The State of Cybersecurity in Healthcare Organizations in 2018

Independently conducted by Ponemon Institute LLC

Sponsored by Merlin

Publication Date: March 2018

The State of Cybersecurity in Healthcare Organizations in 2018

Ponemon Institute, March 2018

Part 1. Introduction

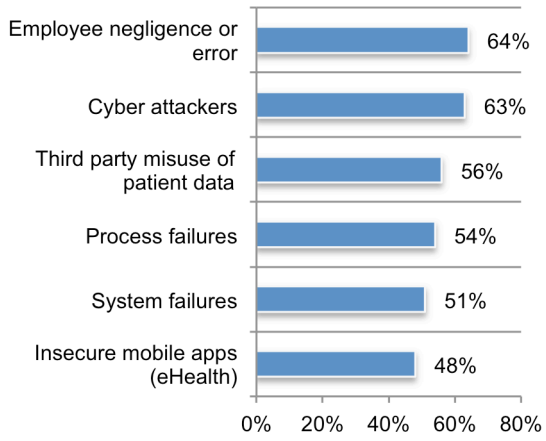
A strong cybersecurity posture in healthcare is critical to patient safety. Attacks on patient information, medical devices and a hospital's systems and operations can have a variety of serious consequences. These can include disrupting the delivery of services, putting patients at risk for medical identity theft and possibly endangering the lives of individuals who have a medical device.

To determine the prognosis for healthcare organizations' ability to reduce cyber attacks, Ponemon Institute conducted *The State of Cybersecurity in Healthcare Organizations in 2018*[1], sponsored by Merlin. We surveyed 627 IT and IT security practitioners in a variety of healthcare organizations that are subject to HIPAA. According to the research, spending on IT increased from an average of $23 million in 2016 to $30 million annually and the average number of cyber attacks each year increased from 11 to 16. On average, organizations spend almost $4 million to remediate an attack.

As shown in Figure 1, healthcare organizations are not immune to the same threats facing other industries. The threats that are the source of most concern are employee errors and cyber attacks. However, third-party misuse of patient data, process and system failures and insecure mobile apps also create significant risk.

Figure 1. Top six security threats for healthcare organizations

Six responses permitted



The following factors are affecting healthcare organizations ability to secure sensitive data and systems

- The existence of legacy systems and disruptive technologies, such as cloud, mobile, big data and Internet of Things, put patient information at risk.
- More attacks evade intrusion prevention systems (IPS) and advanced persistent threats (APTs).
- Disruptions to operations and system downtime caused by denial of service (DDoS) attacks are increasing.
- Healthcare organizations are targeted because of the value of patient medical and billing records.
- Not enough in-house expertise and security leadership makes it more difficult to reduce risks, vulnerabilities and attacks.

[1] *The State of Cybersecurity in Healthcare Organizations in 2016*, conducted by Ponemon Institute, February 2016

Best practices from high- performing healthcare organizations

As part of the research, we did a special analysis of those respondents (59 respondents out of the total sample of 627 respondents) who rated their organizations' effectiveness in mitigating risks, vulnerabilities and attacks against their organizations as very high (9+ on a scale of 1 = low effectiveness to 10 = high effectiveness. These respondents are referred to as high performer and the analysis is presented in this report.

According to the research, these high-performing organizations are able to significantly reduce cyber attacks. Following are characteristics of high-performing organizations:

- More likely to have an incident response plan and a strategy for the security of medical devices.
- Technologies and in-house expertise improve their ability to prevent the loss or exposure of patient data, DDoS attacks and other attacks that evade their IPS and AV solutions.
- High-performing organizations are better at increasing employee awareness about cybersecurity risks.
- High-performing organizations also are more positive about the ability to ensure third-party contracts safeguard the security of patient information.
- High-performing organizations are more likely to have the necessary in-house expertise, including a CISO or equivalent.

Part 2. Key findings

In this section, we provide a deeper analysis of the research. When possible, we compare the findings in this year's research to the 2016 study.

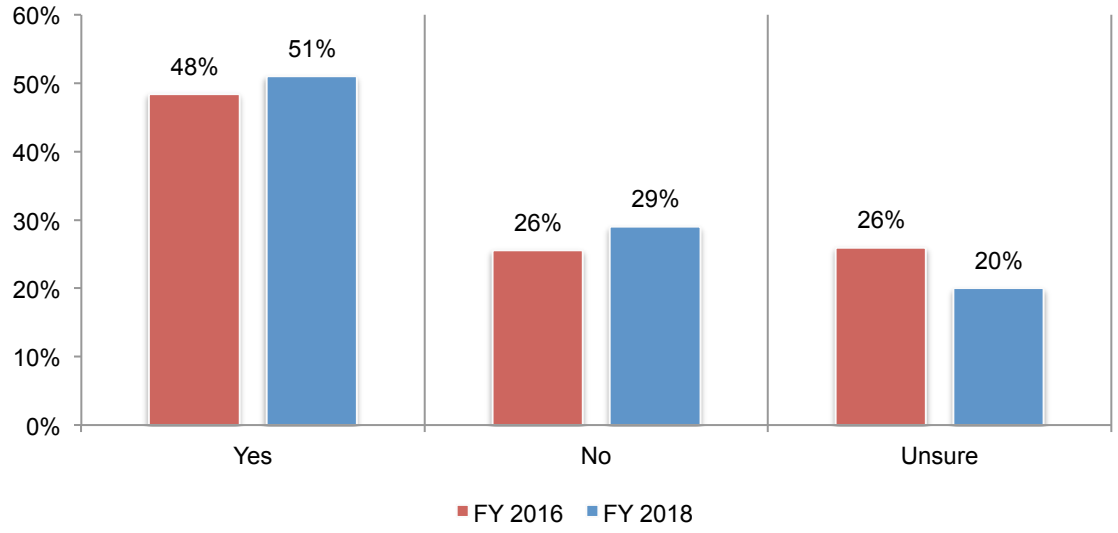
The complete audited findings are presented in the Appendix. The report is organized according to the following topics:

- Trends in risks facing healthcare organizations: Why more cyber attacks are occurring
- Steps taken to improve the security posture of healthcare organizations
- Lessons from high-performing healthcare organizations

Trends in risks facing healthcare organizations: Why more cyber attacks are occurring

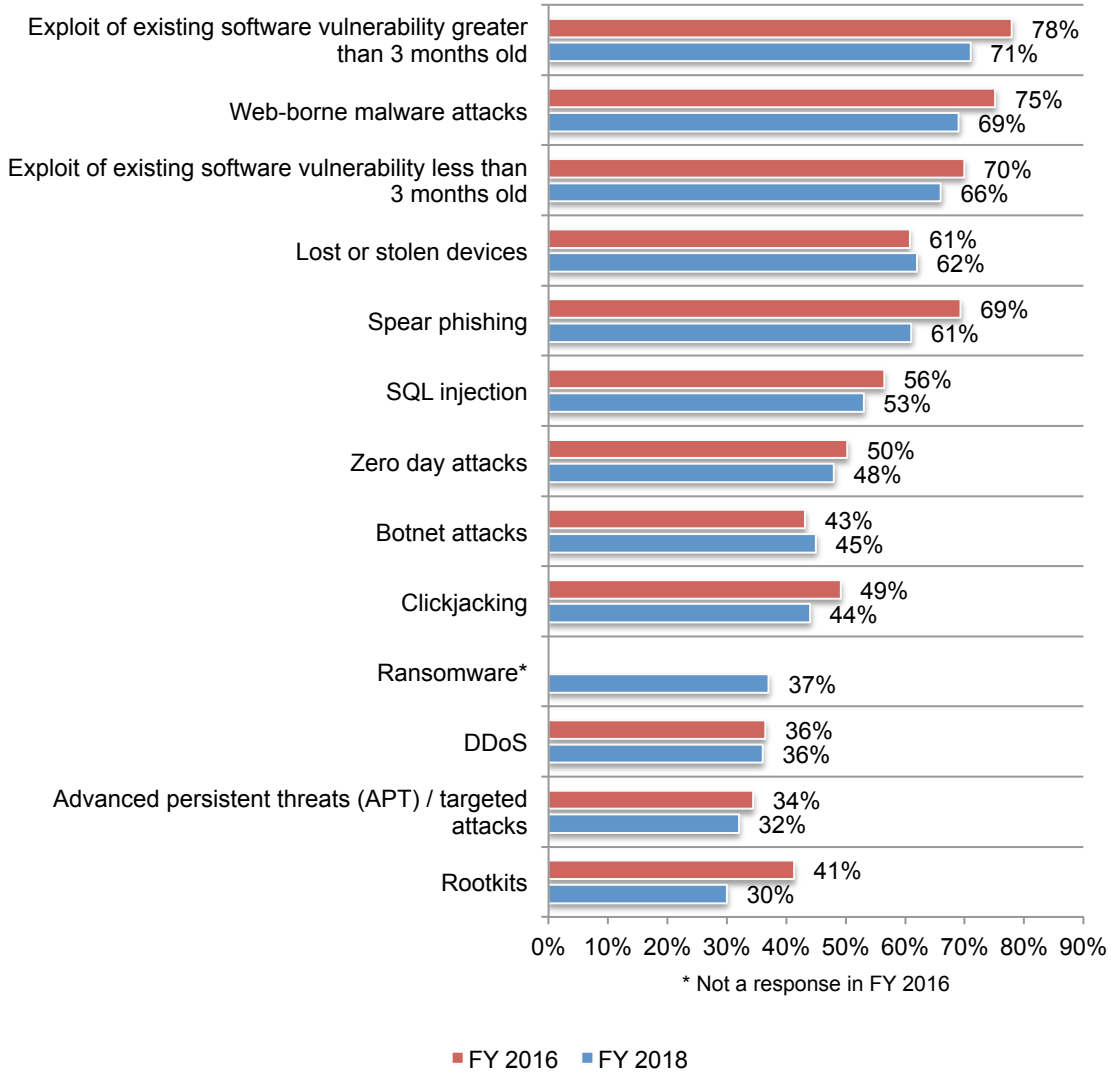
Patient information is under attack and at risk. Annually, on average healthcare organizations experience 16 cyber attacks, an increase from 11 attacks in the 2016 study. As shown in Figure 2, more than half (51 percent of respondents) say their organizations have experienced an incident involving the loss or exposure of patient information in the past 12 months, an increase from 48 percent in 2016.

Figure 2. Has your organization experienced an incident involving the loss or exposure of patient information in the past 12 months?
Extrapolated value = 16.3 attacks



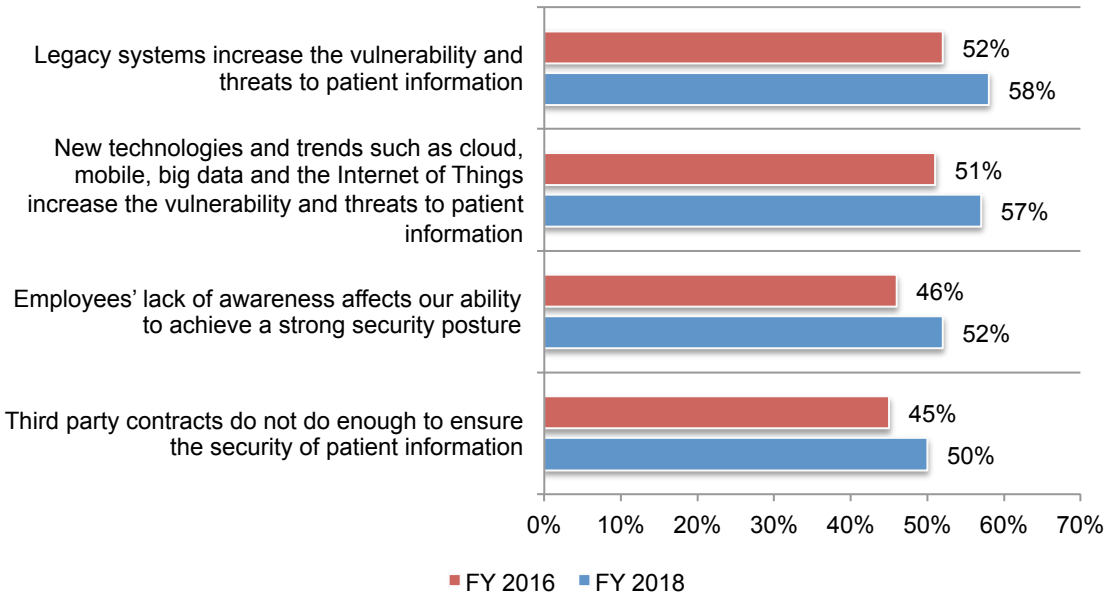
Healthcare organizations are experiencing ransomware attacks. Figure 3 presents trends in the various security incidents experienced by healthcare organizations. For the first time, ransomware attacks were included and 37 percent of respondents say their organizations experienced such an attack. While some security incidents decreased, healthcare organizations continue to be at great risk from a variety of threats.

Figure 3. Trends in the security incidents organizations experience
More than one response permitted



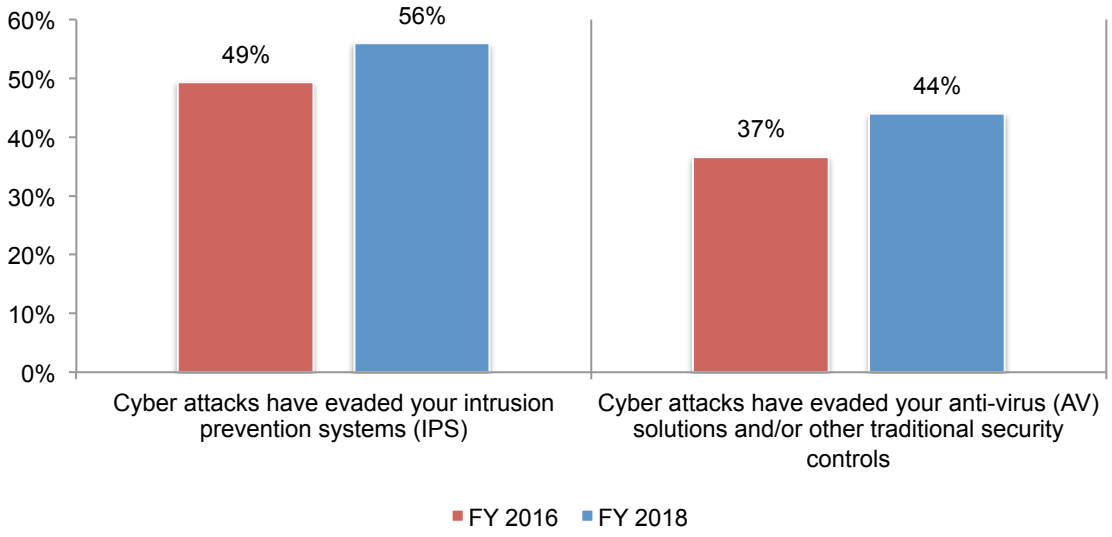
Legacy systems and disruptive technologies, such as cloud, mobile big data and Internet of Things, put patient information at risk. As presented in Figure 4, more organizations consider legacy systems as a serious risk to patient information (58 percent of respondents vs. 52 percent of respondents in 2016). In addition, new technologies and trends such as the cloud, mobile, big data and the Internet of Things are increasing the vulnerability and threats to patient information (51 percent of respondents vs. 57 percent of respondents). More respondents are concerned about the effectiveness of third-party contracts to secure patient information.

Figure 4. Trends in perceptions about why patient information is at risk
Strongly agree and Agree response combined



More attacks evade intrusion prevention systems (IPS) and advanced persistent threats (APTs). As shown in Figure 5, 56 percent of respondents say their organizations have experienced situations where cyber attacks evaded their intrusion prevention, an increase from 49 percent of respondents in 2016. Forty-four percent of respondents say their organizations have experienced cyber attacks that evaded their anti-virus (AV) solutions and/or traditional security controls.

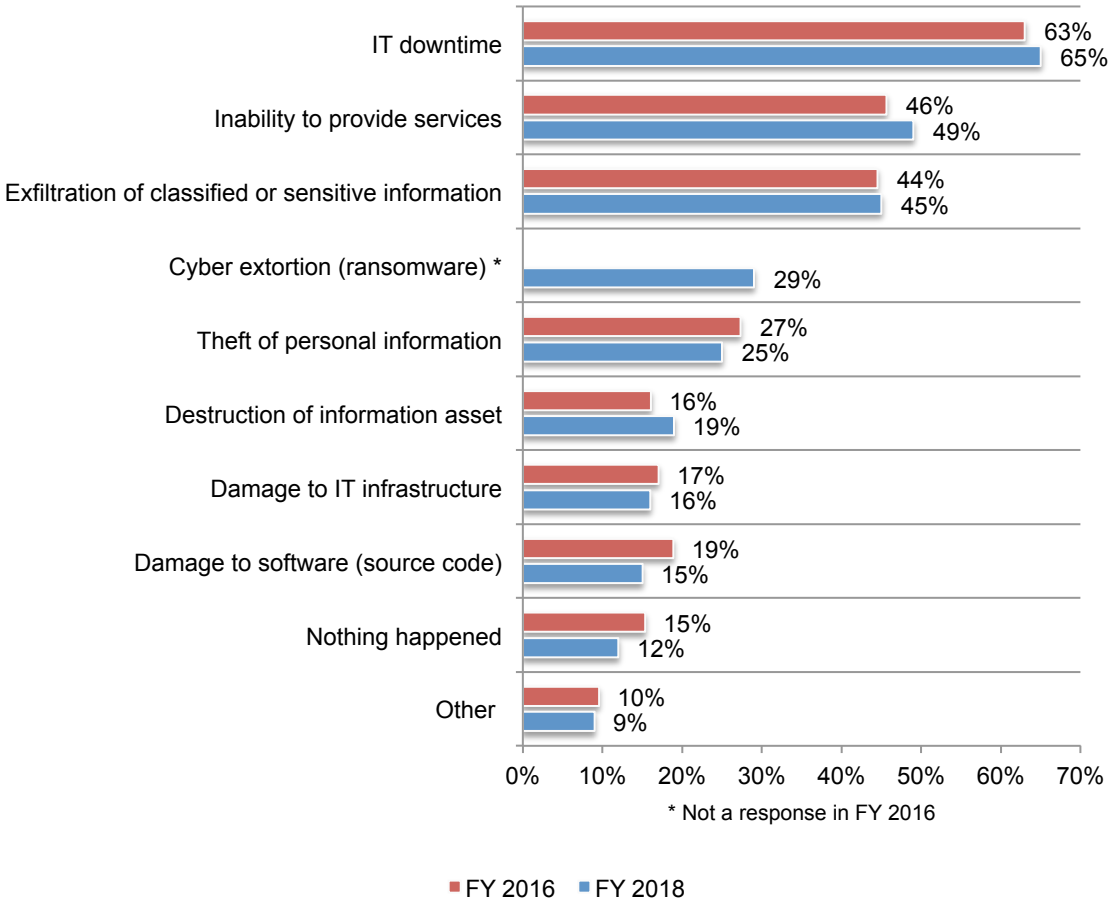
Figure 5. Has your organization experienced cyber attacks that evaded IP, AV solutions and other security controls?



More organizations have systems and controls in place to detect and stop advanced persistent threats (APTs). Thirty-three percent of respondents say their organizations have systems and controls in place to detect and stop APTs, an increase from 26 percent of respondents in 2016.

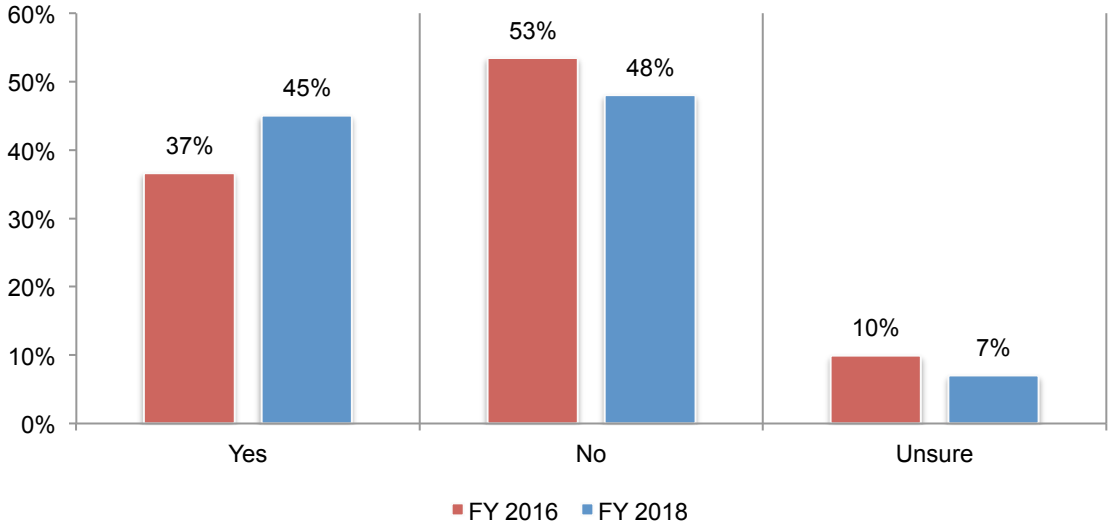
As shown in Figure 6, 65 percent of respondents say the primary consequences of APTs and zero-day attacks were IT downtime, followed by the inability to provide services (49 percent of respondents), which create serious risks in the treatment of patients. However, this year 29 percent of respondents say they experienced a ransomware attack.

Figure 6. What happened as a result of the APTs or zero day threats?
More than one response permitted



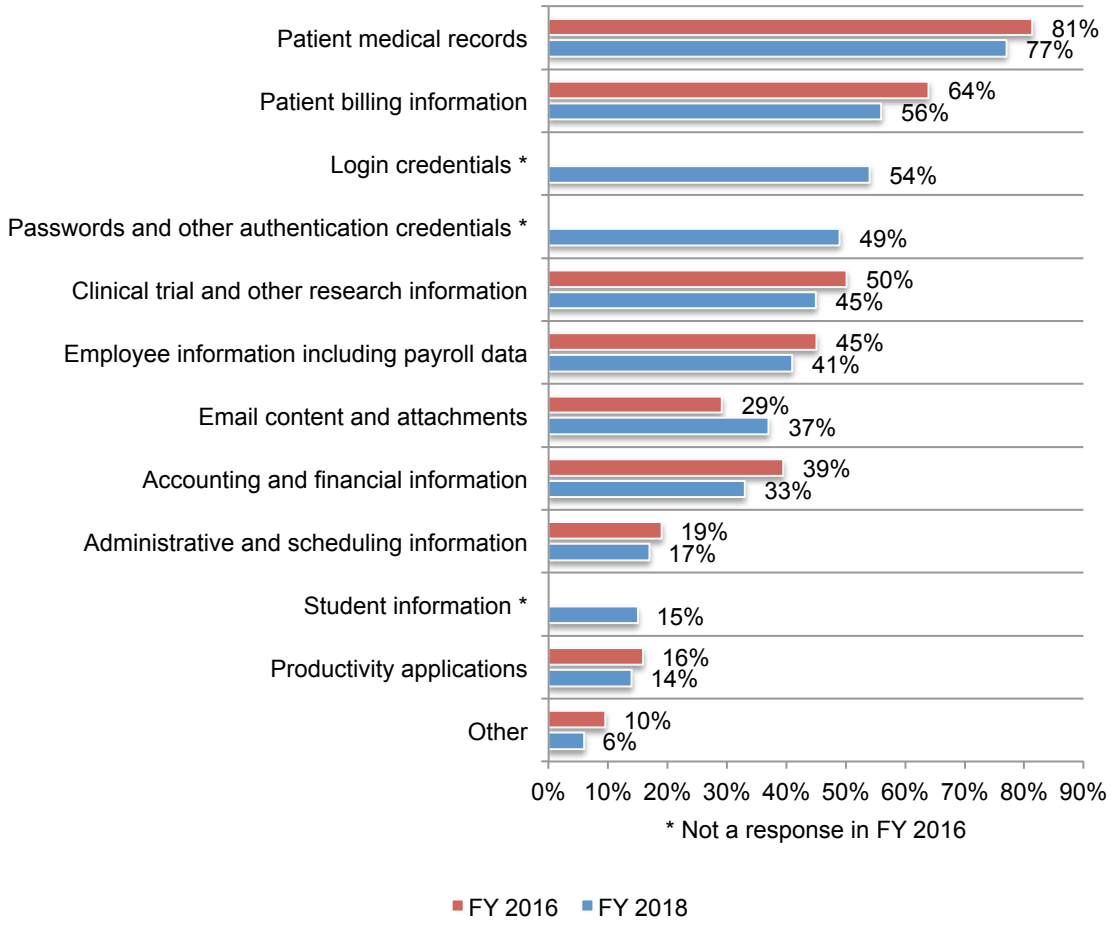
Denial of service (DDoS) attacks increase. As shown in Figure 7, 45 percent of respondents report their organization had a DDoS attack, an increase from 37 percent of respondents in the 2016 research. On average, organizations experienced 2.94 DDoS attacks in the past 12 months, an increase from 2.65 in 2016.

Figure 7. Did your organization experience a DDoS attack that caused a disruption to operations and/or system downtime?



Hackers are most interested in stealing patient information. The most lucrative information for hackers can be found in patients' medical records and billing information according to 77 percent and 56 percent of respondents, respectively (Figure 8).

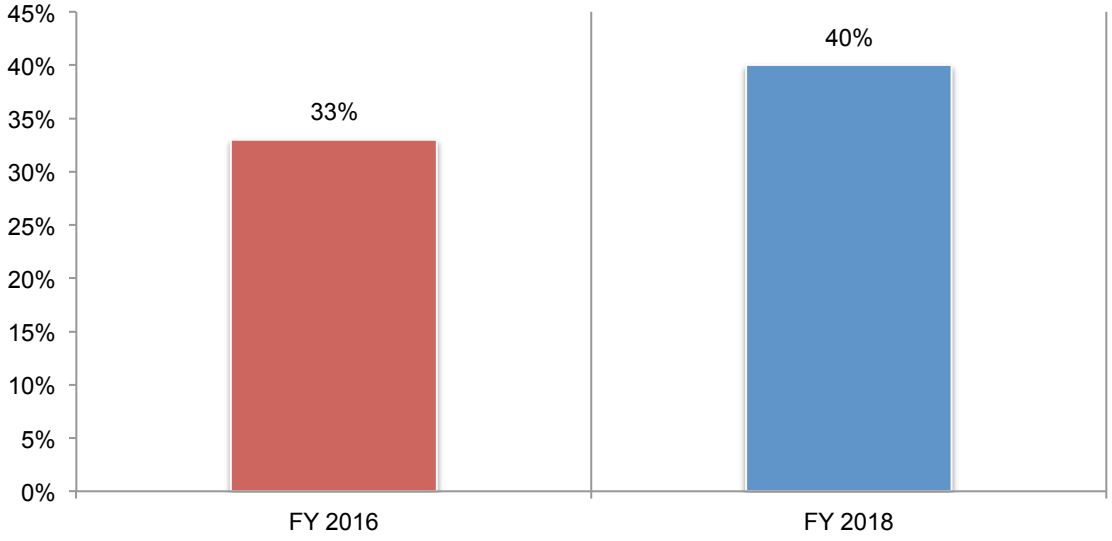
Figure 8. What types of information do you believe hackers are most interested in stealing?
More than one response permitted



Steps taken to improve the cybersecurity posture of healthcare organizations

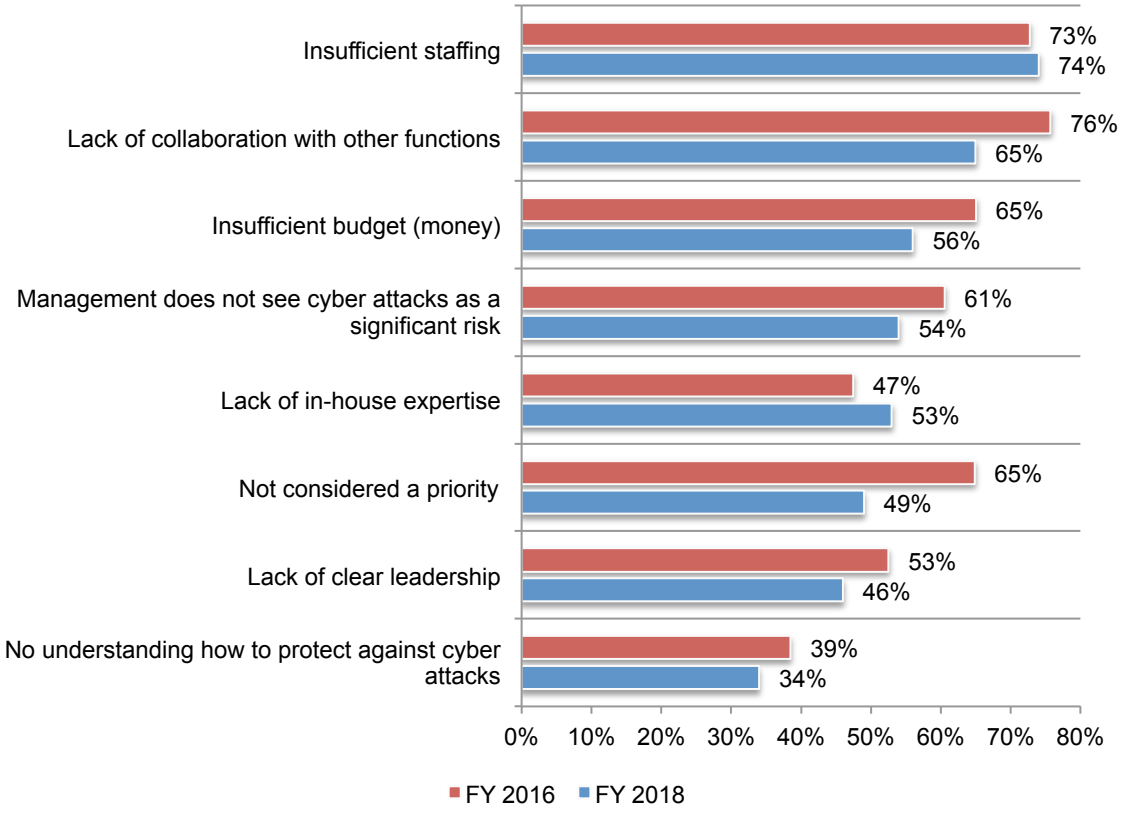
Healthcare organizations' ability to mitigate risks, vulnerabilities and attacks across the enterprise improves. Cyber attacks may be increasing but organizations are improving their responsiveness. When asked to rate the effectiveness of their organization's effectiveness at mitigating risks, vulnerabilities and attacks across the enterprise on a scale of 1 = not effective to 10 = very effective, 40 percent of respondents rate their organizations' cyber security posture as very effective an increase from 33 percent, as shown in Figure 9.

Figure 9. Effectiveness in cybersecurity posture increases
7+ responses on a scale of 1 = not effective to 10 = very effective



Insufficient staffing is the biggest challenge to improving the ability to reduce risks, vulnerabilities and attacks. As presented in Figure 10, the primary barrier to having a more effective cybersecurity posture is insufficient staffing (74 percent of respondents). Related to this is the increase in the challenge of having the necessary in-house expertise to reduce risks, vulnerabilities and attacks (53 percent of respondents).

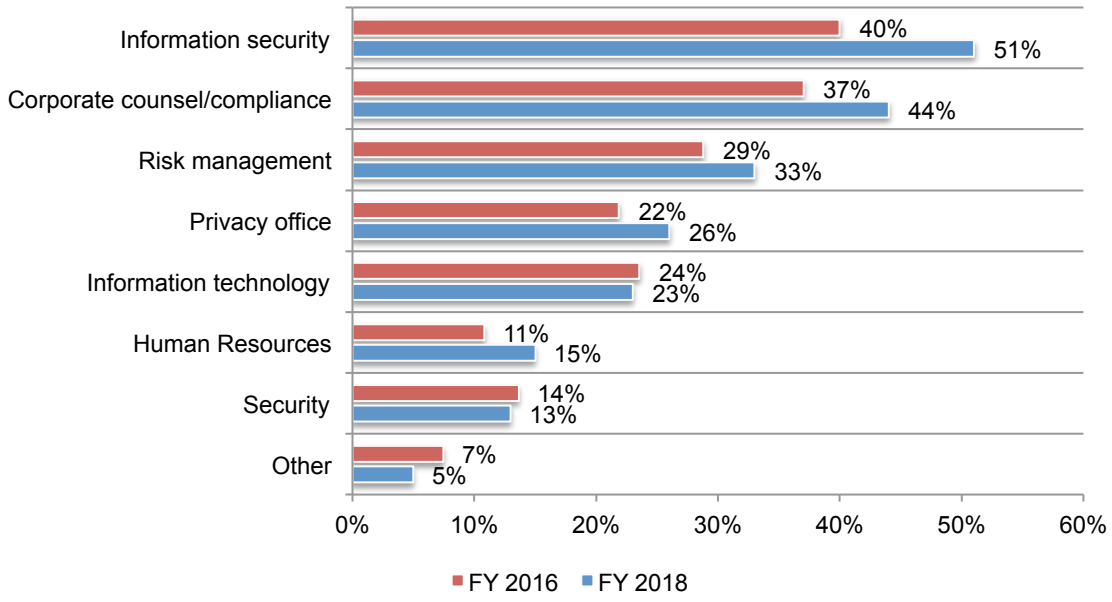
Figure 10. What challenges keep your organization's cybersecurity posture from being fully effective?
More than one response permitted



Corporate compliance and information security increase their involvement in the incident response plan. Fifty-nine percent of respondents say their organization has an incident response plan in place, an increase from 50 percent in the 2016 study.

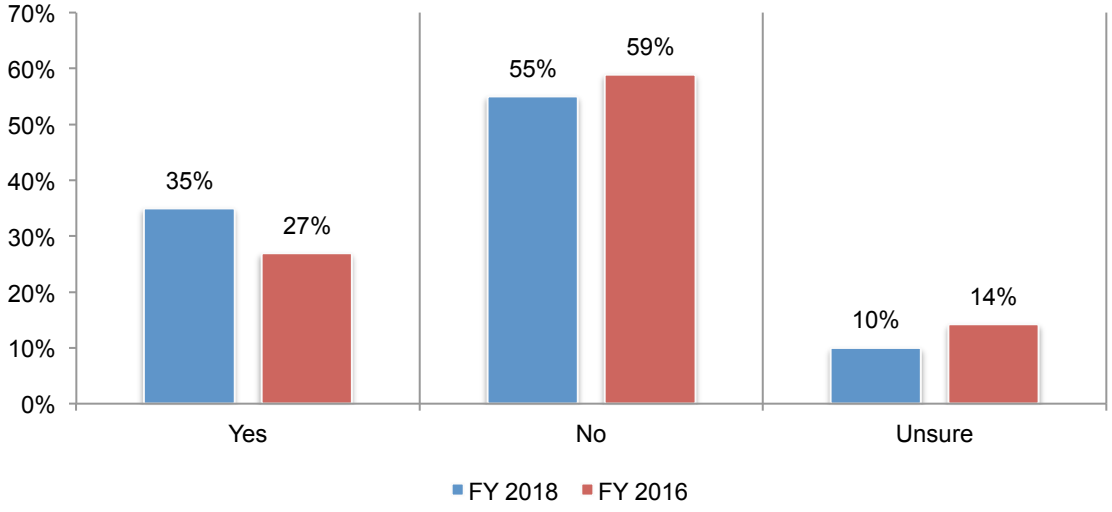
According to Figure 11, information security professionals and corporate counsel/compliance professionals increase their involvement in the incident response process.

Figure 11. Who is involved in the incident response process?
More than one response permitted



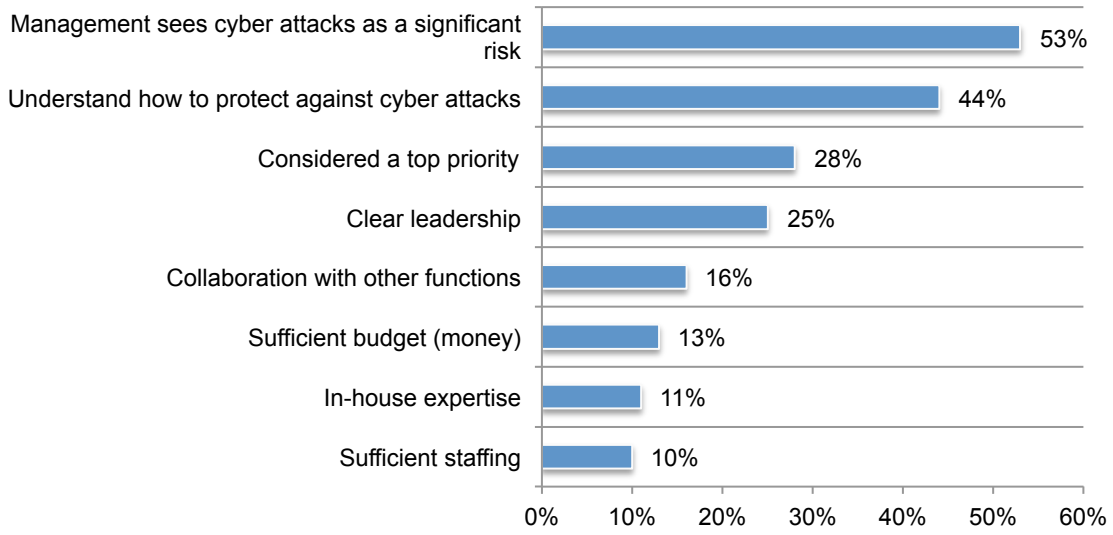
Awareness of the threats to medical devices drives more healthcare organizations to include them in cybersecurity strategies. As shown in Figure 12, 35 percent of respondents say their organizations will take steps, as part of their cybersecurity strategy, to protect medical devices, an increase from 27 percent of respondents in the previous research. Of those organizations that do not address the risk to medical devices, 62 percent will do so in the next 12 months.

Figure 12. Is the security of medical devices part of your cybersecurity strategy?



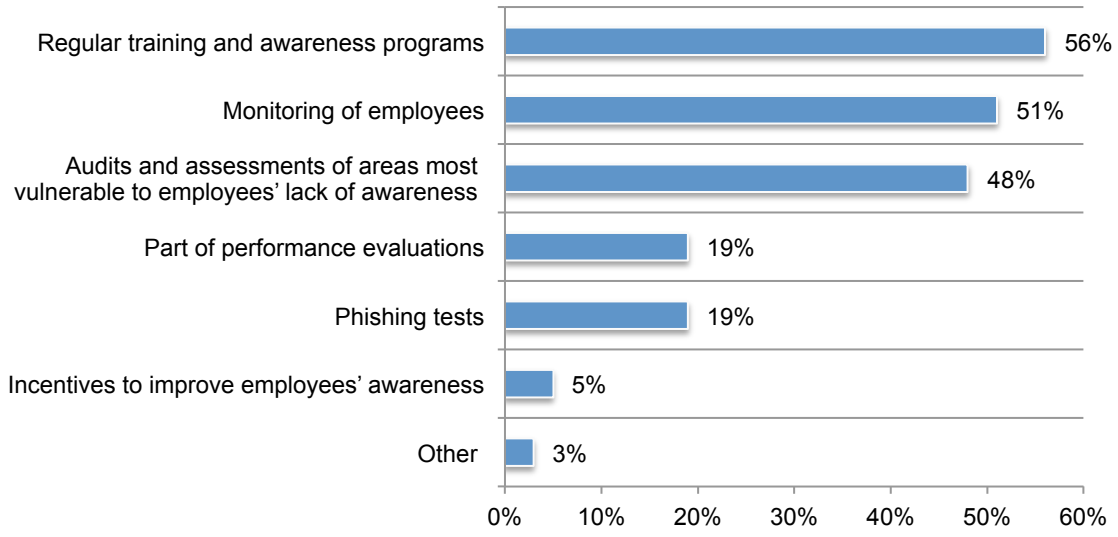
Support from senior leadership is the most important advantage to reducing cybersecurity threats. As shown in Figure 13, more than half (53 percent) of respondents say their management recognizes that cyber attacks is a serious risk and 44 percent of respondents say their organizations understand how to protect against cyber attacks. Only 11 percent of respondents say it is in-house expertise and 10 percent of respondents say sufficient staffing is an advantage. As discussed previously (Figure 10), insufficient staffing is the biggest barrier to achieving a stronger cybersecurity posture.

Figure 13. What are your organization's advantages in mitigating cybersecurity threats?
Two responses permitted



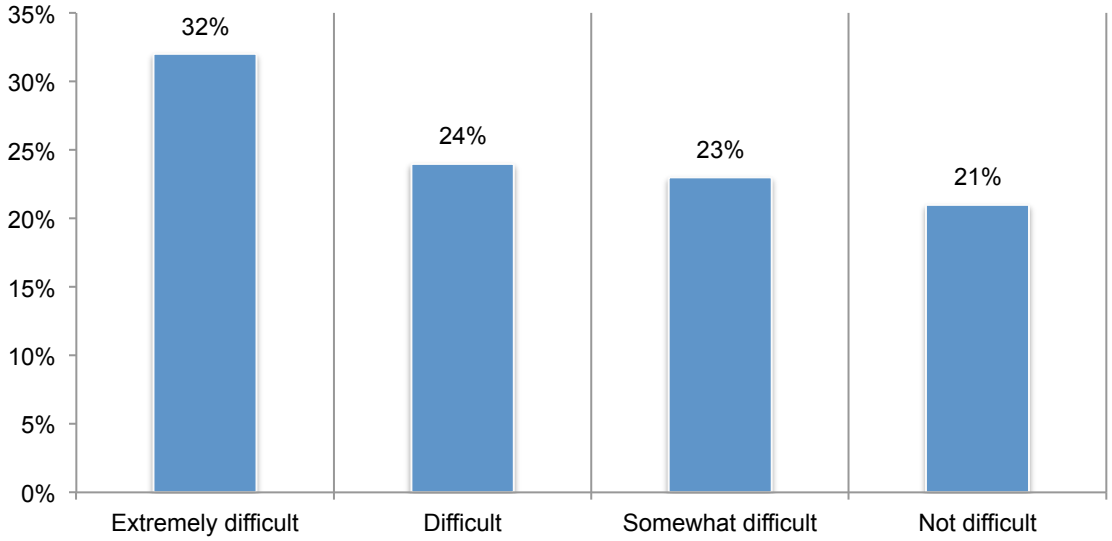
Despite the risk of employee error, many healthcare organizations are not taking steps to increase awareness about cybersecurity threats. Less than half (48 percent) of respondents say they have awareness programs in place. These organizations typically have regular training and awareness programs, monitor employees and conduct audits and assessment of areas most vulnerable to employees' lack of awareness

Figure 14. What steps does your organization take to increase employees' awareness about cybersecurity threats?
More than one response permitted



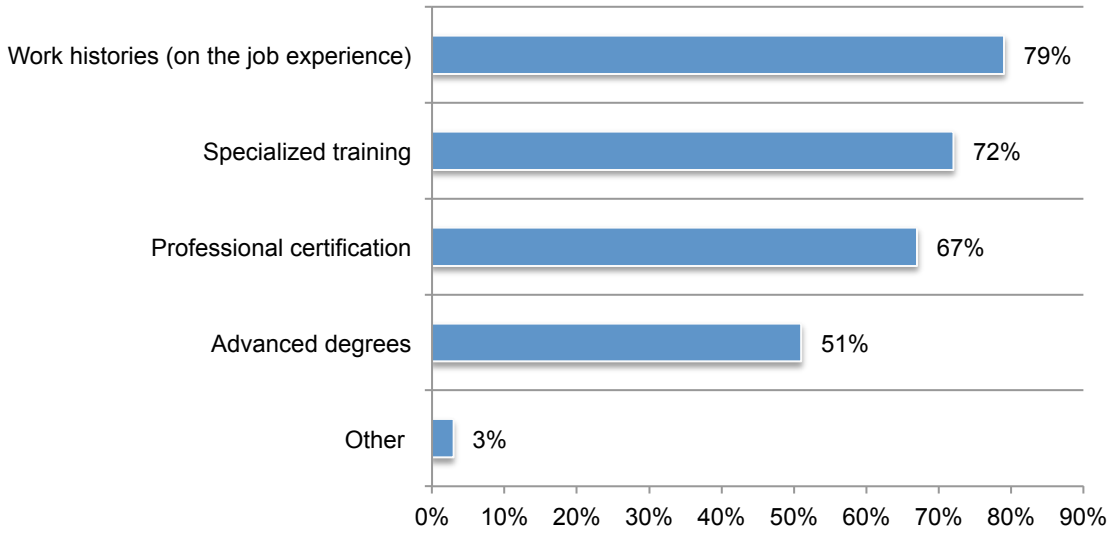
Almost all healthcare organizations find it difficult to staff their IT security function. As shown in Figure 15, 79 percent of respondents say it is difficult to recruit IT security personnel. Slightly more than half (51 percent) of respondents say their organizations have a CISO.

Figure 15. How difficult is it to recruit IT security personnel?



Work histories and specialized training are most important in the hiring of expert personnel. Only 32 percent of respondents say they have a sufficient number of in-house personnel who possess these qualifications. Figure 16 presents the most desirable qualifications for IT security personnel. Of greatest value is actual hands-on experience (79 percent of respondents) and specialized training (72 percent of respondents).

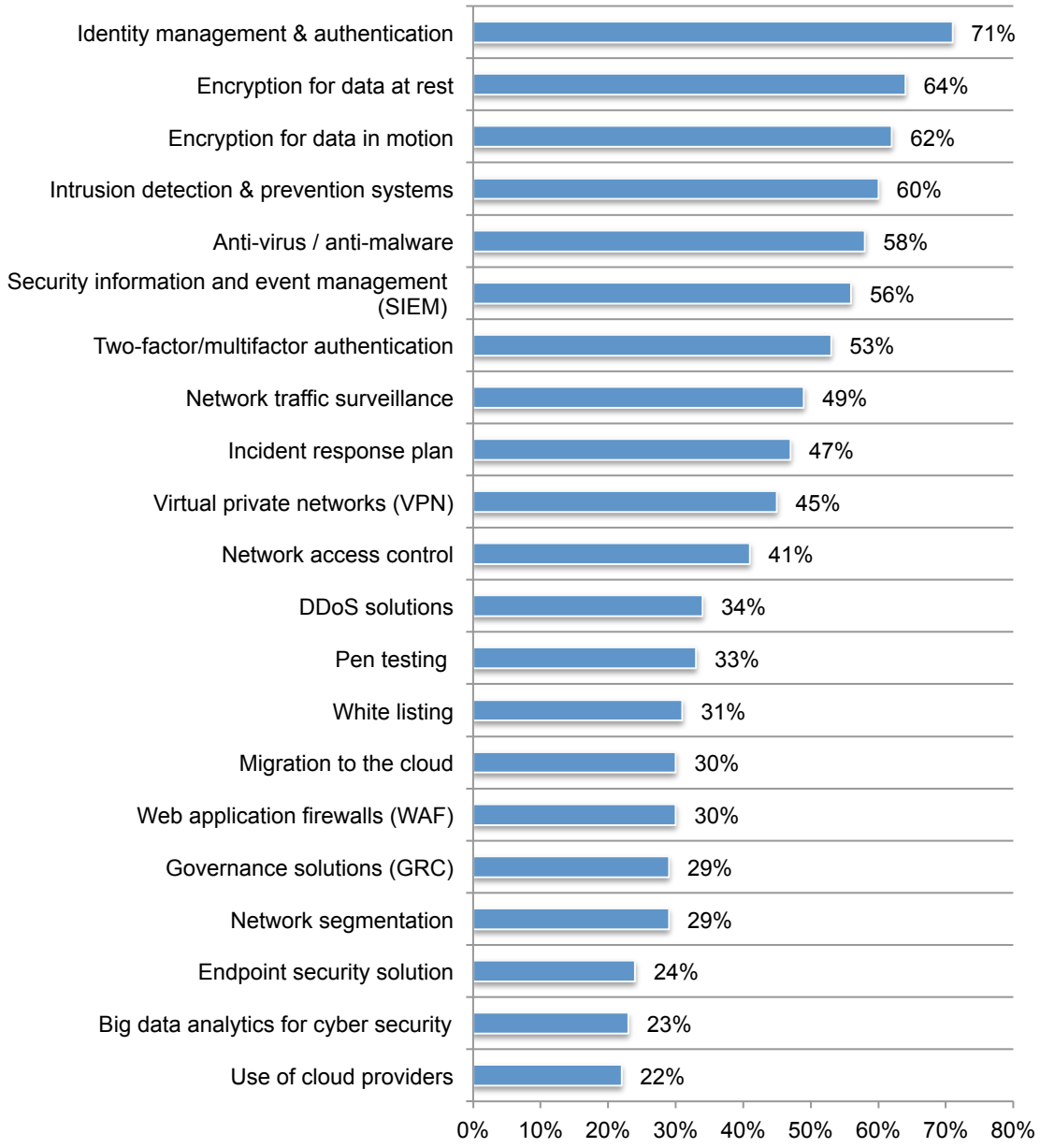
Figure 16. How does your organization determine the qualifications or expertise of personnel who manage cybersecurity risk?
More than one response permitted



Security spending and investment

Most organizations are measuring the effectiveness of technologies deployed. This year, 55 percent of respondents say their organizations are measuring the effectiveness of investments in technology to ensure that they achieve their security objectives, an increase from 51 percent of respondents in the 2016 study. As shown in Figure 17, the technologies considered most effective are: identity management and authentication (71 percent of respondents) and encryption for data at rest (64 percent of respondents).

Figure 17. Which security technologies and services are most effective in achieving security objectives?
More than one response permitted



Healthcare organizations are responding to cybersecurity risks with budget increases. On average, healthcare organizations represented in this research are spending $30 million on IT, an increase from $23 million in 2016. An average of 15 percent of the IT budget is allocated to information security.

Cybersecurity incidents are costly. Healthcare organizations spend an average of $4 million following a cyber attack**.** Table 1 provides a breakdown of the cost of a cybersecurity compromise. As shown, the highest costs are related to remediation and technical support activities and the disruption to normal operations because of system availability problems.

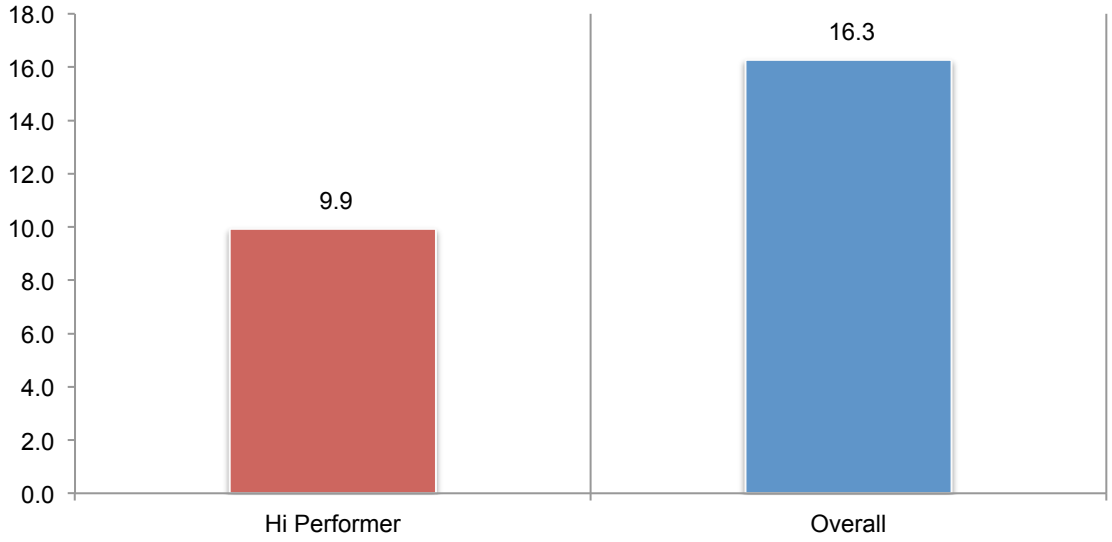
Table 1. The average cost of cybersecurity compromise	Allocated value
Remediation & technical support activities, including forensic investigations, incident response activities, help desk and customer service operations	$1,039,662
Users' idle time and lost productivity because of downtime or system performance delays	$759,753
Disruption to normal operations because of system availability problems	$959,688
Damage or theft of IT assets and infrastructure	$799,740
Reputation loss and brand damage	$439,857
Total	$3,998,700

Lessons from high-performing healthcare organizations

As part of the research, we did a special analysis of those respondents (59 respondents out of the total sample of 627 respondents) who rated their organizations' effectiveness in mitigating risks, vulnerabilities and attacks against their organizations as very high (9+ on a scale of 1 = low effectiveness to 10 = high effectiveness. These respondents are referred to as high performers.

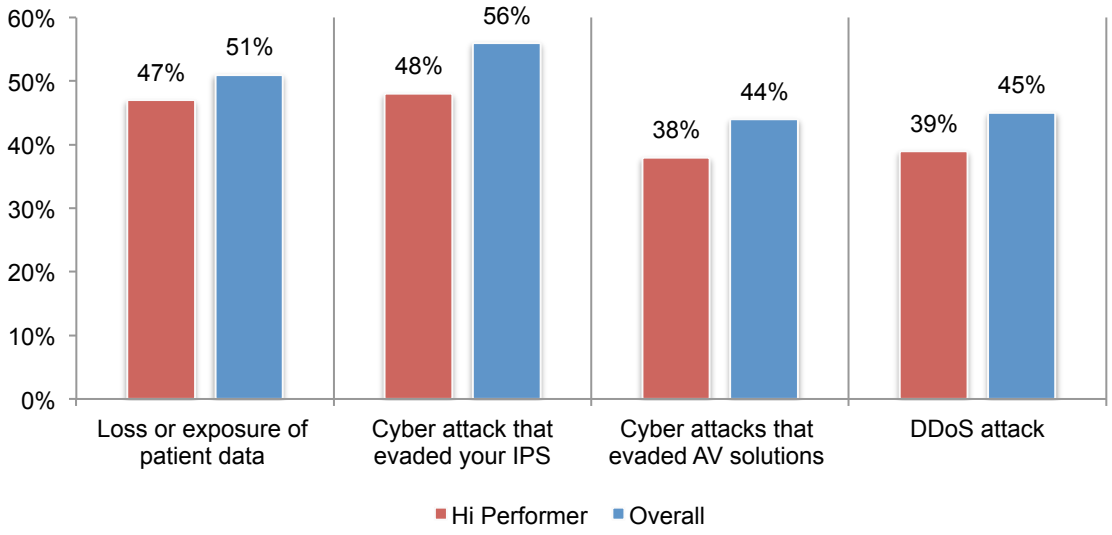
High-performing organizations are able to significantly reduce cyber attacks. As shown in Figure 18, organizations that self-report their cybersecurity posture is highly effective are less likely to have a data breach or cyber attack.

Figure 18. How many cyber attacks has your organization experienced over the past 12 months?
Extrapolated value reported



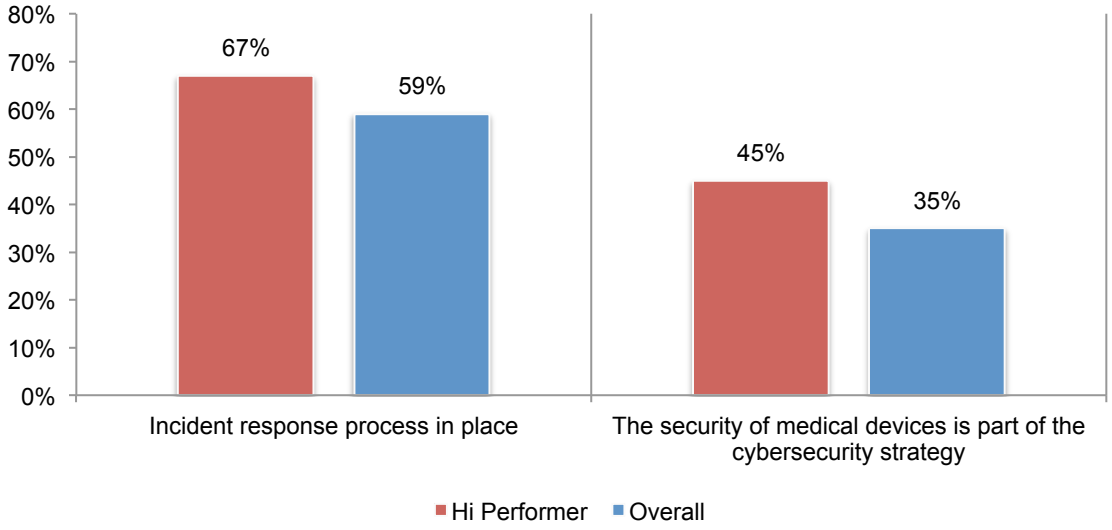
Further, they are better able to prevent the loss or exposure of patient data, DDoS attacks and other attacks that evade their IPS and AV solutions, as shown in Figure 19.

Figure 19. Has your organization experienced a data breach or other types of cyber attack?
Yes responses reported



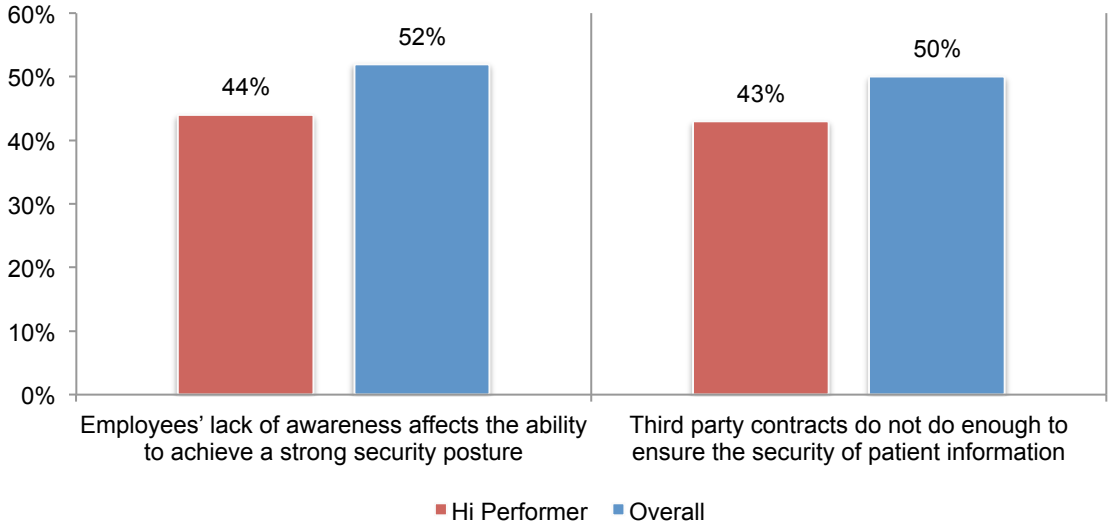
High performing organizations are more likely to have an incident response plan and a strategy for the security of medical devices. As shown in Figure 20, contributing to their stronger cybersecurity posture is having an incident response plan in place and including medical device security as part of their cybersecurity strategy.

Figure 20. Differences in having an incident response plan and a strategy for securing medical devices
Yes responses reported



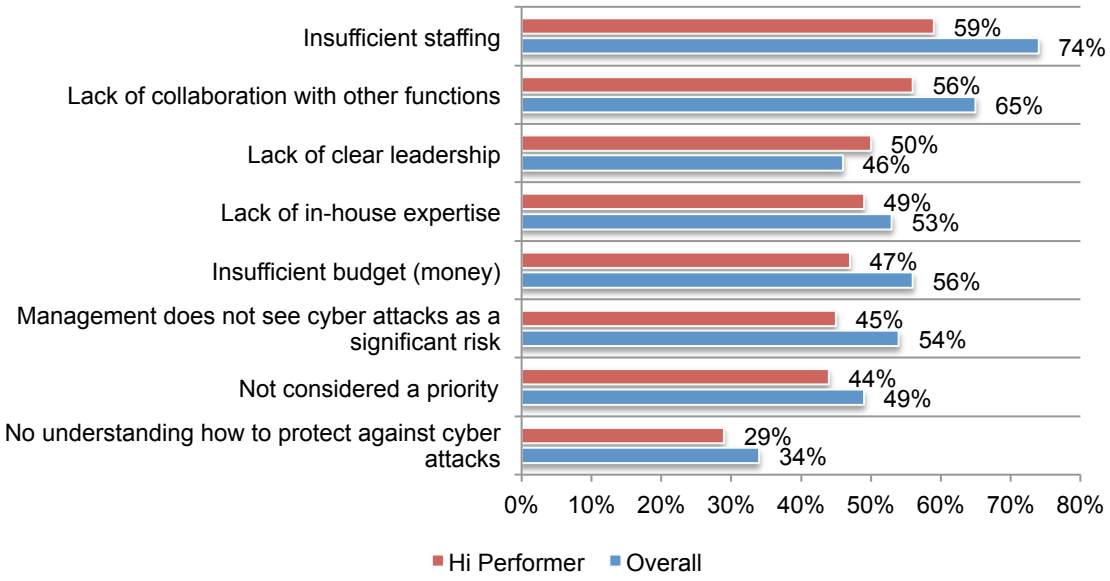
High-performing organizations are better at increasing employee awareness about cybersecurity risks. As discussed previously, employee errors are what respondents say are the biggest threat to their organizations. According to Figure 21, high-performing organizations are more confident in their ability to increase awareness about threats (44 percent of respondents vs. 52 percent of respondents). They also are more positive about the ability to ensure third-party contracts safeguard the security of patient information (43 percent of respondents vs. 50 percent of respondents).

Figure 21. Perceptions about the cybersecurity posture of their organizations
Strongly agree and Agree responses combined



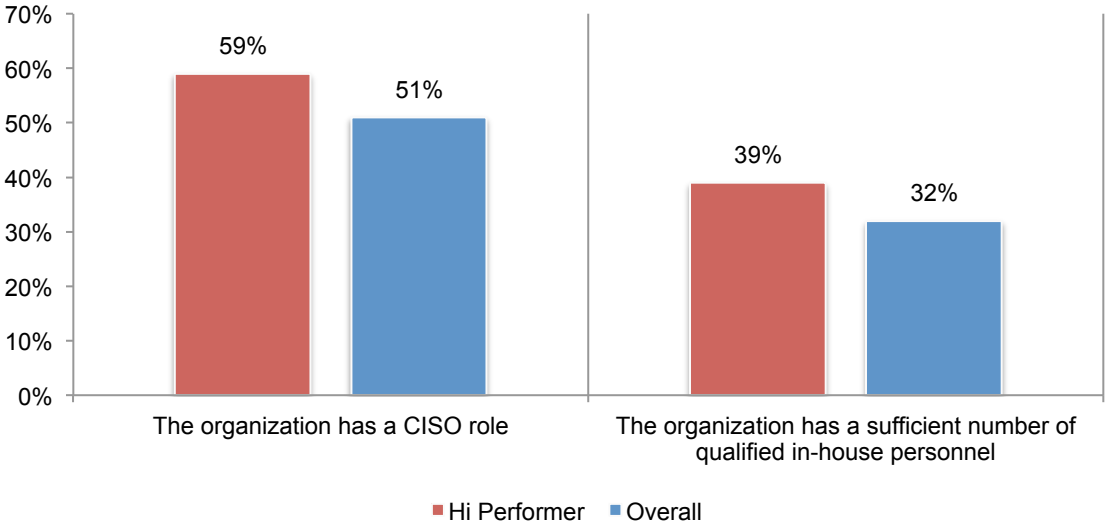
Insufficient staffing is not as big a challenge for high performing organizations. According to Figure 22, high performing organizations are less likely to consider insufficient staffing, collaboration with other functions, insufficient budget and management's lack of recognition of the risk of cyber attack as challenges

Figure 22. What challenges keep your organization's cybersecurity from being fully effective?
More than one response permitted



High-performing organizations are more likely to have the necessary in-house expertise. According to Figure 23, 59 percent of respondents in high-performing organizations have a CISO. Although it is still low, more high-performing organizations have sufficient qualified in-house personnel (39 percent of respondents vs. 32 percent of respondents).

Figure 23. Does your organization have enough qualified personnel and a CISO?
Yes responses reported



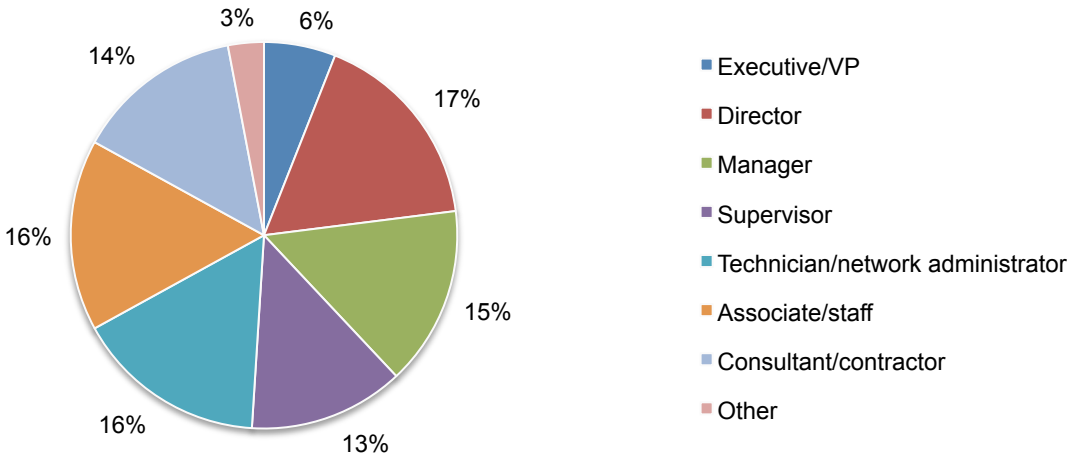
Part 3. Methods and Limitations

A sampling frame of 17,300 individuals who are IT and IT security practitioners, in a variety of healthcare organizations that are subject to HIPAA, were selected as participants in the research. Table 1 shows 703 total returns. Screening and reliability checks required the removal of 76 surveys. Our final sample consisted of 627 surveys, or a 3.6 percent response rate.

Table 2. Sample response	Freq	Pct%
Total sampling frame	17,300	100.0%
Total returns	703	4.1%
Rejected or screened surveys	76	0.4%
Final sample	627	3.6%

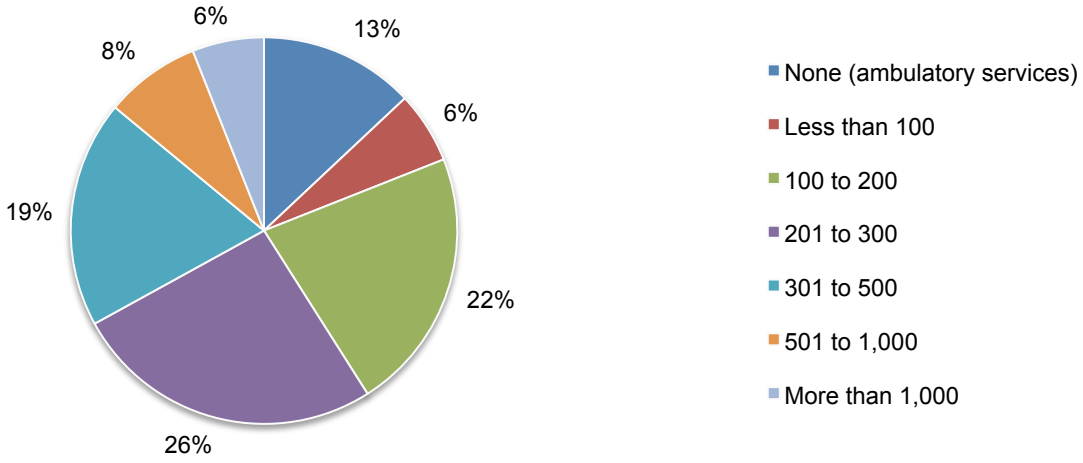
Pie Chart 1 summarizes the approximate position or organizational level of respondents in our study. As can be seen, half of the respondents (51 percent) are at or above the supervisory level.

Pie Chart 1. Distribution of respondents according to position or organizational level



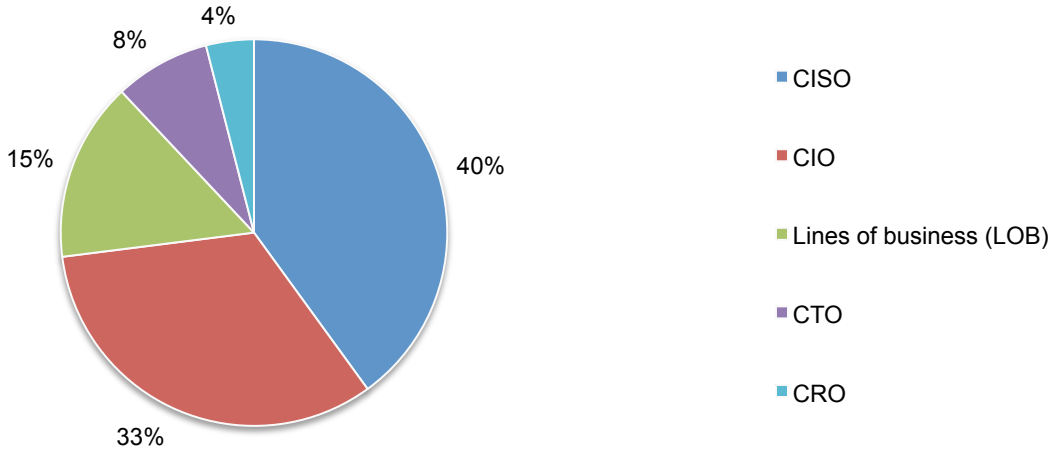
According to Pie Chart 2, the slightly more than half of respondents (59 percent) are located in organizations with headcounts of more than 200 employees.

Pie Chart 2. Distribution of respondents according to world headcount



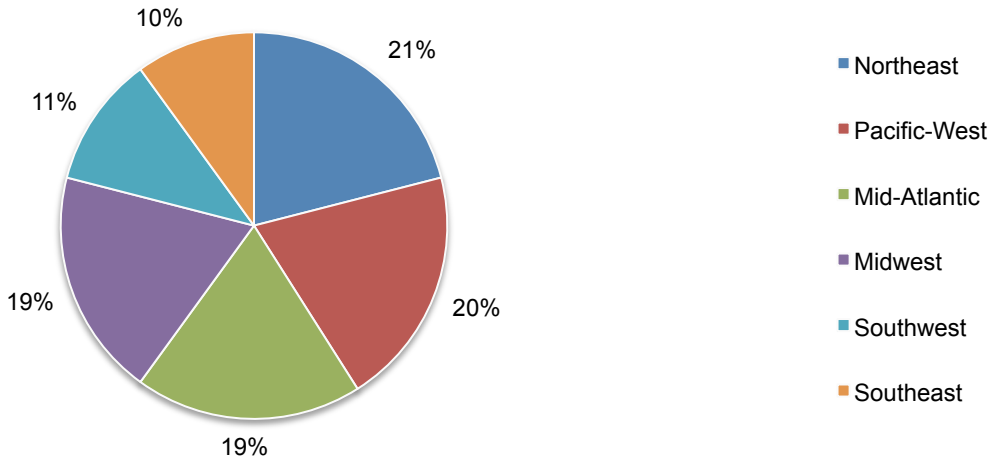
Pie Chart 3 shows that 40 percent of respondents identify the CISO as the person most accountable for the organization's cyber security strategy, followed by the CIO at 33 percent of respondents.

Pie Chart 3. Person most accountable for the organization's cyber security strategy



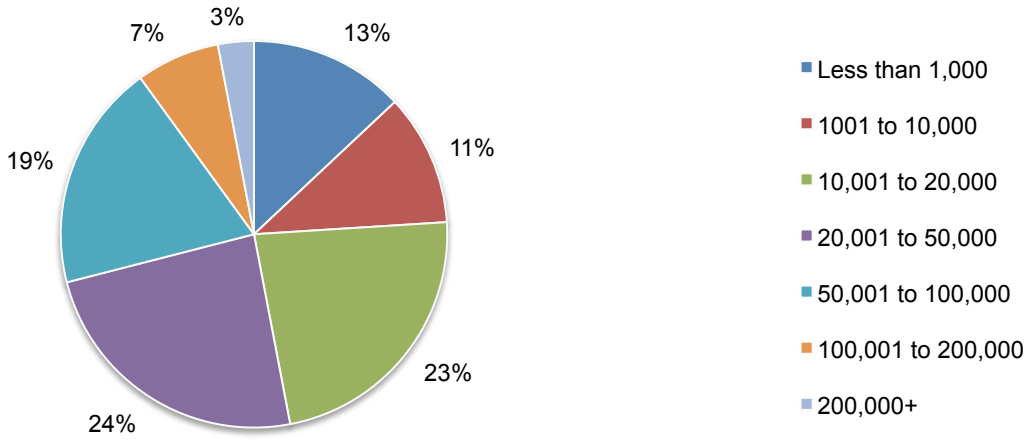
Pie Chart 4 identifies the United States region where respondents are located. Twenty-one percent of respondents are located in the Northeast, 20 percent are located in the Pacific-West region, 19 percent are located in both the Mid-Atlantic and Midwest regions.

Pie Chart 4. The region of the United States where the respondent's are located


10%
21%
11%
19%
20%
19%
Northeast
Pacific-West
Mid-Atlantic
Midwest
Southwest
Southeast

Pie Chart 5 identifies the number of network-connected devices. The majority of respondents (76 percent) indicate their organizations have more than 10,000 network-connected devices.

Pie Chart 5. The number of network connected devices



Limitations

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. We also acknowledge bias caused by compensating subjects to complete this research within a holdout period.

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

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 between December 14, 2017 to January 15, 2018.

Survey response	Freq	Pct%
Total sampling frame	15,445	100.0%
Total returns	621	4.0%
Rejected or screened surveys	86	0.6%
Final sample	535	3.5%

S1. Is your organization a covered entity or business associate subject to HIPAA?	Pct%
Covered entity	64%
Business associate	36%
No (Stop)	0%
Total	100%

S2. Which of the following best describes your role in managing the IT function within your organization? Check all that apply.	Pct%
Setting IT priorities	77%
Determining IT strategy	76%
Managing IT budgets	75%
Selecting vendors and contractors	71%
Evaluating program performance	66%
Managing risk	58%
Bolstering IT security	57%
Overseeing governance and compliance	50%
None of the above [Stop]	0%

Part I: Organizational characteristics: Please select the category that best describes your role and your organization.	
Q1a. What best describes your organization:	Pct%
Public healthcare provider	8%
Private healthcare provider	17%
Government agency	16%
Health insurer	15%
Healthcare clearinghouse	8%
Data / claims processor	4%
IT services/cloud services	7%
Medical devices & products	8%
Pharmaceuticals	8%
Government agency	6%
Transcription or other medical related services	3%
Other	0%
Total	100%

Q1b. What best describes your position or organizational level?	Pct%
Executive/VP	6%
Director	18%
Manager	16%
Supervisor	13%
Technician/network administrator	14%
Associate/staff	15%
Consultant/contractor	15%
Other	4%
Total	100%

Q1c. What headcount of your organization?	Pct%
< 100	8%
101 to 200	25%
201 to 300	22%
301 to 400	20%
401 to 500	21%
>501	4%
Total	100%

Q1d. Who is most accountable for your organization's cyber security strategy?	Pct%
CIO	40%
CTO	13%
CISO	38%
CRO	6%
Other	2%
Total	100%

Q1e. Please indicate the region of the United States where you are located.	Pct%
Northeast	21%
Mid-Atlantic	19%
Midwest	18%
Southeast	9%
Southwest	11%
Pacific-West	21%
Total	100%

Q1f. How many network connected devices does your organization have?	Pct%
< 100	4%
101 to 200	16%
201 to 300	22%
301 to 400	22%
401 to 500	20%
501 to 1,000	15%
> 1,000	2%
Total	100%

Q2. What security threats is your organization most concerned about? Please select the top three.	Pct%
Employee-owned mobile devices or BYOD	76%
Mobile device insecurity	72%
Use of public cloud services	71%
Unsecure medical devices	77%
Business associate misuse of patient data	68%
Employee negligence or error	57%
Malicious insiders	62%
Cyber attackers	77%
Identity thieves	73%
Insecure mobile apps (eHealth)	69%
System failures	79%
Process failures	65%
Other	10%

Q3. Which of these types of incidents did your organization experience? Please check all that apply.	Pct%
Exploit of existing software vulnerability greater than 3 months old	78%
Web-borne malware attacks	75%
Exploit of existing software vulnerability less than 3 months old	70%
Spear phishing	69%
Lost or stolen devices	61%
SQL injection	56%
Zero day attacks	50%
Spyware	50%
Clickjacking	49%
Botnet attacks	43%
Rootkits	41%
DDoS	36%
Advanced persistent threats (APT) / targeted attacks	34%
Other	15%

Q4a. Does your organization have an incident response process in place?	Pct%
Yes	50%
No	50%
Total	100%

Q4b. Who is involved in the incident response process? Please check all that apply.	Pct%
Information security	40%
Corporate counsel/compliance	37%
Risk management	29%
Information technology	24%
Privacy office	22%
Security	14%
Human Resources	11%
Other	7%

Q5. Will changes in HIPAAHITECH regulations change assessment requirements and compliance?	Pct%
Yes	29%
No	56%
Unsure	15%
Total	100%

Q6. What types of information do you believe hackers are most interested in stealing? Please select all that apply.	Pct%
Patient medical records	81%
Patient billing information	64%
Clinical trial and other research information	50%
Employee information including payroll data	45%
Accounting and financial information	39%
Email content and attachments	29%
Administrative and scheduling information	19%
Productivity applications	16%
Other	10%

Q7. Is the security of medical devices part of your cyber security strategy?	Pct%
Yes	27%
No	59%
Unsure	14%
Total	100%

Part 2. Attributions: Please rate the following statements from strongly agree to strongly disagree using the scale below each item.	
Q8a. Employee negligence affects our ability to achieve a strong security posture	Pct%
Strongly agree	22%
Agree	24%
Unsure	29%
Disagree	17%
Strongly disagree	8%
Total	100%

Q8b. Business Associate Agreements do not do enough to ensure the security of patient information.	Pct%
Strongly agree	18%
Agree	27%
Unsure	28%
Disagree	17%
Strongly disagree	10%
Total	100%

Q8c. New technologies and trends such as cloud, mobile, big data and the Internet of Things increase the vulnerability and threats to patient information.	Pct%
Strongly agree	18%
Agree	33%
Unsure	19%
Disagree	20%
Strongly disagree	9%
Total	100%

Q8d. Legacy systems increase the vulnerability and threats to patient information.	Pct%
Strongly agree	16%
Agree	36%
Unsure	27%
Disagree	10%
Strongly disagree	11%
Total	100%

Part 3: Your organization's security posture	
Q9. How would you rate your organization's cyber security posture (in terms of its effectiveness at mitigating risks, vulnerabilities and attacks across the enterprise)? 1 = not effective to 10 = very effective	Pct%
1 or 2	13%
3 or 4	24%
5 or 6	30%
7 or 8	28%
9 or 10	5%
Total	100%

Q10. What challenges keep your organization's cyber security posture from being fully effective? Please select all that apply.	Pct%
Lack of collaboration with other functions	76%
Insufficient staffing	73%
Insufficient budget (money)	65%
Not considered a priority	65%
Management does not see cyber attacks as a significant risk	61%
Lack of clear leadership	53%
Lack of in-house expertise	47%
No understanding how to protect against cyber attacks	39%

Part 4: Cyber attack experience	
Q11. How many cyber attacks has your organization experienced over the past 12 months?	Pct%
None	32%
1 to 5	19%
6 to 10	15%
11 to 25	10%
26 to 50	6%
51 to 100	3%
More than 100	1%
Unsure	13%
Total	100%

Q12. Has your organization experienced an incident involving the loss or exposure of patient information in the past 12 months?	Pct%
Yes	48%
No	26%
Unsure	26%
Total	100%

Q13a. Has your organization ever experienced situations when cyber attacks have evaded your intrusion prevention systems (IPS)?	Pct%
Yes	49%
No	23%
Unsure	27%
Total	100%

Q13b. Has your organization ever experienced situations when cyber attacks have evaded your anti-virus (AV) solutions and/or other traditional security controls?	Pct%
Yes	37%
No	39%
Unsure	25%
Total	100%

Q13c. Has your organization every benefited from HIPAA/HITECH notification rules when a data breach involving protected health information (PHI) is encrypted?	Pct%
Yes	27%
No	39%
Unsure	35%
Total	100%

Q14. Does your organization have systems and controls in place to detect and stop Advanced Persistent Threats (APTs)?	Pct%
Yes	26%
No	52%
Unsure	21%
Total	100%

Q15. How many separate APT-related incidents did your organization experience over the past 12 months?	Pct%
None	24%
1 to 2	25%
3 to 4	12%
5 to 6	5%
7 to 8	9%
9 to 10	7%
More than 10	5%
Unsure how to identify incidents as APTs	13.1%
Total	100%

Q16. What happened to your organization as a result of the APTs or zero day threats it experienced? Please select all that apply.	Pct%
IT downtime	63%
Inability to provide services	46%
Exfiltration of classified or sensitive information	44%
Theft of personal information	27%
Damage to software (source code)	19%
Damage to IT infrastructure	17%
Destruction of information asset	16%
Nothing happened	15%
Other (please specify)	10%

Q17a. Did your organization experience a denial of service (DDoS) attack that caused a disruption to operations and/or system downtime?	Pct%
Yes	37%
No	53%
Unsure	10%
Total	100%

Q17b. If yes, how many such attacks occurred in the past 12 months?	Pct%
None	27%
1 to 2	27%
3 to 4	12%
5 to 6	9%
7 to 8	6%
9 to 10	3%
More than 10	2%
Unsure	14%
Total	100%

Q17c. If yes, how much did disruptions and system downtimes cost your organization in the past 12 months.	Pct%
Zero	8%
Less than $10,000	11%
50,001 to $100,000	11%
100,001 to $250,000	10%
250,001 to $500,000	9%
500,001 to $1,000,000	7%
1,000,001 to $5,000,000	6%
5,000,001 to $10,000,000	2%
10,000,001 to $25,000,000	2%
More than $25,000,000	1%
Cannot estimate	34%
Total	100%

Part 5. Cost estimation	
Q18. To understand the relationship of each of the five categories to the total cost of a cyber security compromise, please allocate points to each category for a total of 100 points.	Allocated value
Remediation & technical support activities, including forensic investigations, incident response activities, help desk and customer service operations	171,151
Users' idle time and lost productivity because of downtime or system performance delays	399,106
Disruption to normal operations because of system availability problems	297,354
Damage or theft of IT assets and infrastructure	128,919
Reputation loss and brand damage	324,767
Total	1,321,297

Part 6. Security spending & investment	
Q19.What is your organization's approximate annual budget for IT (not including capital expenditures).	Pct%
Less than $1,000,000	4%
1,000,000 to $5,000,000	17%
5,000,001 to $10,000,000	24%
10,000,001 to $25,000,000	21%
25,000,001 to $50,000,000	21%
More than $50,000,000	12%
Cannot estimate	1%
Total	100%

Q20. What percentage of your organization's IT budget is dedicated to information security?	Pct%
Less than 5%	15%
5 to 10%	35%
11 to 15%	30%
16 to 20%	10%
21 to 30%	6%
31 to 40%	3%
More than 40%	0%
Total	100%

Q21a. Does your organization measure how effective investments in technology are in achieving your security objectives?	Pct%
Yes	51%
No	39%
Unsure	10%
Total	100%

Q21b. If yes, which of the following security technologies and services have been the most effective in helping your organization achieve its security objectives. Please select your **top eight choices**.	Pct%
Identity management & authentication	80%
Encryption for data at rest	77%
Encryption for data in motion	76%
Intrusion detection & prevention systems	74%
Anti-virus / anti-malware	68%
Security information and event management (SIEM)	67%
Network traffic surveillance	60%
Virtual private networks (VPN)	47%
Web application firewalls (WAF)	38%
Pen testing	31%
White listing	29%
Endpoint security solution	23%
Anti-DDoS solutions	17%
Wireless security solutions	16%
Next generation firewalls	16%
Governance solutions (GRC)	16%
Data tokenization technology	16%
Data loss prevention (DLP)	15%
Big data analytics for cyber security	15%
Other	17%

For more information about this study, please contact Ponemon Institute by sending an email to research@ponemon.org or calling us at 1.800.887.3118.

Ponemon Institute

Advancing Responsible Information Management

Ponemon Institute is dedicated to independent research and education that advances responsible information and privacy management practices within business and government. Our mission is to conduct high quality, empirical studies on critical issues affecting the management and security of sensitive information about people and organizations.

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.