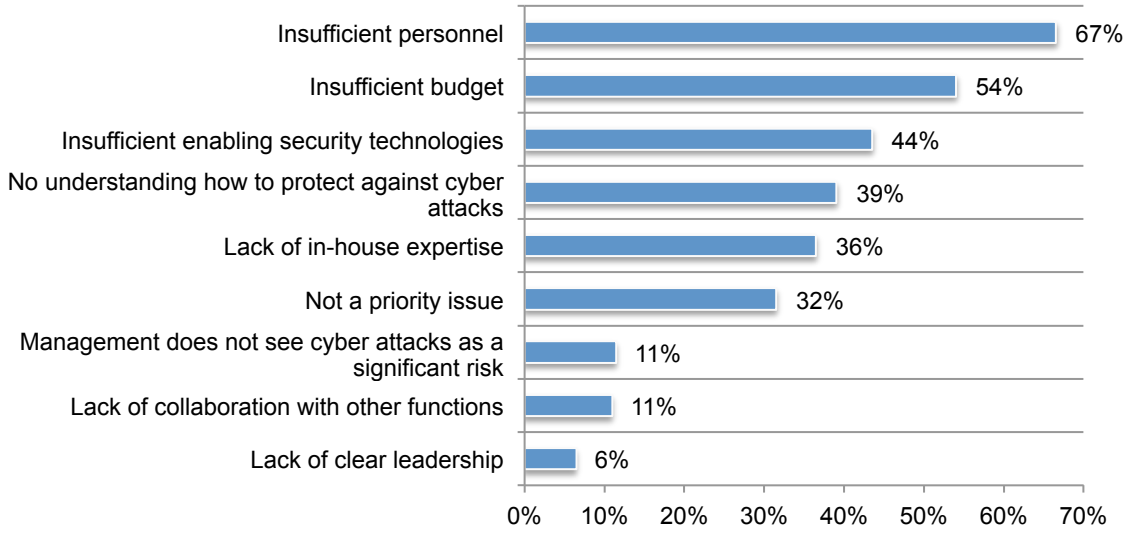
Figure 7. How effective is your company in mitigating risks, vulnerabilities and attacks across the enterprise? 1 = not effective; 10 = very effective



Personnel, budget and technologies are insufficient to have a strong security posture. 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 (67 percent of respondents). Insufficient budget (54 percent of respondents) and insufficient enabling security technologies (44 percent of respondents) are also barriers to a stronger cybersecurity posture. Collaboration with other functions and management's lack of recognition of cyber attacks as a significant risk are not major challenges.

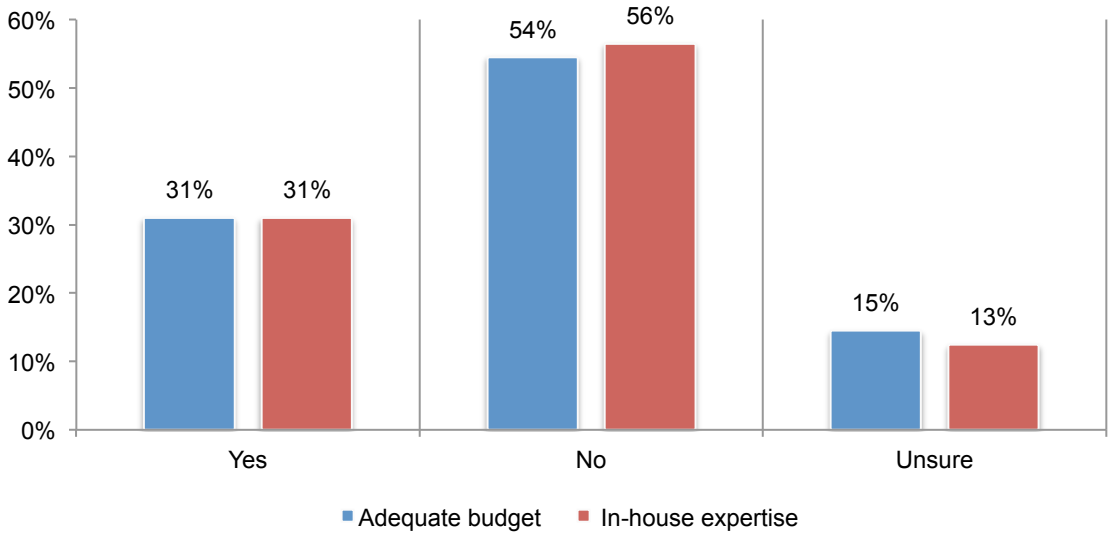
Figure 8. What challenges keep your IT security posture from being fully effective?



Sixty-nine percent of respondents say their organizations do not have the budget (54 percent + 15 percent) and another 69 percent of respondents (56 percent + 13 percent) say they do not have the have in-house expertise adequate for achieving a strong cybersecurity posture.

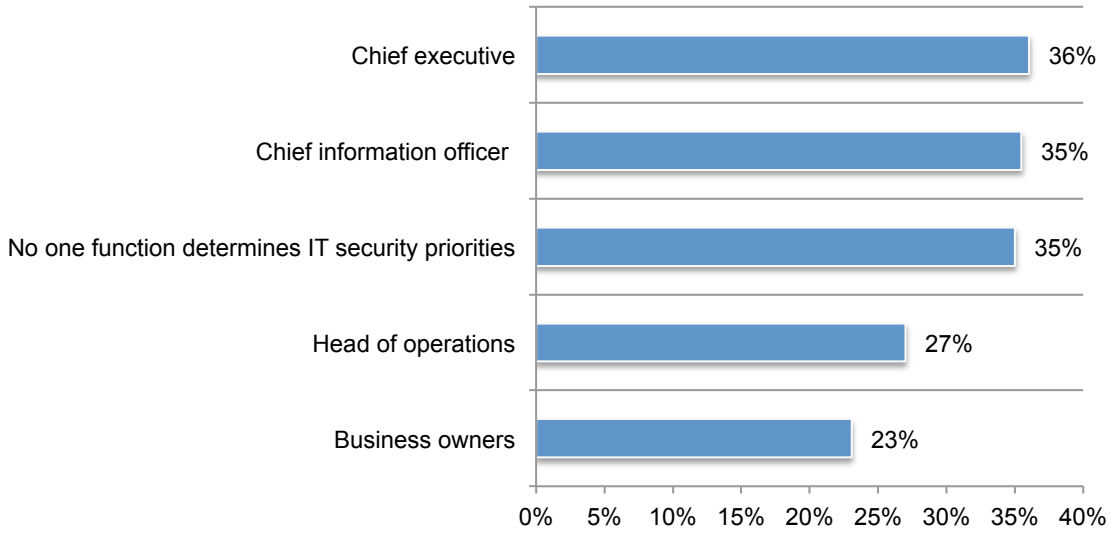
The company's IT personnel must deal with both IT and security challenges. On average, 54 percent of the company's IT personnel support IT security operations.

Figure 9. Does your organization have an adequate budget and in-house expertise to achieve a strong cybersecurity posture?



Determination of IT security priorities is not centralized. As shown in Figure 10, 36 percent of respondents say the chief executive is responsible. However, 35 percent of respondents say it is either the chief information officer (CIO) or no one function determines IT security priorities.

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

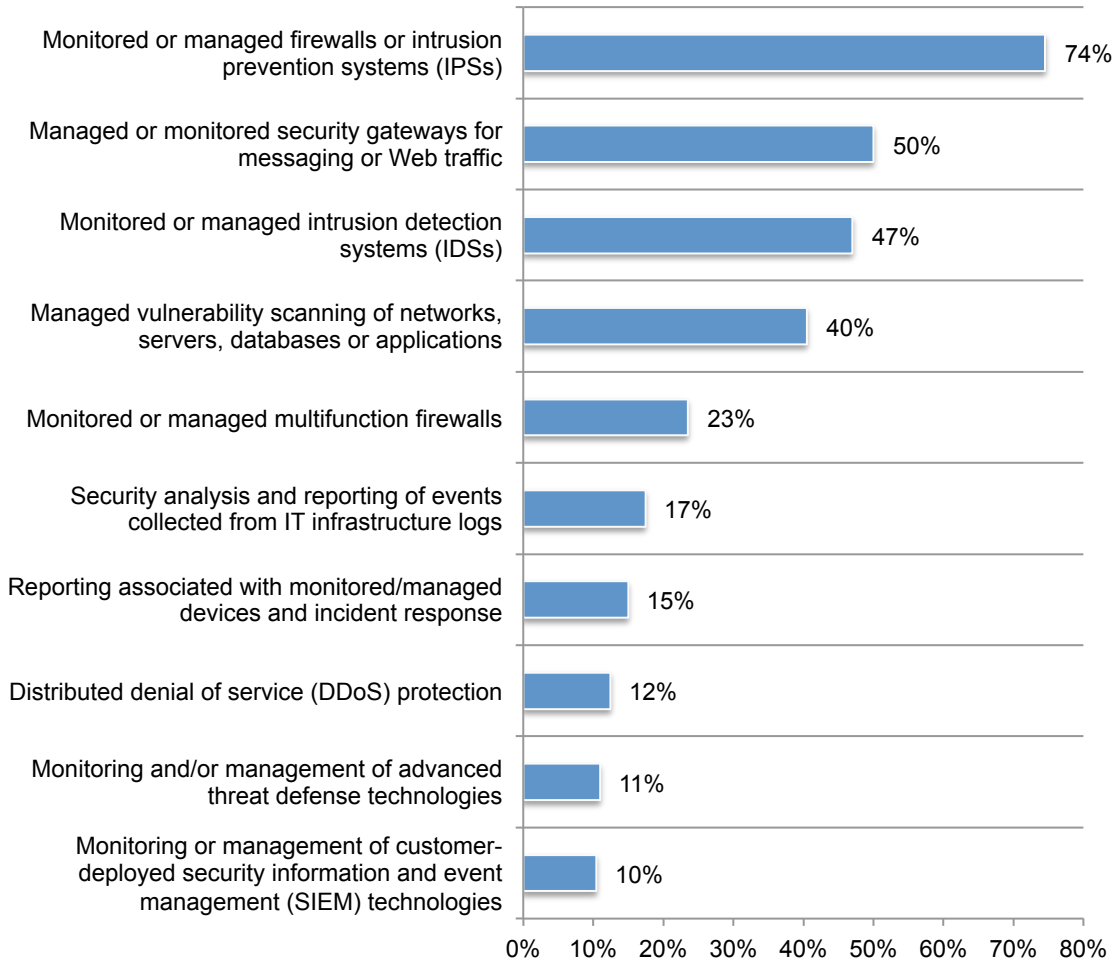


Managed security services providers (MSSPs) are engaged to support the IT security function. On average, 34 percent of a company's IT security operations are supported by MSSPs.

According to Figure 11, 74 percent of respondents say their MSSP monitors or manages firewalls or intrusion prevention systems or security gateways for messaging or Web traffic (50 percent of respondents). Forty-seven percent of respondents say their MSSP monitors or manages intrusion detection systems.

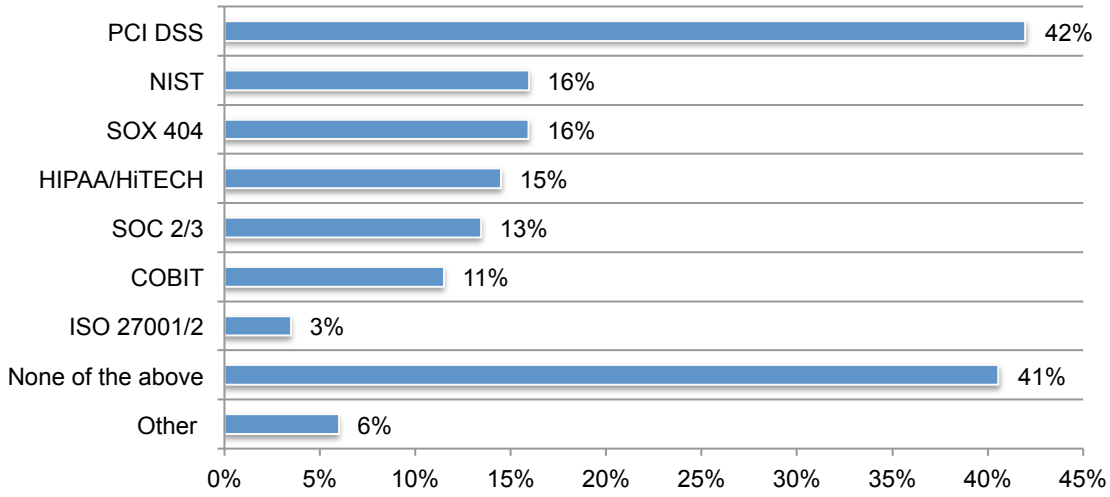
A much smaller percentage of services are used to stop advanced threats. Only 11 percent of respondents say their MSSP provides monitoring and/or management of advanced threat defense technologies and 10 percent of respondents say it provides monitoring or management of customer-deployed security information and event management (SIEM) technologies.

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



Companies mostly comply with PCI DSS. Figure 12 presents the leading IT security guidelines and standards. Forty-two percent of respondents say they comply with PCI DSS, but 41 percent say they do not comply with any of the standards.

Figure 12. Which IT security guidelines or standards does your company comply with?
More than one choice permitted

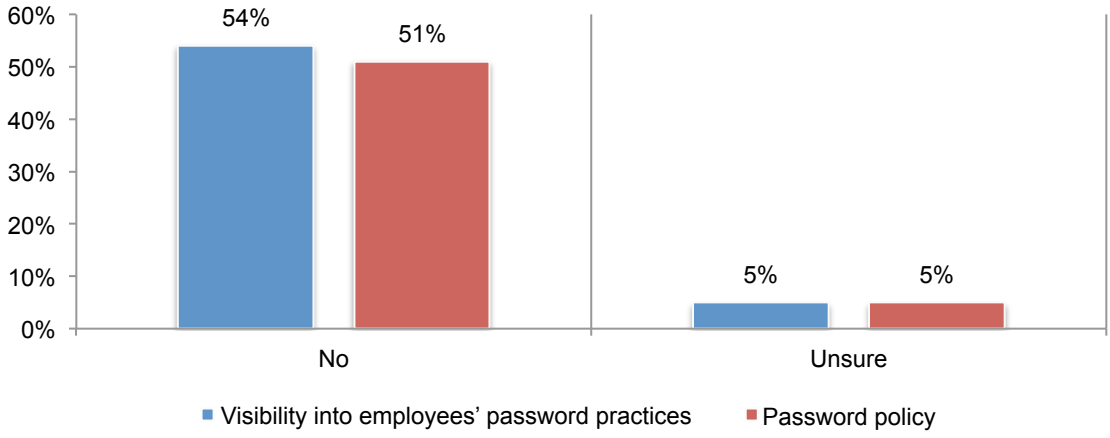


Technologies in place to address the threat

Strong passwords and biometrics are an essential part of the security defense. Sixty percent of respondents say they rely upon strong passwords and/or biometrics to reduce the risk of attack. Moreover, 76 percent of respondents believe passwords or biometric authentication for securing endpoints and/or entry points to their organizations' networks and enterprise systems are essential or very important.

However, as shown in Figure 13, 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-six 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.

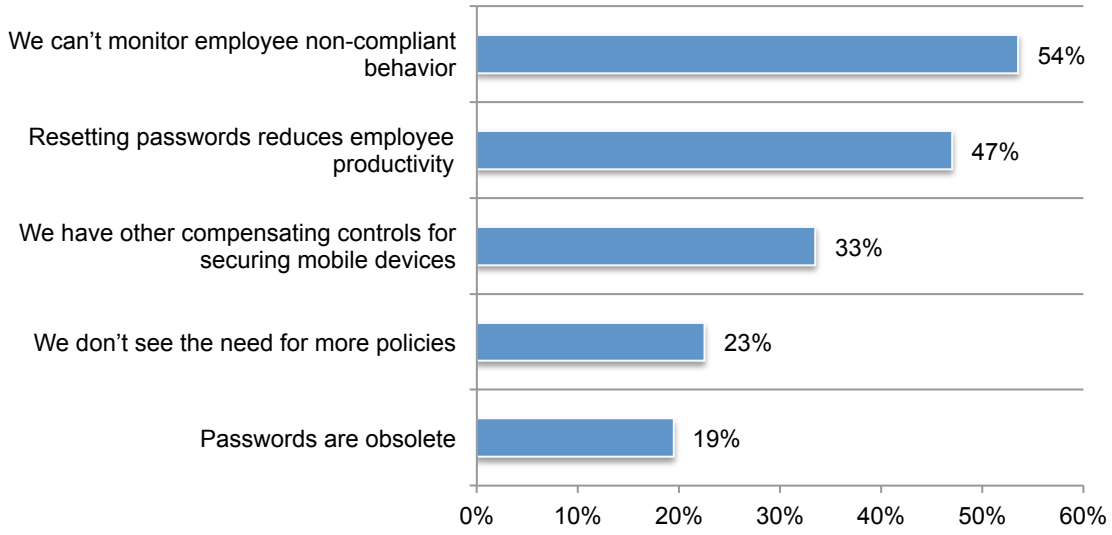
Figure 13. Does your organization have visibility into employees' password practices and a password policy?
No and Unsure responses



Password policies are not strictly enforced. If their company has a password policy, 65 percent of respondents say they do not strictly enforce it. Moreover, it does not require employees to use a password or biometric to secure access to mobile devices.

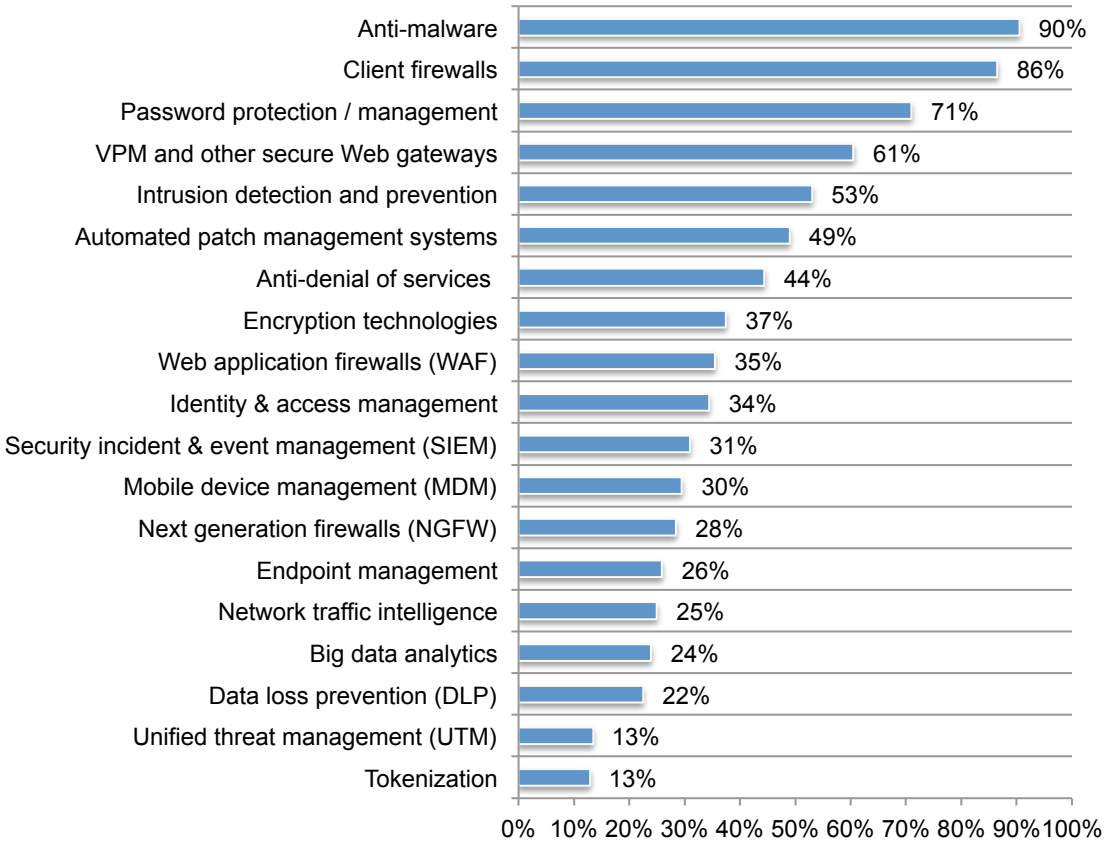
As shown in Figure 14, if companies do not require passwords or biometric protections on mobile devices, the primary reasons are inability to monitor employee non-compliant behavior (54 percent of respondents), resetting passwords reduces employee productivity (47 percent of respondents) or there are other compensating controls for securing mobile devices (33 percent of respondents).

Figure 14. Why doesn't your organization require password or biometric protections on mobile devices?
More than one choice permitted



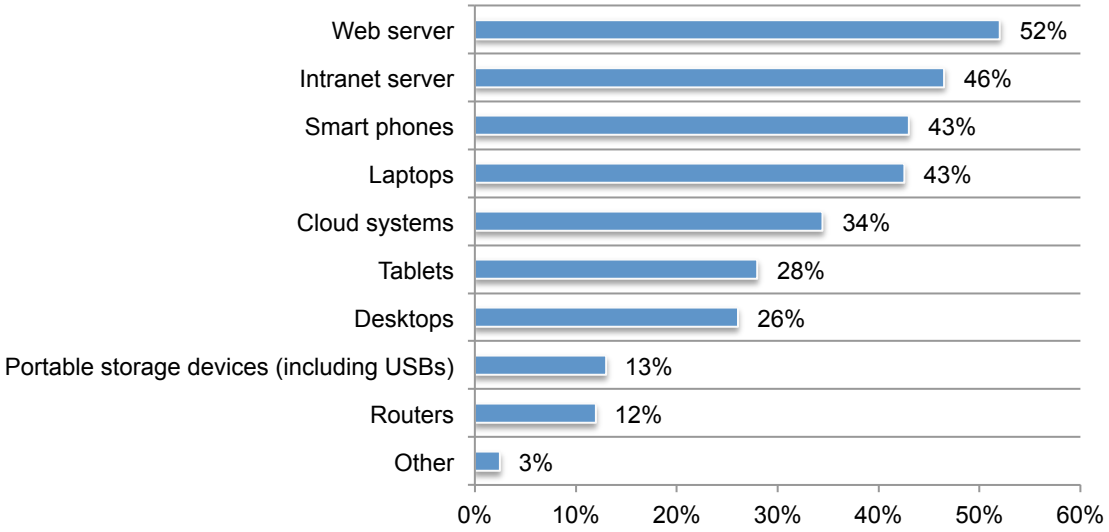
Anti-malware and client firewalls are considered the most important security technologies. According to Figure 15, 90 percent of respondents believe anti-malware is critical. Almost as many say the same of client firewalls (86 percent of respondents). Seventy-one percent of respondents emphasize password protection and management are important and 61 percent of respondents say VPM and other secure Web gateways are key.

Figure 15. Security technologies considered essential and very important



Web and intranet servers are the most vulnerable endpoints or entry points to networks and enterprise systems. Fifty-two percent of respondents say their companies' Web servers and 46 percent of respondents say their intranet servers are most vulnerable to attack. However, as shown above, the technologies needed to mitigate these threats are not considered as important to the current security strategy.

Figure 16. What are the most vulnerable endpoints or entry points to your organization's networks and enterprise systems?
Three choices permitted

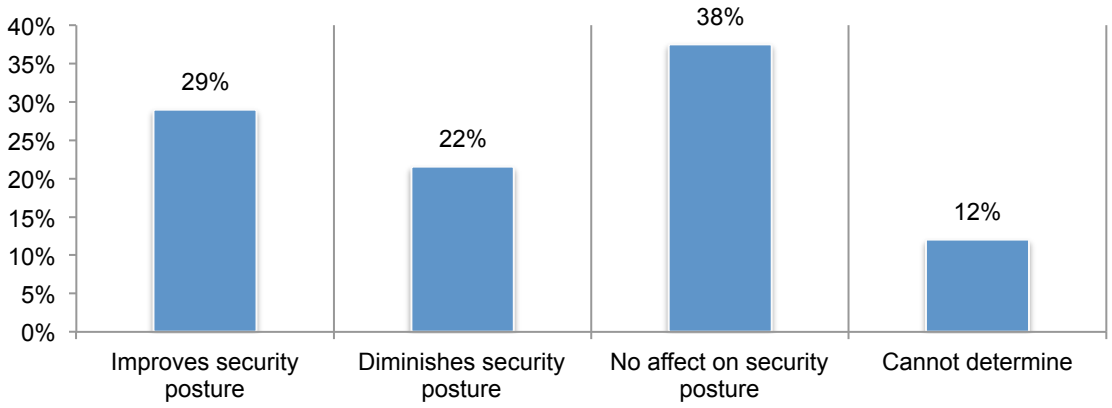


The impact of disruptive technologies on IT security posture

Cloud usage will increase. On average, 33 percent of an organization's total IT needs is fulfilled by cloud applications and/or infrastructure services and 39 percent of respondents say their use of cloud applications and/or IT infrastructure services will increase over the next 12 months. The Cloud is becoming more prevalent because of its benefits and it is not considered by their companies to be a significant impediment to cloud adoption, according to 72 percent of respondents.

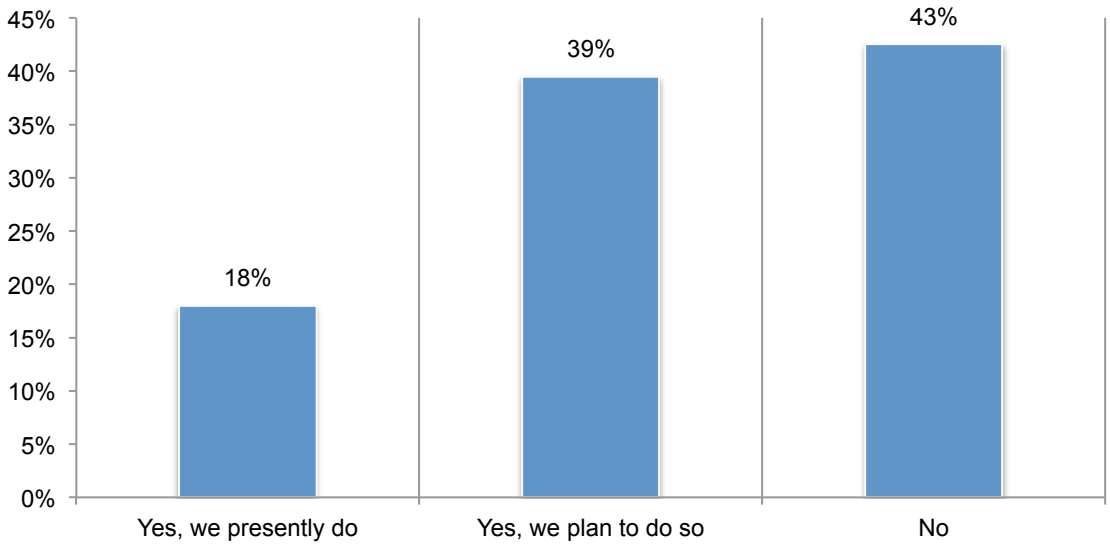
As shown in Figure 17, 38 percent of respondents say cloud applications and IT infrastructure services have no affect on security posture. However, 22 percent of respondents say it would diminish security posture but 12 percent of respondents are not sure what the impact will be on security.

Figure 17. How does the use of cloud applications and/or IT infrastructure services affect your organization's security posture?



Companies are vulnerable to cloud security risks. As shown in Figure 18, to address security, only 18 percent of respondents say their companies use cloud-based IT security services. However, another 39 percent of respondents say they will adopt these security services in the next 12 months. Such services include identity and access management, security incident event management (SIEM), encryption and key management.

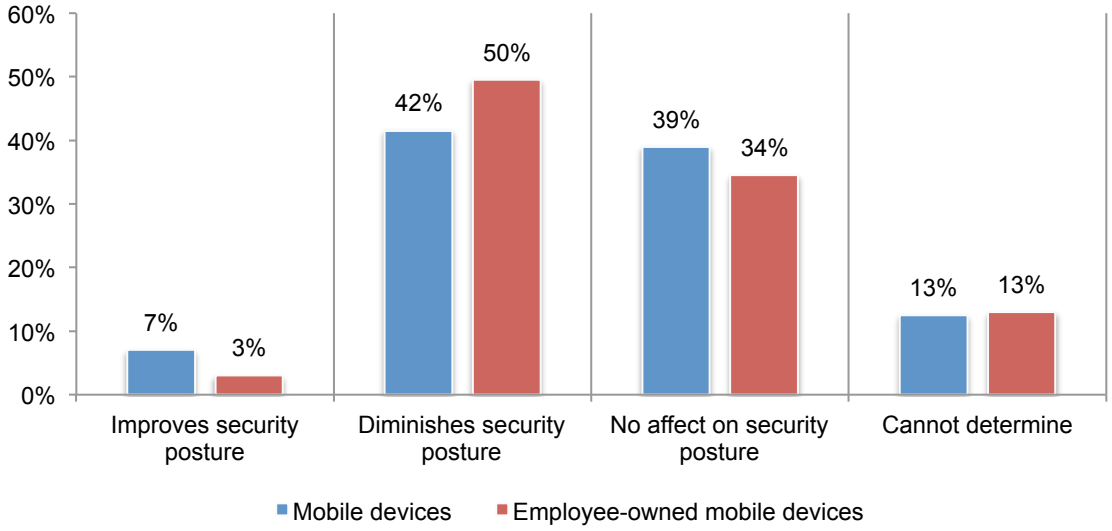
Figure 18. Does your organization use or plan to use cloud-based IT security services in the next year?



More mobile devices will be used to access business-critical applications and IT infrastructure. Currently, on average, 44 percent of business critical applications are accessed from mobile devices such as smartphones and tablets. Forty-two percent of respondents expect this to increase and another 42 percent of respondents say it will stay the same.

While mobile access is expected to increase or stay the same, 51 percent of respondents say security concerns do pose a significant impediment to the adoption of tablets and smartphones and as shown in Figure 19, 42 percent of respondents say they diminish security posture. If the mobile devices are employee-owned (BYOD) 50 percent of respondents say they diminish security posture.

Figure 19. How does the use of mobile devices to access business-critical applications and IT infrastructure affect your organization's security posture?



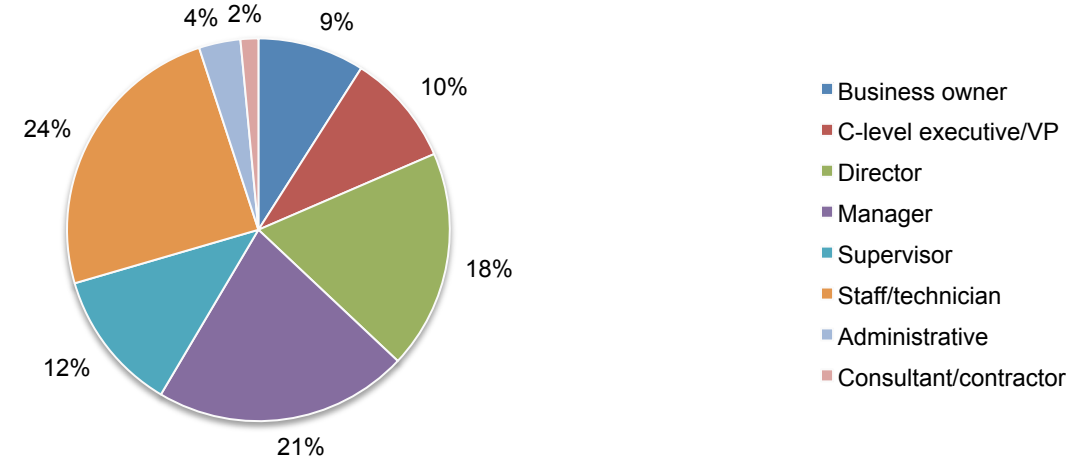
Part 3. Methods

A sampling frame of 16,401 IT and IT security practitioners in companies with a headcount from less than 100 to 1,000 were selected as participants in the research. Table 1 shows 665 total returns. Screening and reliability checks required the removal of 67 surveys. Our final sample consisted of 598 surveys or a 3.6 percent response.

Table 1. Sample response	Freq	Pct%
Sampling frame	16,401	100.0%
Total returns	665	4.1%
Rejected or screened surveys	67	0.4%
Final sample	598	3.6%

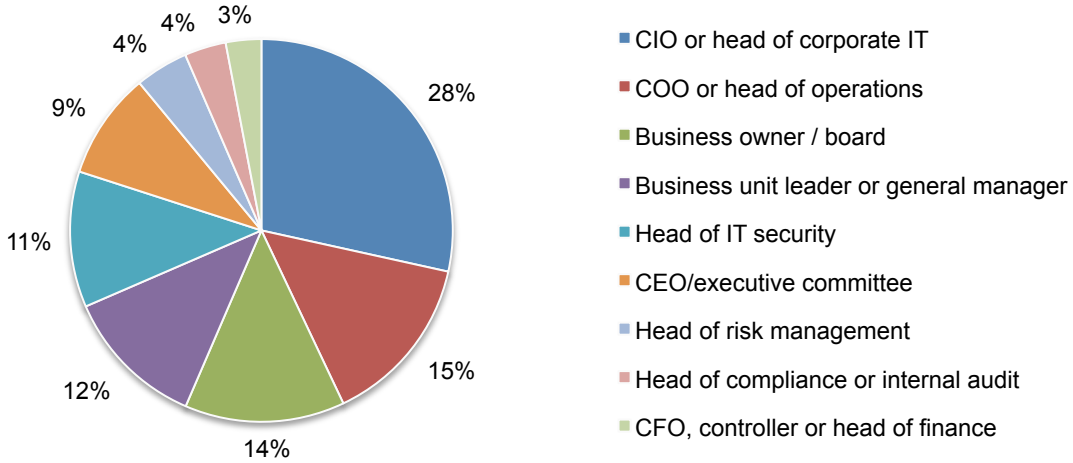
Pie Chart 1 reports the respondents' organizational level within participating organizations. By design, 70 percent of respondents are at or above the supervisory levels.

Pie Chart 1. Position level within the organization



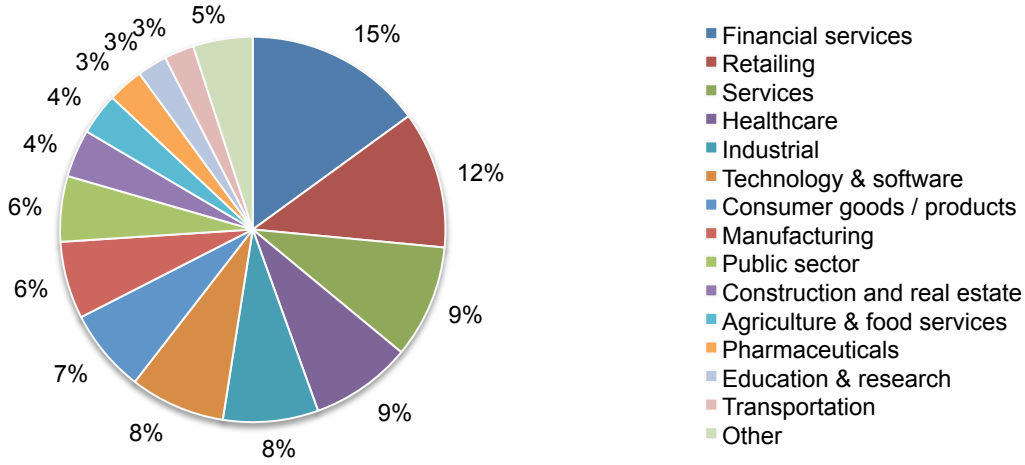
As shown in Pie Chart 2, 28 percent of respondents report directly to the CIO or head of corporate IT and 15 percent report to the COO or head of operations.

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 (15 percent) as the largest segment, followed by retailing (12 percent), services and healthcare both 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 from April 25, 2016 through May 9, 2016.

Survey response	Freq	Pct%
Total sampling frame	16,401	100.0%
Total returns	665	4.1%
Rejected or screened surveys	67	0.4%
Final sample	598	3.6%

Part 1. Screening Questions

S1. What range best describes the full-time employee headcount of your organization?	Total
Less than 100	81
100 to 250	104
251 to 500	116
501 to 750	157
751 to 1,000	140
More than 1,000 [STOP]	0
Total	598
Sample weighting	100.0%

S2. What best describes your role in managing the IT security function or activities within your organization? Check all that apply.	Total
Setting IT security priorities	61%
Managing IT security budgets	56%
Selecting vendors and contractors	49%
Determining IT security strategy	50%
Evaluating program performance	50%
None of the above [STOP]	0%
Total	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?	Total
Very high level of involvement	33%
High level of involvement	43%
Moderate level of involvement	22%
Low level of involvement	2%
Not involved [STOP]	0%
Total	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)?	Total
1 or 2	16%
3 or 4	46%
5 or 6	24%
7 or 8	10%
9 or 10	4%
Total	100%
Extrapolated value	4.25

Q2. What challenges keep your organization's IT security posture from being fully effective? Top 3 choices.	Total
Insufficient personnel	67%
Insufficient budget (money)	54%
Insufficient enabling security technologies	44%
No understanding how to protect against cyber attacks	39%
Lack of in-house expertise	36%
Not a priority issue	32%
Management does not see cyber attacks as a significant risk	11%
Lack of collaboration with other functions	11%
Lack of clear leadership	6%
Total	300%

Q3. What types of information are you most concerned about protecting from cyber attackers? Top 2 choices.	Total
Customer records	66%
Intellectual property	49%
Customer credit or debit card information	46%
Financial information	26%
Employee records	8%
Business correspondence	5%
Other (please specify)	1%
Total	200%

Q4. Who determines IT security priorities in your organization? Top 2 choices.	Total
Chief information officer (CIO)	35%
Chief executive	36%
No one function determines IT security priorities	35%
Head of operations	27%
Business owners	23%
Board of directors	11%
Lines of business	8%
Chief technology officer (CTO)	7%
Chief information security officer (CISO)	7%
General counsel	5%
Compliance officer	3%
Other (please specify)	1%
Total	200%

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

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

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

Q8. What percentage of your organization's IT personnel support IT security operations?	Total
None	1%
Less than 10%	3%
10 to 25%	19%
26 to 50%	22%
51 to 75%	20%
76 to 100%	34%
Total	100%
Extrapolated value	54%

Q9a. What percentage of your organization's IT security operations are supported by managed security services providers (MSSPs)?	Total
None [Skip Q8b]	54%
Less than 10%	11%
10% to 25%	13%
26% to 50%	9%
51% to 75%	9%
76% to 100%	4%
Total	100%
Extrapolated value	16%

Q9a. **ADJUSTED** What percentage of your organization's IT security operations are supported by managed security services providers (MSSPs)?	Total
None [Removed]	0%
Less than 10%	24%
10% to 25%	28%
26% to 50%	20%
51% to 75%	18%
76% to 100%	9%
Total	100%
Extrapolated value	34%

Q9b. Following are core services typically provided by MSSPs. Please check all services provided by MSSPs to support your organization's IT security posture.	Total
Monitored or managed firewalls or intrusion prevention systems (IPSs)	74%
Monitored or managed intrusion detection systems (IDSs)	47%
Monitored or managed multifunction firewalls	23%
Managed or monitored security gateways for messaging or Web traffic	50%
Security analysis and reporting of events collected from IT infrastructure logs	17%
Reporting associated with monitored/managed devices and incident response	15%
Managed vulnerability scanning of networks, servers, databases or applications	40%
Distributed denial of service (DDoS) protection	12%
Monitoring or management of customer-deployed security information and event management (SIEM) technologies	10%
Monitoring and/or management of advanced threat defense technologies	11%
Total	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.	Total
PCI DSS	42%
ISO 27001/2	3%
SOC 2/3	13%
COBIT	11%
SOX 404	16%
NIST	16%
HIPAA/HiTECH	15%
None of the above	41%
Other (please specify)	6%
Total	163%

Part 3: Cyber Attacks

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

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

Q12a. 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?	Total
Yes	50%
No [skip to Q12]	38%
Unsure [skip to Q12]	12%
Total	100%

Q12b. If yes, with respect to your organization's largest breach over the past months, how many individual records were lost or stolen?	Total
Less than 100	35%
100 to 500	29%
501 to 1,000	19%
1,001 to 10,000	8%
10,001 to 50,000	5%
50,001 to 100,000	4%
100,001 to 1,000,000	0%
More than 1,000,000	0%
Total	100%
Extrapolated value	5,079

Q12c. If yes, what were the root causes of the data breaches experienced by your organization? Please select that apply.	Total
Malicious insider	5%
External (hacker) attacks	27%
Negligent employee or contractor	48%
Error in system or operating process	35%
Third party mistakes	41%
Other (please specify)	2%
Don't know	32%
Total	189%

Q13. Does your organization have an incident response plan for responding to cyber attacks and data breaches?	Total
Yes	48%
No	48%
Unsure	3%
Total	100%

Q14a. Has your organization ever experienced situations when exploits and malware have evaded your intrusion detection system?	Total
Yes	57%
No	21%
Don't have IDS	22%
Total	100%

Q14b. Has your organization ever experienced situations when exploits and malware have evaded your anti-virus solutions?	Total
Yes	76%
No	21%
Don't have anti-virus	3%
Total	100%

Please rate the following statements using the five-point scale provided below each item. % Strongly Agree and Agree responses combined	Total
Q15a. Cyber attacks experienced by my organization are becoming more **targeted**.	52%
Q15b. Cyber attacks experienced by my organization are becoming more **sophisticated**.	51%
Q15c. Cyber attacks experienced by my organization are becoming more **severe** in terms of negative consequences (such as financial impact).	51%
Q15d. The use of strong passwords and/or biometrics is an essential part of my organization's security defense.	60%

Part 4. Disruptive Technology Trends

Q16. What percent of your organization's total IT needs are fulfilled by **cloud** applications and/or infrastructure services?	Total
Zero	28%
Less than 10%	10%
11 to 25%	10%
36 to 50%	18%
51 to 75%	23%
76 to 100%	11%
Total	100%
Extrapolated value	33%

Q17. Over the next 12 months, will your organization's use of **cloud** applications and/or IT infrastructure services increase, decrease or stay at about the same level?	Total
Increase	39%
Decrease	2%
Stay the same	47%
Cannot determine	13%
Total	100%

Q18. [skip if Zero was selected in Q15]. In your opinion, how does the use of **cloud** applications and/or IT infrastructure services affect your organization's security posture?	Total
Improves security posture	29%
Diminishes security posture	22%
No affect on security posture	38%
Cannot determine	12%
Total	100%

Q19. In your opinion, do you view security concerns as a significant impediment to cloud adoption within your organization?	Total
Yes	28%
No	72%
Total	100%

Q20. Does your organization use (or plan to use) **cloud-based** IT security services in the next 12 months (such as identity and access management, security incident event management (SIEM), encryption, key management, etc.)?	Total
Yes, we presently do	18%
Yes, we plan to do so	39%
No	43%
Total	100%

Q21. 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.	Total
Zero	4%
Less than 10%	5%
11 to 25%	15%
36 to 50%	38%
51 to 75%	25%
76 to 100%	13%
Total	100%
Extrapolated value	44%

Q22. Does your organization have **visibility** 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?	Total
Yes	41%
No	54%
Unsure	5%
Total	100%

Q23a. Does your organization have a policy pertaining to employees' use of passwords and/or biometrics (such as a fingerprint)?	Total
Yes	44%
No	51%
Unsure	5%
Total	100%

Q23b. If yes, does your organization strictly enforce this policy?	Total
Yes	31%
No	65%
Unsure	4%
Total	100%

Q23b-1. If Q22a=yes, does this policy require employees to use a password or biometric to secure access to mobile devices?	Total
Yes	42%
No	54%
Unsure	4%
Total	100%

Q23b-2. If no, why doesn't your organization require password or biometric protections on mobile devices? More than one choice permitted	Total
We have other compensating controls for securing mobile devices	33%
We don't see the need for more policies	23%
Passwords are obsolete	19%
Resetting passwords reduces employee productivity	47%
We can't monitor employee non-compliant behavior	54%
Total	176%

Q24. Over the next 12 months, will your employees' use of mobile devices to access business-critical applications and IT infrastructure increase, decrease or stay at about the same level?	Total
Increase	42%
Decrease	4%
Stay the same	42%
Cannot determine	12%
Total	100%

Q25. 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?	Total
Improves security posture	7%
Diminishes security posture	42%
No affect on security posture	39%
Cannot determine	13%
Total	100%

Q26. In your opinion, do you view security concerns as a significant impediment to the adoption of tablets and smart phones within your organization?	Total
Yes	51%
No	49%
Total	100%

Q27. What percent of mobile devices used to access business-critical applications are **employee-owned** (a.k.a. BYOD)?	Total
Zero	28%
Less than 10%	6%
11 to 25%	8%
36 to 50%	9%
51 to 75%	20%
76 to 100%	29%
Total	100%
Extrapolated value	43%

Q28. Over the next 12 months, will the use of **employee-owned** mobile devices or BYOD to access business-critical applications and IT infrastructure increase, decrease or stay at about the same level?	Total
Increase	30%
Decrease	6%
Stay the same	52%
Cannot determine	12%
Total	100%

Q29. In your opinion, how does the use of **employee-owned** mobile devices to access business-critical applications and IT infrastructure affect your organization's security posture?	Total
Improves security posture	3%
Diminishes security posture	50%
No affect on security posture	34%
Cannot determine	13%
Total	100%

Q30. In your opinion, do you view security concerns as a significant impediment to the adoption of BYOD within your organization?	Total
Yes	61%
No	39%
Total	100%

Part 5. Enabling Security Technologies

Q31. Do the security technologies currently used by your organization detect and block most cyber attacks?	Total
Yes	33%
No	67%
Total	100%

Q32. 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.	Total
Anti-malware	90%
Client firewalls	86%
Password protection / management	71%
VPM and other secure web gateways	61%
Intrusion detection and prevention	53%
Automated patch management systems	49%
Anti-denial of services	44%
Encryption technologies	37%
Web application firewalls (WAF)	35%
Identity & access management	34%
Security incident & event management (SIEM)	31%
Mobile device management (MDM)	30%
Next generation firewalls (NGFW)	28%
Endpoint management	26%
Network traffic intelligence	25%
Big data analytics	24%
Data loss prevention (DLP)	22%
Unified threat management (UTM)	13%
Tokenization	13%
Total	775%

Q33. In your opinion, what are the most vulnerable endpoints or entry points to your organization's networks and enterprise systems? Top 3 responses.	Total
Desktops	26%
Laptops	43%
Tablets	28%
Smart phones	43%
Web server	52%
Intranet server	46%
Routers	12%
Portable storage devices (including USBs)	13%
Cloud systems	34%
Other (please specify)	3%
Total	300%

Q34. Please rate the importance of passwords or biometric authentication for securing endpoints and/or entry points to your organization's networks and enterprise systems.	Total
Essential	40%
Very important	36%
Important	12%
Not important	8%
Irrelevant	3%
Total	100%

Part 6. Cost Estimation

Q35a. Approximately, how much did damage or theft of IT assets and infrastructure cost you organization over the past 12 months?	Total
We had no compromises	39%
Less than $5,000	9%
$5,001 to $10,000	6%
$10,001 to $50,000	5%
$50,001 to $100,000	7%
$100,001 to $250,000	6%
$250,001 to $500,000	4%
$500,001 to $999,999	10%
$1 million to $5 million	8%
$5 million to $10 million	5%
More than $10 million	1%
Total	100%
Extrapolated value	$879,582

Q35b. Approximately, how much did disruption to normal operations cost your organization over the past 12 months?	Total
We had no compromises	39%
Less than $5,000	2%
$5,001 to $10,000	3%
$10,001 to $50,000	5%
$50,001 to $100,000	9%
$100,001 to $250,000	10%
$250,001 to $500,000	5%
$500,001 to $999,999	10%
$1 million to $5 million	10%
$5 million to $10 million	5%
More than $10 million	1%
Total	100%

Extrapolated value	$955,429

Part 7. Role & Organizational Characteristics

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

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

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