Ponemon INSTITUTE

THE STATE OF CYBERSECURITY IN HEALTHCARE ORGANIZATIONS IN 2016

ESET ENJOY SAFER TECHNOLOGY®

The State of Cybersecurity in Healthcare Organizations in 2016

Independently conducted by Ponemon Institute LLC

Sponsored by ESET | Publication Date: February, 2016

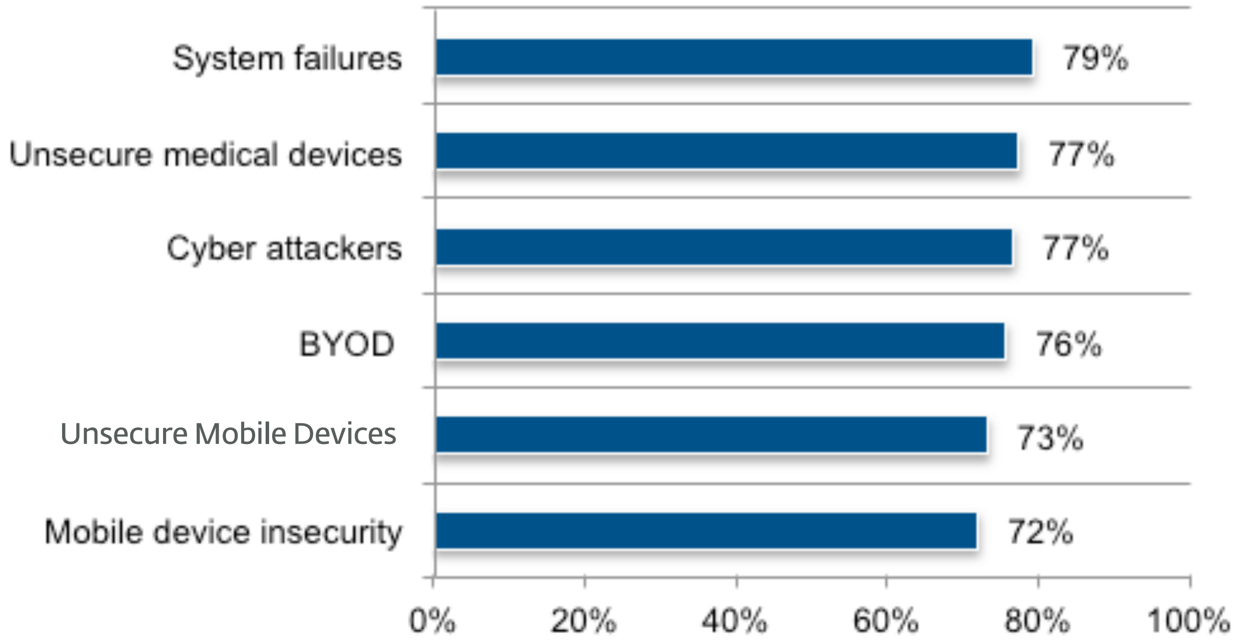
Part 1. Introduction

Healthcare organizations are in the cross hairs of cyber attackers as evidenced in the *2016 State of Cybersecurity in Healthcare Organizations Study* sponsored by ESET. On average, healthcare organizations represented in this research have had almost one cyber attack per month over the past 12 months. Almost half (48 percent) of respondents say their organizations have experienced an incident involving the loss or exposure of patient information during this same period, but 26 percent of respondents are unsure.

We surveyed 535 IT and IT security practitioners in a variety of healthcare organizations such as private and public healthcare providers and government agencies[1]. Sixty-four percent of respondents are employed in covered entities and 36 percent of respondents in business associates. Eighty-eight percent of organizations represented in this study have a headcount of between 100 and 500.

Figure 1. The top security threats for healthcare organizations

More than one response permitted



[1] A complete list of the healthcare organizations represented in this research is in the appendix of this report.

With cyber attacks against healthcare organizations growing increasingly frequent and complex, there is more pressure to refine cybersecurity strategies. Moreover, healthcare organizations have a special duty to secure data and systems against cyber hacks. The misuse of patient information and system downtime can not only put sensitive and confidential information at risk but the lives of patients as well.

As shown in Figure 1, healthcare organizations are struggling to deal with a variety of threats such as system failures (79 percent of respondents), unsecure medical devices (77 percent of respondents), cyber attackers (77 percent of respondents), employee-owned mobile devices or BYOD (76 percent of respondents), identity thieves (73 percent of respondents) and unsecure mobile device (72 percent of respondents). Despite citing unsecure medical devices as a top security threat, only 27 percent of respondents say their organization has the security of medical devices as part of their cybersecurity strategy.

The following are key findings from this research:

Healthcare organizations experience monthly cyber attacks. Healthcare organizations experience, on average, a cyber attack almost monthly (11.4 attacks on average per year) as well as the loss or exposure of sensitive and confidential patient information. However, 13 percent are unsure how many cyber attacks they have endured.

Almost half of respondents (48 percent) say their organization experienced an incident involving the loss or exposure of patient information in the past 12 months. As a consequence, many patients are at risk for medical identity theft.

Exploits of existing software vulnerabilities and web-borne malware attacks are the most common security incidents. According to 78 percent of respondents, the most common security incident is the exploitation of existing software vulnerabilities greater than three months old. A close second, according to 75 percent of respondents, are web-borne malware attacks. This is followed by exploits of existing software vulnerability less than three months old (70 percent of respondents), spear phishing (69 percent of respondents) and lost or stolen devices (61 percent of respondents).

How effective are measures to prevent attacks? Forty-nine percent of respondents say their organizations experienced situations when cyber attacks have evaded their intrusion prevention systems (IPS) but many respondents (27 percent) are unsure. Thirty-seven percent of respondents say their organizations have experienced cyber attacks that evaded their anti-virus (AV) solutions and/or traditional security controls but 25 percent of respondents are unsure.

On average, organizations have an APT incident every three months. Only 26 percent of respondents say their organizations have systems and controls in place to detect and stop advanced persistent threats (APTs) and 21 percent are unsure. On average, over a 12-month period, organizations represented in this research had an APT attack about every 3 months (3.46 APT-related incidents in one year).

Sixty-three percent of respondents say the primary consequences of APTs and zero day attacks were IT downtime, followed by the inability to provide services (46 percent of respondents), which create serious risks in the treatment of patients. Forty-four percent of respondents say these incidents resulted in the theft of personal information.

DDoS attacks have cost organizations on average $1.32 million in the past 12 months. T hirty-seven percent of respondents say their organization experienced a DDoS attack that caused a disruption to operations and/or system downtime about every four months and cost an average of $1.32 million. The largest cost component is lost productivity followed by reputation loss and brand damage.

Respondents are pessimistic about their ability to mitigate risks, vulnerabilities and attacks across the enterprise. Only 33 percent of respondents rate their organizations' cybersecurity posture as very effective. The primary challenges to becoming more effective are a lack of collaboration with other functions (76 percent of respondents), insufficient staffing (73 percent of respondents), not enough money and not considered a priority (both 65 percent of respondents).

Organizations are evenly divided in the deployment of an incident response plan. Fifty percent of respondents say their organization has an incident response plan in place. Information security and corporate counsel/compliance are the individuals most involved in the incident response process, according to 40 percent of respondents and 37 percent of respondents, respectively.

Technology poses a greater risk to patient information than employee negligence. The majority of respondents say legacy systems (52 percent of respondents) and new technologies and trends such as cloud, mobile, big data and the Internet of Things are both increasing vulnerability and threats to patient information. Respondents are also concerned about the impact of employee negligence (46 percent of respondents) and the ineffectiveness of business associate agreements to ensure the security of patient information (45 percent of respondents).

System failures are the security threat healthcare organizations worry most about. Seventy-nine percent of respondents say this is one of the top three threats facing their organizations followed by 77 percent of respondents who say it is cyber attackers and unsecure medical devices. Employee-owned mobile devices in healthcare settings are also considered a significant threat for 76 percent of respondents. Once again respondents are more concerned about technology risks than employee negligence or error.

Hackers are most interested in stealing patient information. The most lucrative information for hackers can be found in patients' medical records, according to 81 percent of respondents. This is followed by patient billing information (64 percent of respondents) and clinical trial and other research information (50 percent of respondents).

Healthcare organizations need a healthy dose of investment in technologies. On average, healthcare organizations represented in this research are spending $23 million on IT and an average of 12 percent is allocated to information security. Since an average of $1.3 million is spent annually just to deal with DDoS attacks, the business case can be made to increase technology investments to reduce the frequency of successful attacks.

Most organizations are measuring the effectiveness of technologies deployed. At this time, 51 percent of respondents say their organizations are measuring the effectiveness of investments in technology to ensure they achieve their security objectives. The technologies considered most effective are: identity management and authentication (80 percent of respondents) and encryption for data at rest (77 percent of respondents).

Part 2. Key findings

In this section, we provide an analysis of the key findings. The report is organized according to the following topics:

- Cyber attack experience of healthcare organizations
- The cybersecurity posture of healthcare organizations
- Security spending and investment

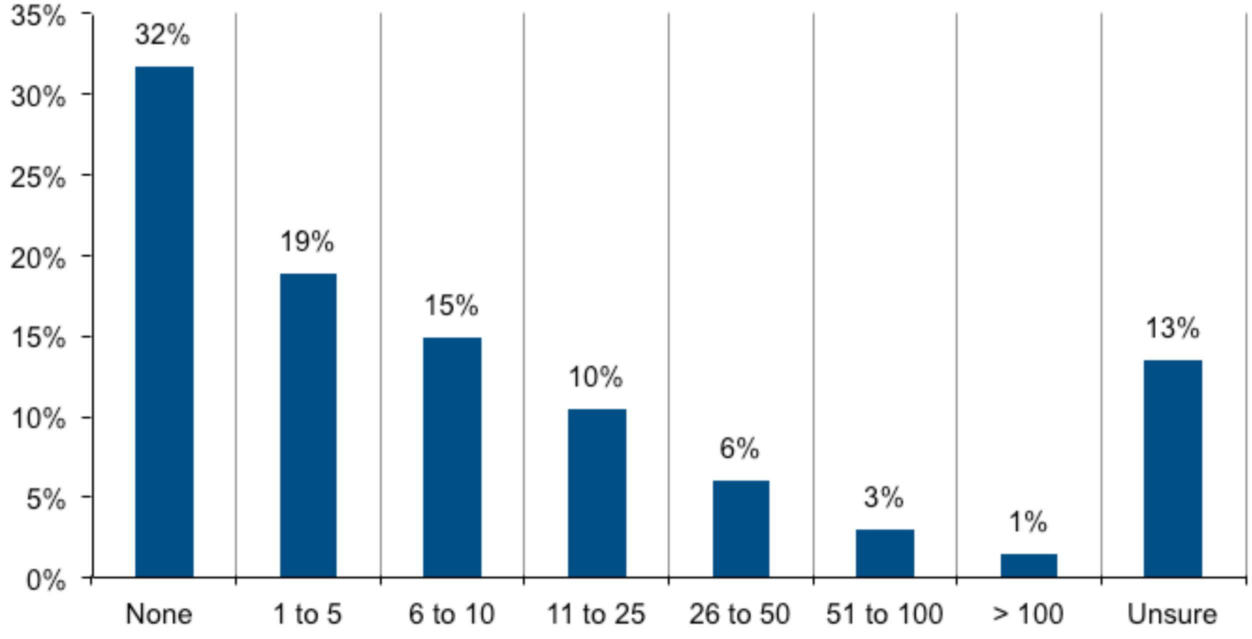
Cyber attack experience of healthcare organizations:

Healthcare organizations experience monthly cyber attacks. As shown in Figure 2, healthcare organizations experience on average a cyber attack almost monthly (11.4 attacks on average) as well as the loss or exposure of sensitive and confidential patient information. However, 13 percent are unsure how many cyber attacks they have endured.

Almost half of respondents (48 percent) say their organization experienced an incident involving the loss or exposure of patient information in the past 12 months. As a consequence, many patients are at risk for medical identity theft.

Figure 2. How many cyber attacks has your organization experienced over the past 12 months?

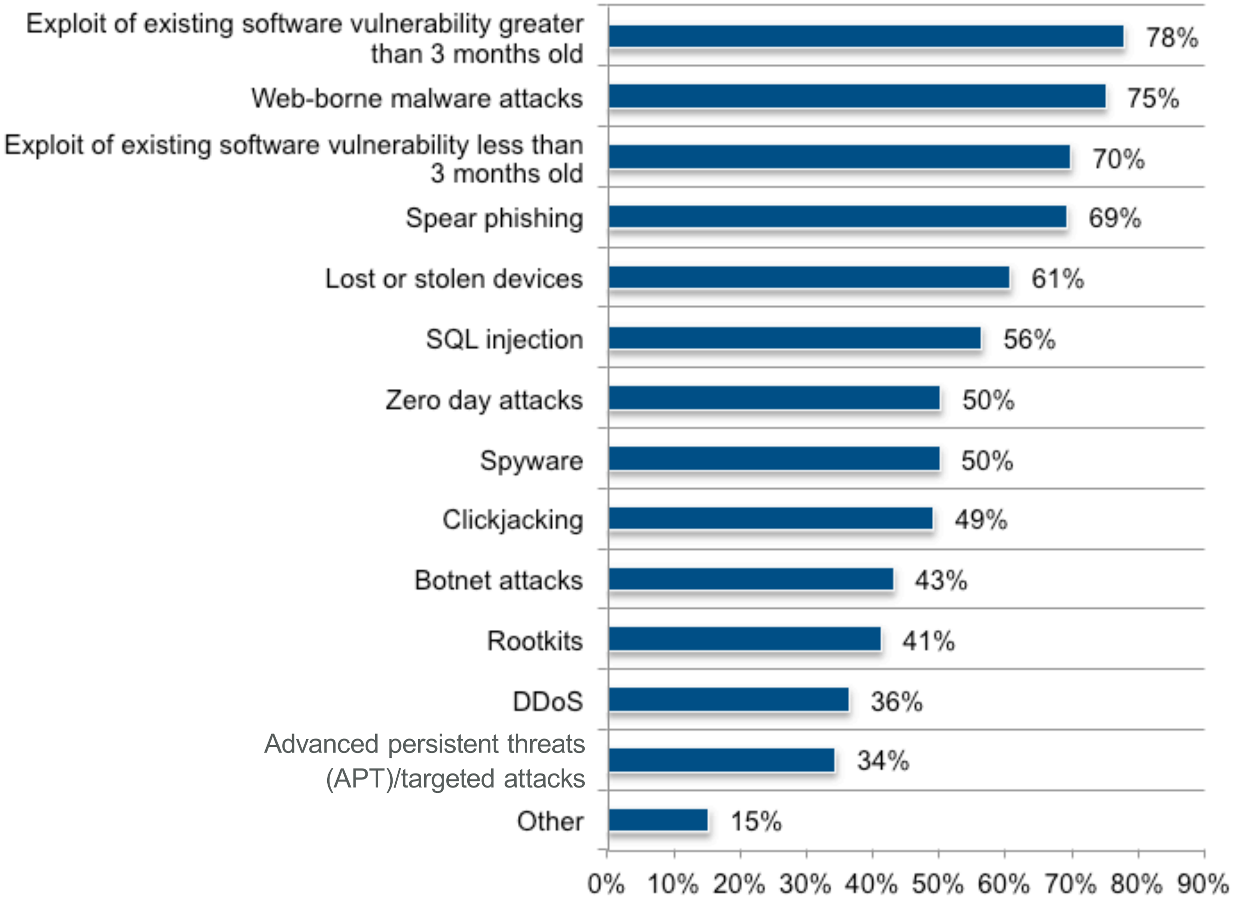
Extrapolated value = 11.4 attacks



Exploits of existing software vulnerabilities and web-borne malware attacks are the most common security incidents. According to 78 percent of respondents, the most common security incident is the exploitation of existing software vulnerabilities greater than three months old. A close second, according to 75 percent of respondents, are web-borne malware attacks. This is followed by exploits of existing software vulnerability less than three months old (70 percent of respondents), spear phishing (69 percent of respondents) and lost or stolen devices (61 percent of respondents), as shown in Figure 3.

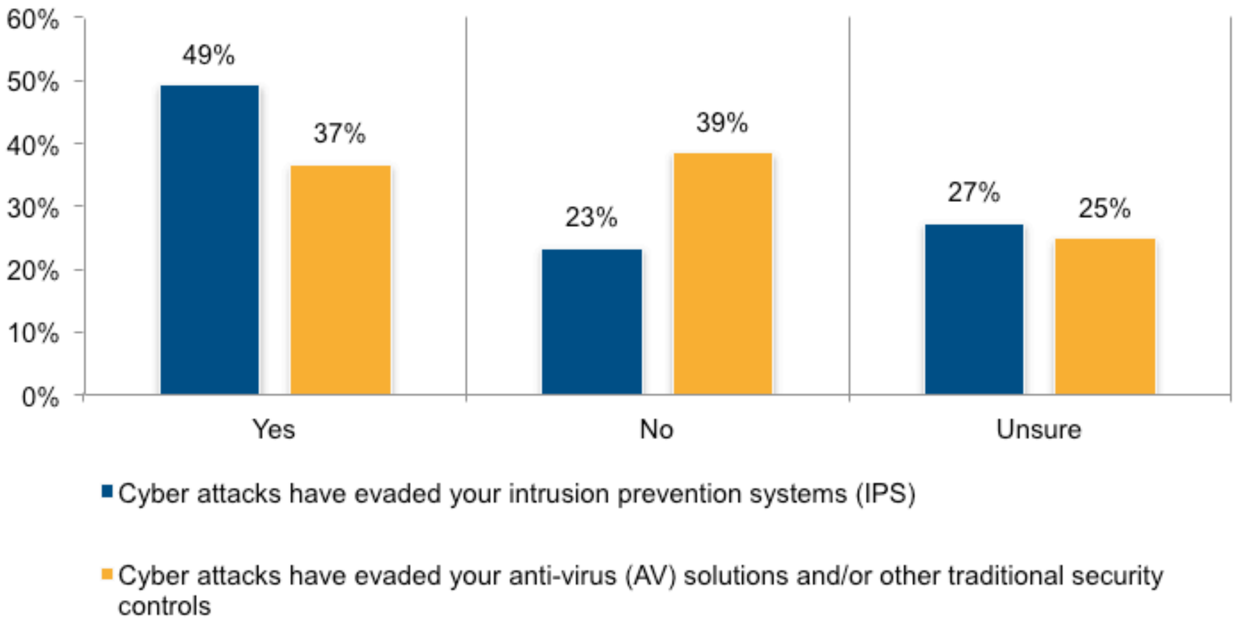
Figure 3. Which incidents did your organization experience?

More than one response permitted



How effective are measures to prevent attacks? As shown in Figure 4, 49 percent of respondents say their organizations experienced situations when cyber attacks have evaded their intrusion prevention systems (IPS), but many respondents (27 percent) are unsure. Thirty-seven percent of respondents say their organizations have experienced cyber attacks that evaded their anti-virus (AV) solutions and/or traditional security controls, but 25 percent of respondents are unsure.

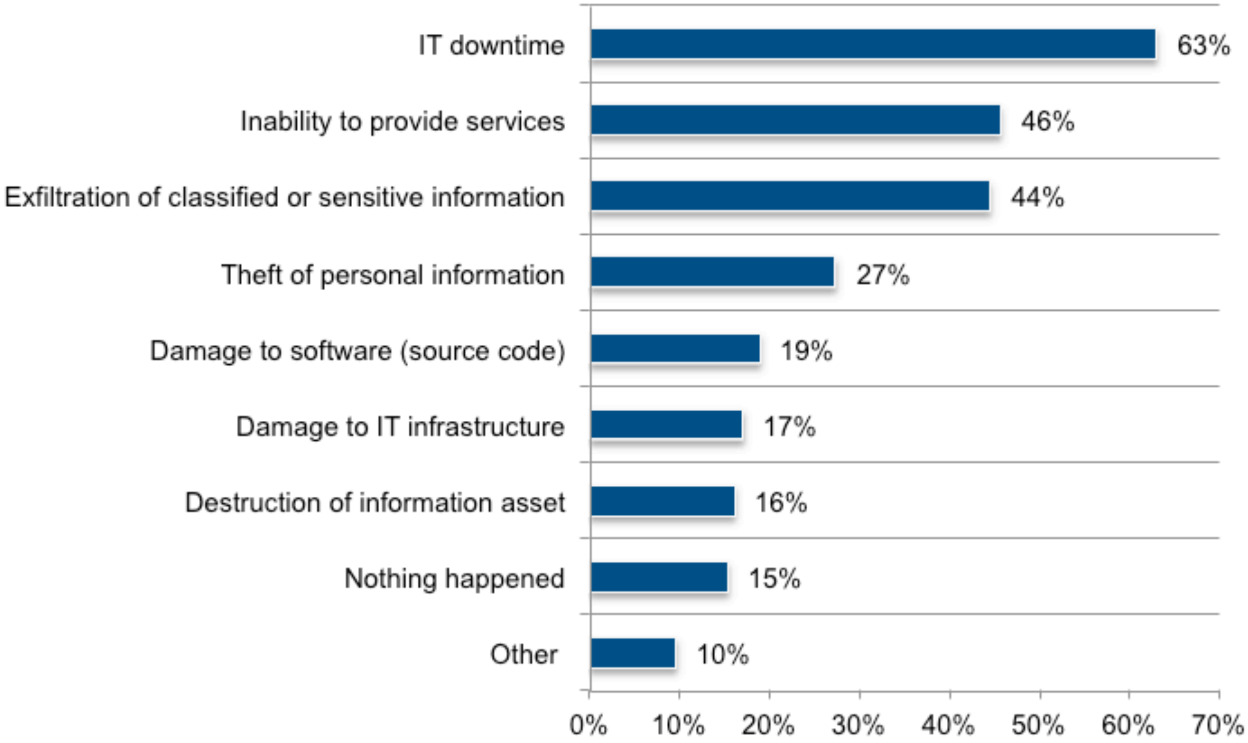
Figure 4. Has your organization experienced cyber attacks that evaded IPS, AV solutions and other security controls?



On average, organizations have an APT incident every three months. Only 26 percent of respondents say their organizations have systems and controls in place to detect and stop advanced persistent threats (APTs) and 21 percent are unsure. On average, over a 12-month period, organizations represented in this research had an APT attack about every 3 months (3.46 APT-related incidents in one year).

Figure 5. What happened as a result of the APTs or zero day threats?

More than one response permitted



As shown in Figure 5, 63 percent of respondents say the primary consequences of APTs and zero day attacks were IT downtime, followed by the inability to provide services (46 percent of respondents), which create serious risks in the treatment of patients. Forty-four percent of respondents say these incidents resulted in the theft of personal information.

DDoS attacks have cost organizations on average $1.32 million in the past 12 months. Thirty-seven percent of respondents say their organization experienced a DDoS attack that caused a disruption to operations and/or system downtime about every four months and cost an average of $1.32 million. The largest cost component is lost productivity followed by reputation loss and brand damage.

As shown in Table 1, this cost is determined by the following categories: remediation and 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) and reputation loss and brand damage ($324,767).

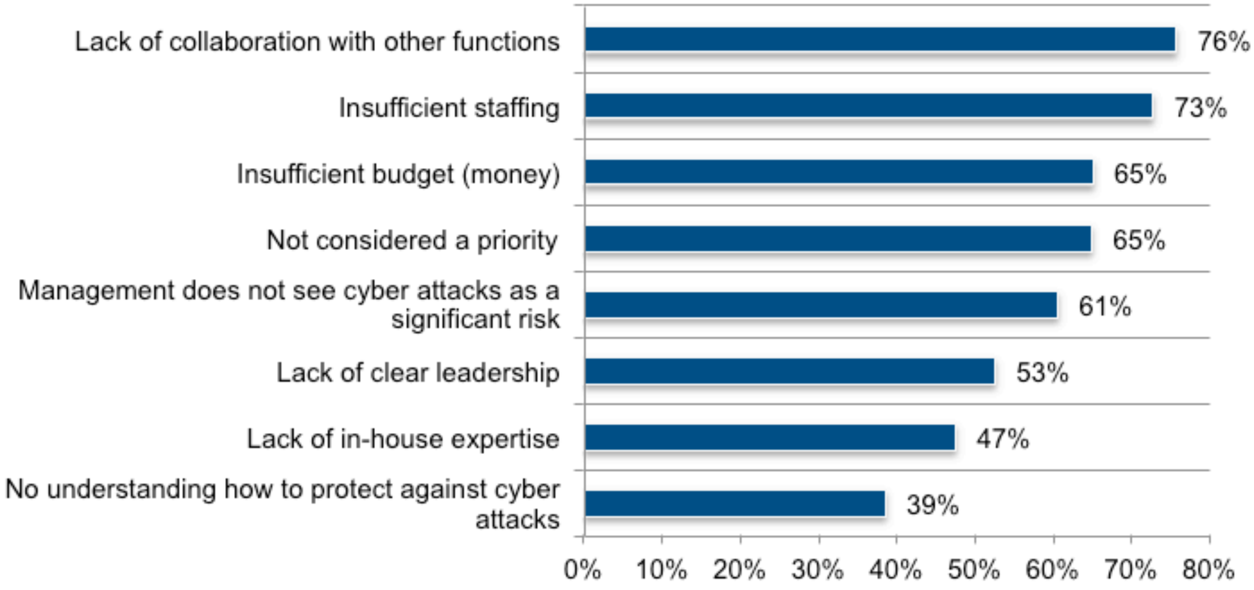
Table 1. The average cost of DDoS attacks	Allocated value
Users' idle time and lost productivity because of downtime or system performance delays	$399,106
Reputation loss and brand damage	$324,767
Disruption to normal operations because of system availability problems	$297,354
Remediation & technical support activities, including forensic investigations, incident response activities, help desk and customer service operations	$171,151
Damage or theft of IT assets and infrastructure	$128,919
Total	$1,321,297

The cybersecurity posture of healthcare organizations:

Respondents are pessimistic about their ability to mitigate risks, vulnerabilities and attacks across the enterprise. Only 33 percent of respondents rate their organizations' cybersecurity posture as very effective. As presented in Figure 6, the primary challenges to becoming more effective are a lack of collaboration with other functions (76 percent of respondents), insufficient staffing (73 percent of respondents), not enough money and not considered a priority (both 65 percent of respondents).

Figure 6. What challenges keep your organization's cybersecurity posture from being fully effective?

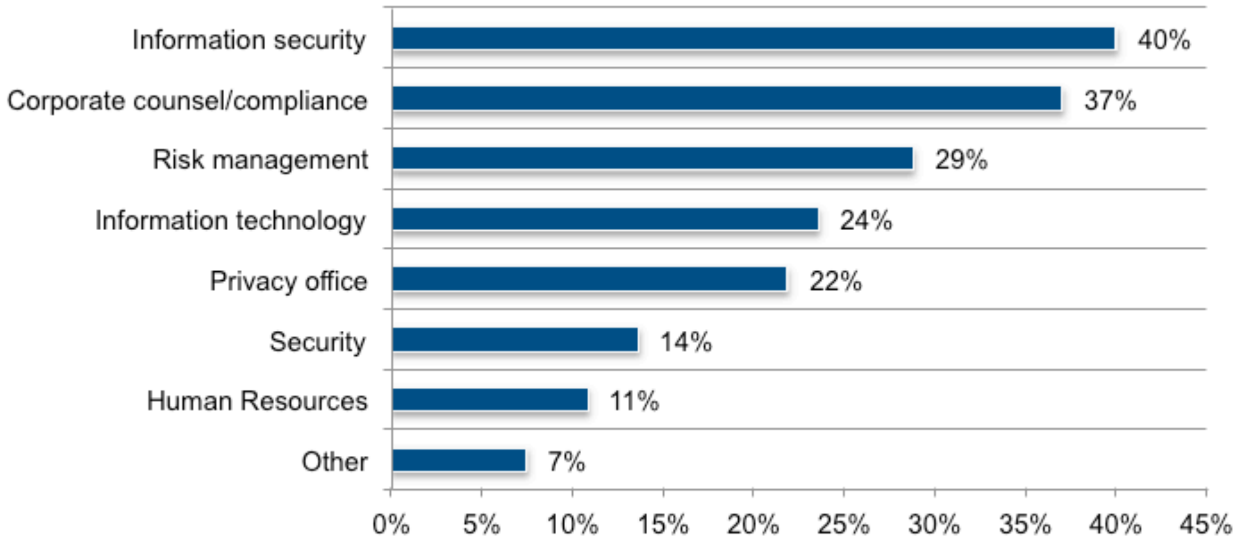
More than one response permitted



Organizations are evenly divided in the deployment of an incident response plan.
Fifty percent of respondents say their organization has an incident response plan in place. According to Figure 7, information security and corporate counsel/compliance are the individuals most involved in the incident response process, according to 40 percent of respondents and 37 percent of respondents, respectively.

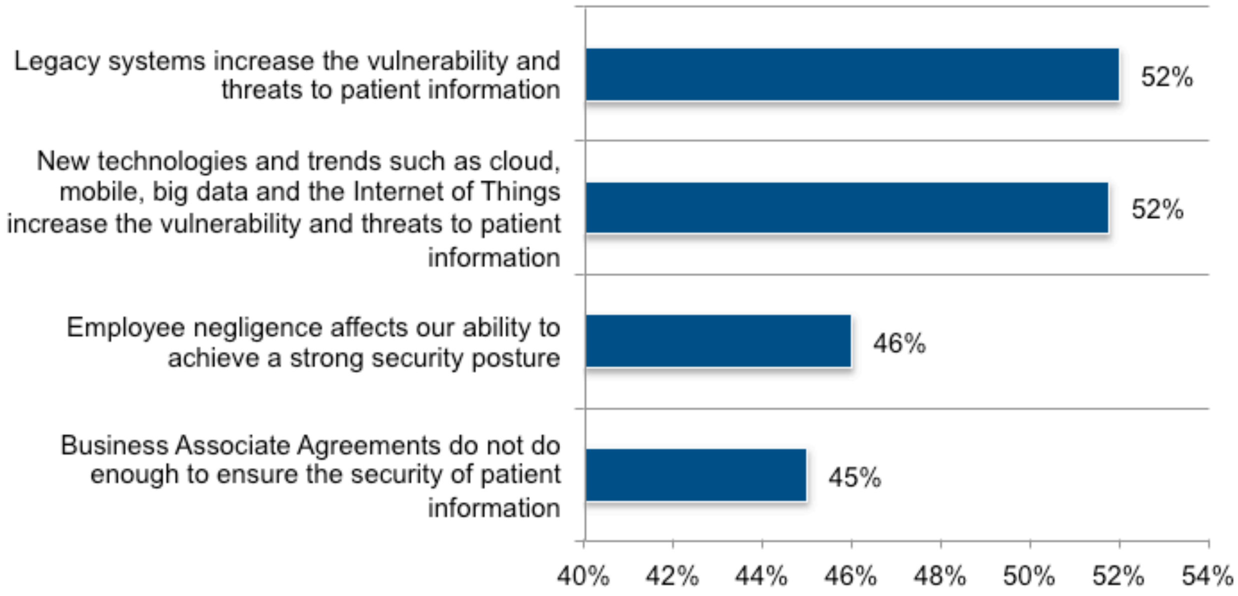
Figure 7. Who is involved in the incident response process?

More than one response permitted



Technology poses a greater risk to patient information than employee negligence.
As presented in Figure 8, the majority of respondents say legacy systems (52 percent of respondents), new technologies and trends such as cloud, mobile, big data and the Internet of Things are both increasing the vulnerability and threats to patient information. Respondents are also concerned about the impact of employee negligence (46 percent of respondents) and the ineffectiveness of business associate agreements to ensure the security of patient information (45 percent of respondents).

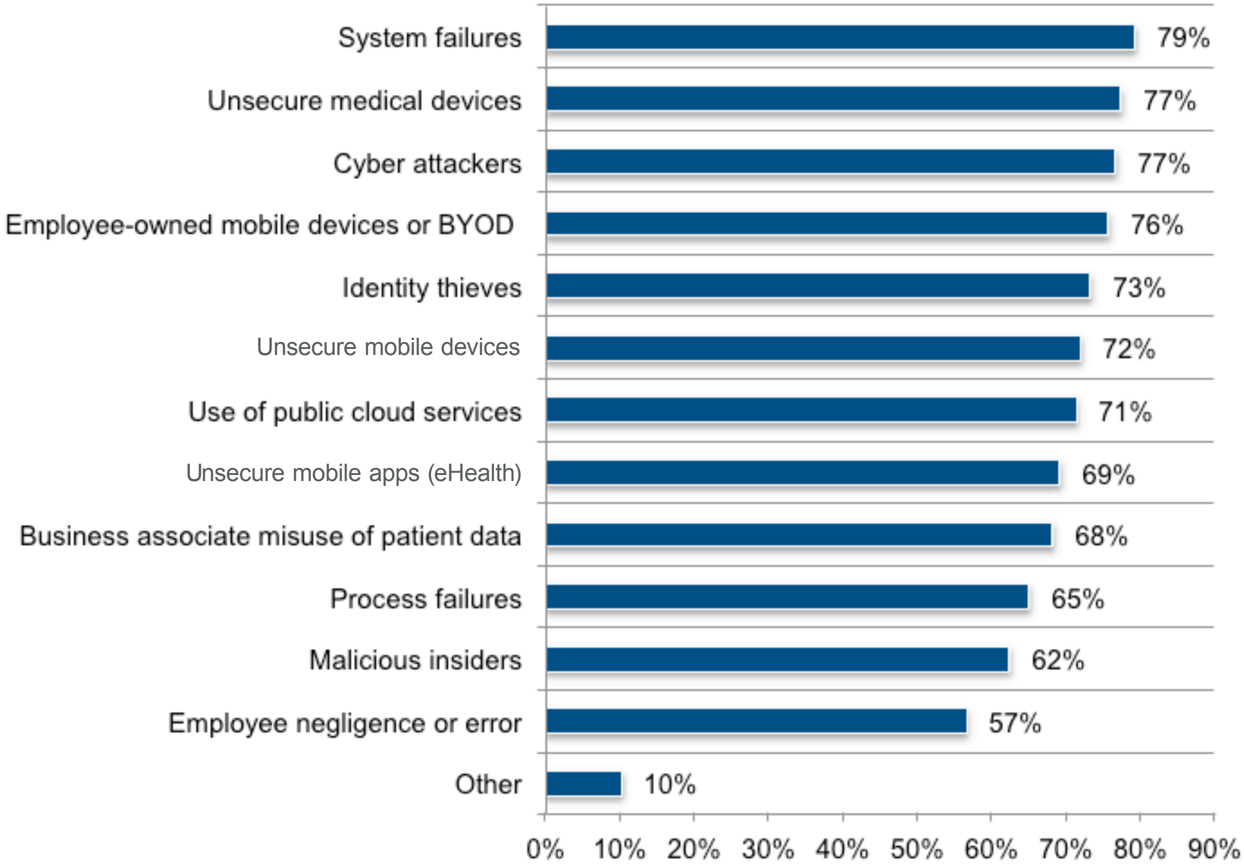
Figure 8. Perceptions about why patient information is at risk
Strongly agree and agree responses combined



System failures are the security threat healthcare organizations worry most about. As presented in Figure 9, 79 percent of respondents say this is one of the top three threats facing their organizations followed by 77 percent of respondents who say it is cyber attackers and unsecure medical devices. Employee-owned mobile devices in healthcare settings are also considered a significant threat for 76 percent of respondents. Once again, respondents are more concerned about technology risks than employee negligence or error.

Figure 9. What security threats is your organization most concerned about?

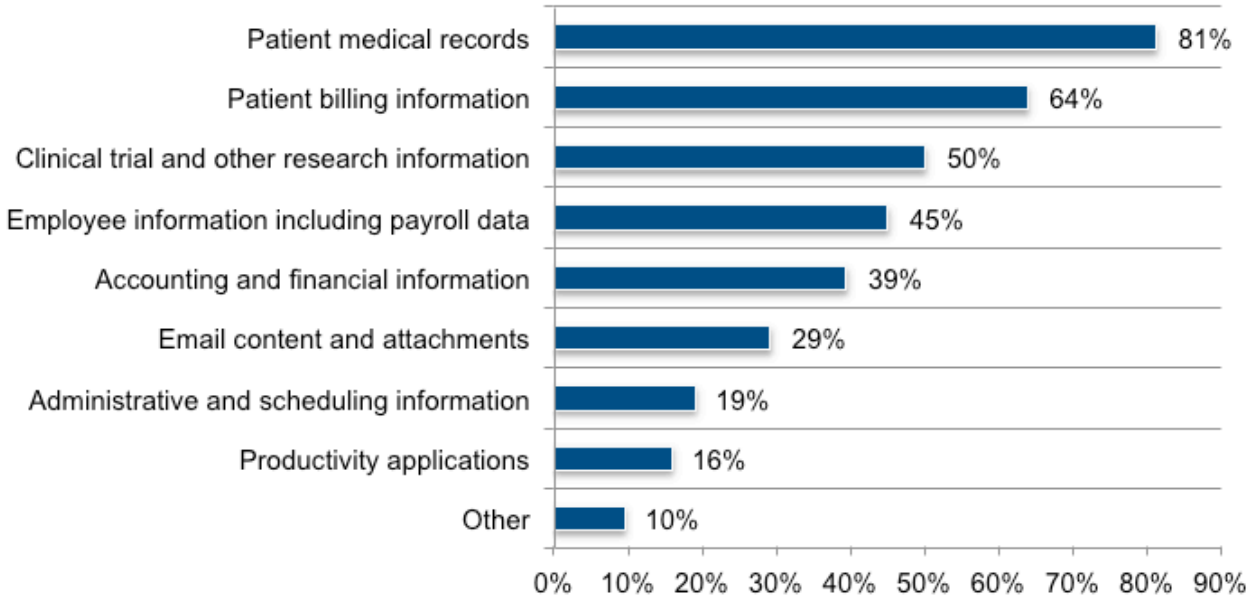
More than one response permitted



Hackers are most interested in stealing patient information. The most lucrative information for hackers can be found in patients' medical records, according to 81 percent of respondents (Figure 10). This is followed by patient billing information (64 percent of respondents) and clinical trial and other research information (50 percent of respondents).

Figure 10. What types of information do you believe hackers are most interested in stealing?

More than one response permitted



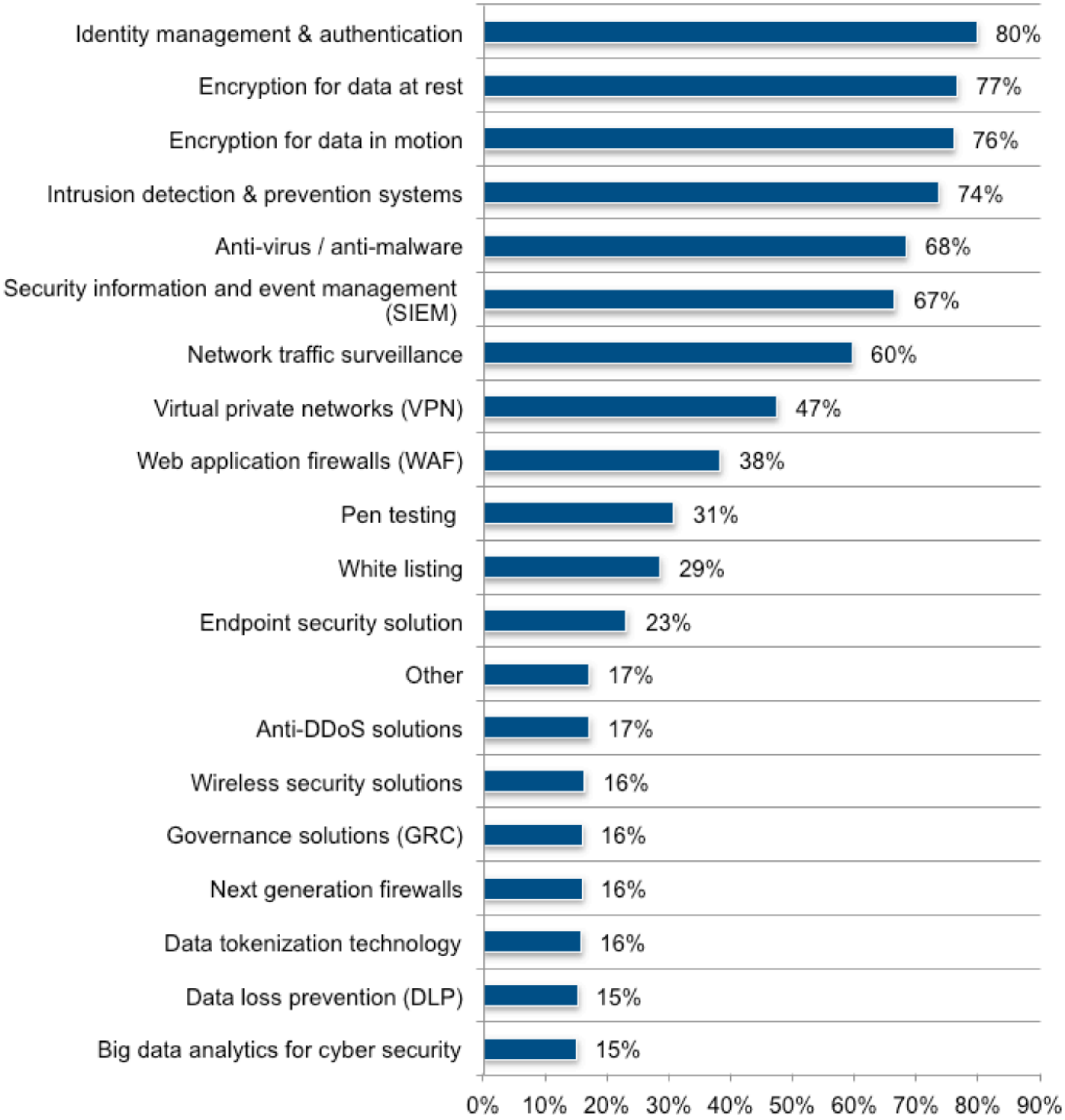
Security spending and investment:

Healthcare organizations need a healthy dose of investment in technologies. On average, healthcare organizations represented in this research are spending $23 million on IT and an average of 12 percent is allocated to information security. Since an average of $1.3 million is spent annually just to deal with DDoS attacks, the business case can be made to increase technology investments to reduce the frequency of successful attacks.

Most organizations are measuring the effectiveness of technologies deployed. At this time, 51 percent of respondents say their organizations are measuring the effectiveness of investments in technology to ensure they achieve their security objectives. As shown in Figure 11, the technologies considered most effective are: identity management and authentication (80 percent of respondents) and encryption for data at rest (77 percent of respondents).

Figure 11. Which security technologies and services are most effective in achieving security objectives?

More than one response permitted



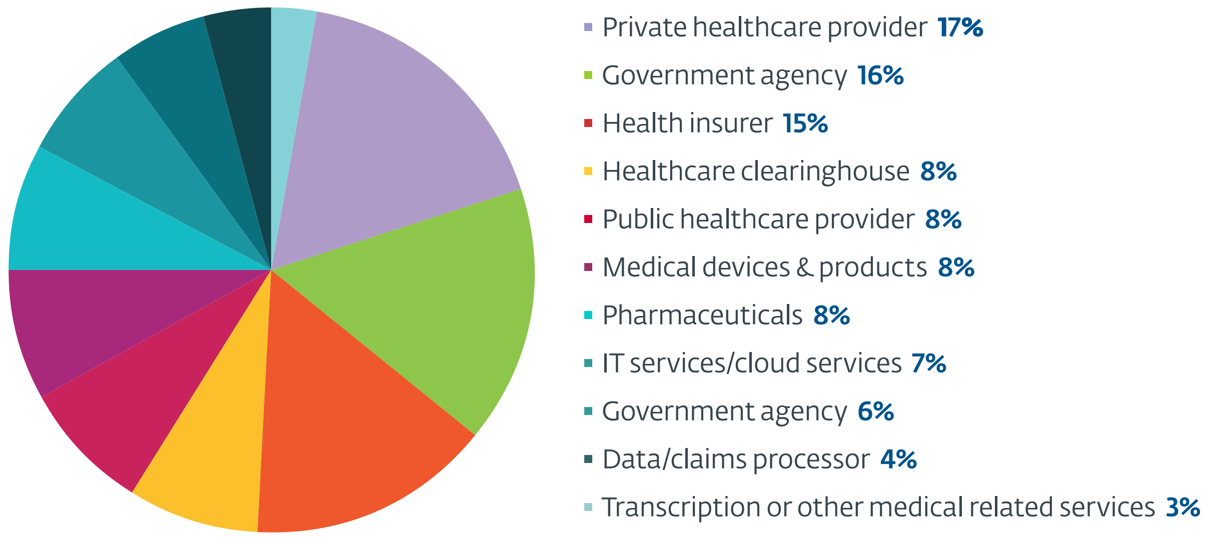
Part 3. Methods & Limitations

A sampling frame of 15,445 experienced IT and IT security practitioners in a variety of healthcare organizations such as private and public healthcare providers and government agencies were selected as participants in this survey. From this sampling frame, we captured 621 returns of which 86 were rejected for reliability issues. Our final sample was 535, thus resulting in an overall 3.5 percent response rate, as shown in Table 1.

Table 1. Sample 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%

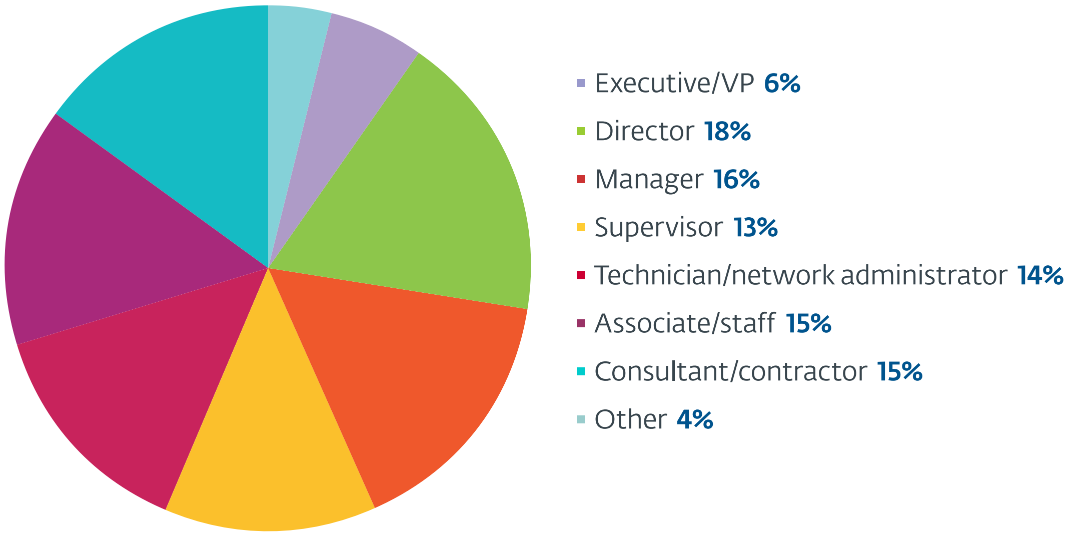
Pie Chart 1 reports the category that best describes the respondent's organization. As can be seen, 17 percent of respondents describe their organization as a private healthcare provider, 16 percent responded government agency and 15 percent responded health insurer.

Pie Chart 1. Category that best describes the organization



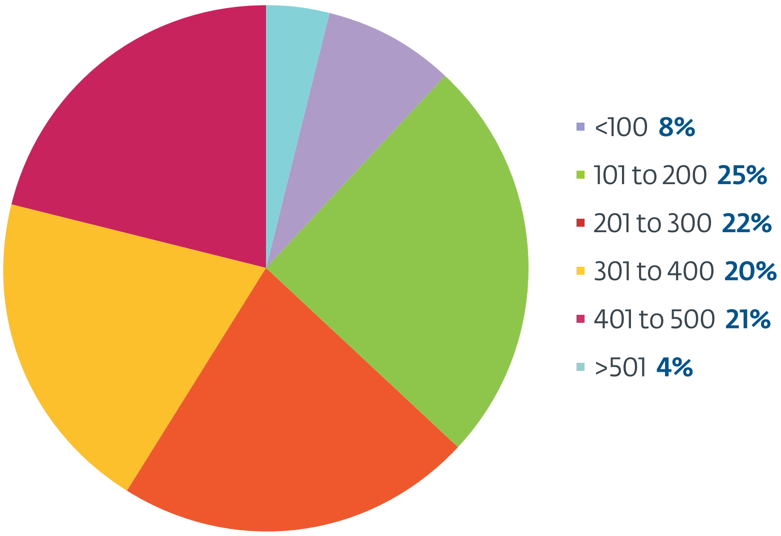
Pie Chart 2 summarizes the approximate position levels of respondents in our study. As can be seen, the majority of respondents (53 percent) are at or above the supervisory level.

Pie Chart 2. Distribution of respondents according to position level



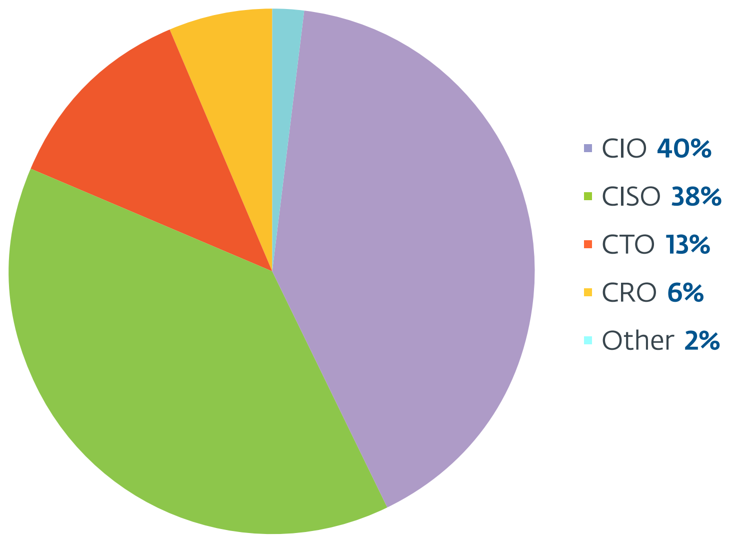
According to Pie Chart 3, the majority of respondents (55 percent) are located in organizations with a headcount of more than 200 employees.

Pie Chart 3. Distribution of respondents according to world headcount



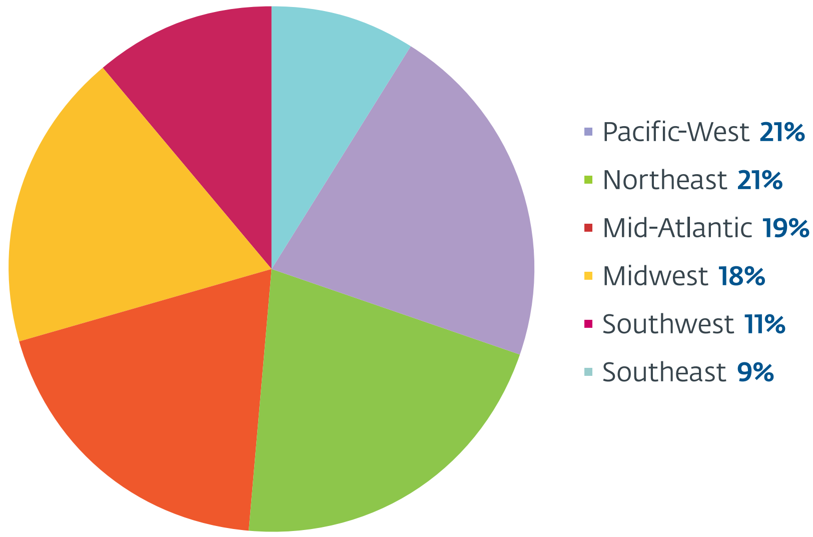
As shown in Pie Chart 4, forty percent of respondents indicated the CIO is most accountable for the organization's cybersecurity and 38 percent responded the CISO.

Pie Chart 4. Person most accountable for the organization's cybersecurity strategy



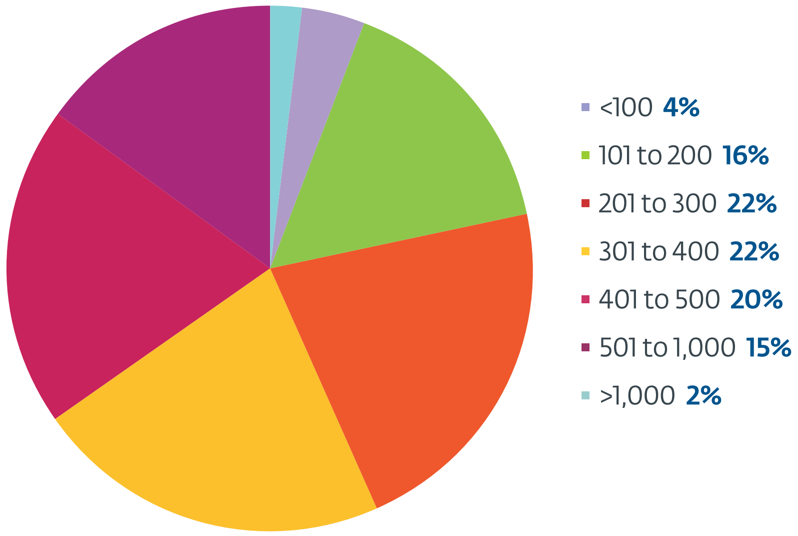
Pie Chart 5 identifies the United States region where respondents are located. Twenty-one percent of respondents are located in the Pacific-West, another 21 percent are located in the Northeast and 19 percent are in the Mid-Atlantic region.

Pie Chart 5. The region of the United States where the respondents are located



Pie Chart 6 identifies the number of network connected devices. The majority of respondents (59 percent) indicated their organizations have more than 300 network connected devices.

Pie Chart 6. 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.

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%

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 mid-December 2015 through January 4, 2016.

Survey response	Freq	Pct%
Total sampling frame	15,445	100%
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%

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 is the 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%
Unsecure mobile devices	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%
Unsecure 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 HIPAA/HITECH 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 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 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 ever benefited from HIPAA/HITECH notification rules when a data breach involved protected health information (PHI) that had been 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 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.

For over 25 years, ESET® has been developing industry-leading security software for businesses and consumers worldwide. With security solutions ranging from endpoint and mobile defense to encryption and two-factor authentication, ESET's high-performing, easy-to-use products give users and businesses the peace of mind to enjoy the full potential of their technology. ESET unobtrusively protects and monitors 24/7, updating defenses in real time to keep users safe and businesses running uninterrupted. For more information, visit www.eset.com.

ENJOY SAFER TECHNOLOGY®