Ponemon INSTITUTE

Fifth Annual Benchmark Study on Privacy & Security of Healthcare Data

Sponsored by ID Experts

Independently conducted by Ponemon Institute LLC

Publication Date: May 2015

Fifth Annual Benchmark Study on Privacy & Security of Healthcare Data

Presented by Ponemon Institute, May 2015

Part 1. Executive Summary

The *Fifth Annual Benchmark Study on Privacy & Security of Healthcare Data* reveals that the majority of healthcare organizations represented in this study have experienced multiple security incidents and nearly all have faced a data breach. Despite the universal risk for data breach, the study found that many organizations lack the funds and resources to protect patient data and are unprepared to meet the changing cyber threat environment.

The 2015 study was expanded beyond healthcare organizations to include business associates. Represented in this study are 90 covered entities[1] (hereafter referred to as healthcare organizations) and 88 business associates (hereafter may be referred to as either business associates or BAs). A BA is a person or entity that performs services for a covered entity that involves the use or disclosure of protected health information (PHI), according to the U.S. Department of Health & Human Services. The inclusion of BAs provides a broader perspective of the healthcare industry as a whole and demonstrates the impact third parties have on the privacy and security of patient data. Respondents were surveyed about their privacy and security practices and experiences with data breaches, as well as their experiences with both electronic and paper security incidents.[2]

Data breaches in healthcare continue to put patient data at risk and are costly. Based on the results of this study, we estimate that data breaches could be costing the industry $6 billion.[3] More than 90 percent of healthcare organizations represented in this study had a data breach, and 40 percent had more than five data breaches over the past two years. According to the findings of this research, the average cost of a data breach for healthcare organizations is estimated to be more than $2.1 million. No healthcare organization, regardless of size, is immune from data breach. The average cost of a data breach to BAs represented in this research is more than $1 million. Despite this, half of all organizations have little or no confidence in their ability to detect all patient data loss or theft.

For the first time, criminal attacks are the number one cause of data breach in healthcare. Criminal attacks on healthcare organizations are up 125 percent compared to five years ago. In fact, 45 percent of healthcare organizations say the root cause of the data breach was a criminal attack and 12 percent say it was due to a malicious insider. In the case of BAs, 39 percent say a criminal attacker caused the breach and 10 percent say it was due to a malicious insider.

The percentage of criminal-based security incidents is even higher; for instance, web-borne malware attacks caused security incidents for 78 percent of healthcare organizations and 82 percent for BAs. Despite the changing threat environment, however, organizations are not changing their behavior—only 40 percent of healthcare organizations and 35 percent of BAs are concerned about cyber attackers.

Security incidents are part of everyday business. Sixty-five percent of healthcare organizations and 87 percent of BAs report their organizations experienced electronic information-based security incidents over the past two years. Fifty-four percent of healthcare organizations suffered paper-based security incidents and 41 percent of BAs had such an incident. However, many

---

[1] Covered entities are defined in the HIPAA rules as (1) health plans, (2) health care clearinghouses, and (3) health care

[2] A security incident is defined as a violation of an organization's security or privacy policies involving protected information such as social security numbers or confidential medical information. A data breach is an incident that meets specific legal definitions per applicable breach law(s). Data breaches require notification to the victims and may result in regulatory investigation, corrective actions, and fines.

[3] This is based on multiplying $1,067,400 (50% of the average two year cost of a data breach experienced by the 90 healthcare organizations in this research) x 5,686 (the total number of registered US hospitals per the AHA).

organizations do not have the budget and resources to protect both electronic and paper-based patient information. For instance, 56 percent of healthcare organizations and 59 percent of BAs don't believe their incident response process has adequate funding and resources. In addition, the majority of both types of organizations fail to perform a risk assessment for security incidents, despite the federal mandate to do so.

Even though medical identity theft nearly doubled in five years, from 1.4 million adult victims to over 2.3 million in 2014,[4] the harms to individuals affected by a breach are not being addressed. Many medical identity theft victims report they have spent an average of $13,500 to restore their credit, reimburse their healthcare provider for fraudulent claims and correct inaccuracies in their health records.[5] However, nearly two-thirds of both healthcare organizations and BAs do not offer any protection services for patients whose information has been breached.

Since 2010, this study has tracked privacy and security trends of patient data at healthcare organizations. Although the annual economic impact of a data breach has remained consistent over the past five years, the most-often reported root cause of a data breach is shifting from lost or stolen computing devices to criminal attacks. At the same time, employee negligence remains a top concern when it comes to exposing patient data. Even though organizations are slowly increasing their budgets and resources to protect healthcare data, they continue to believe not enough investment is being made to meet the changing threat landscape.

[4] These statistics are from the Ponemon/MIFA *2014 Fifth Annual Study on Medical Identity Theft.*
[5] Ibid.

Part 2. Key Findings

In this section, we provide a deeper analysis of the findings. The complete audited findings are presented in the appendix of this report. Descriptions of the organizations participating in this research can be found in the demographics section and appendix of this report. We have organized this report according to the two following topics:

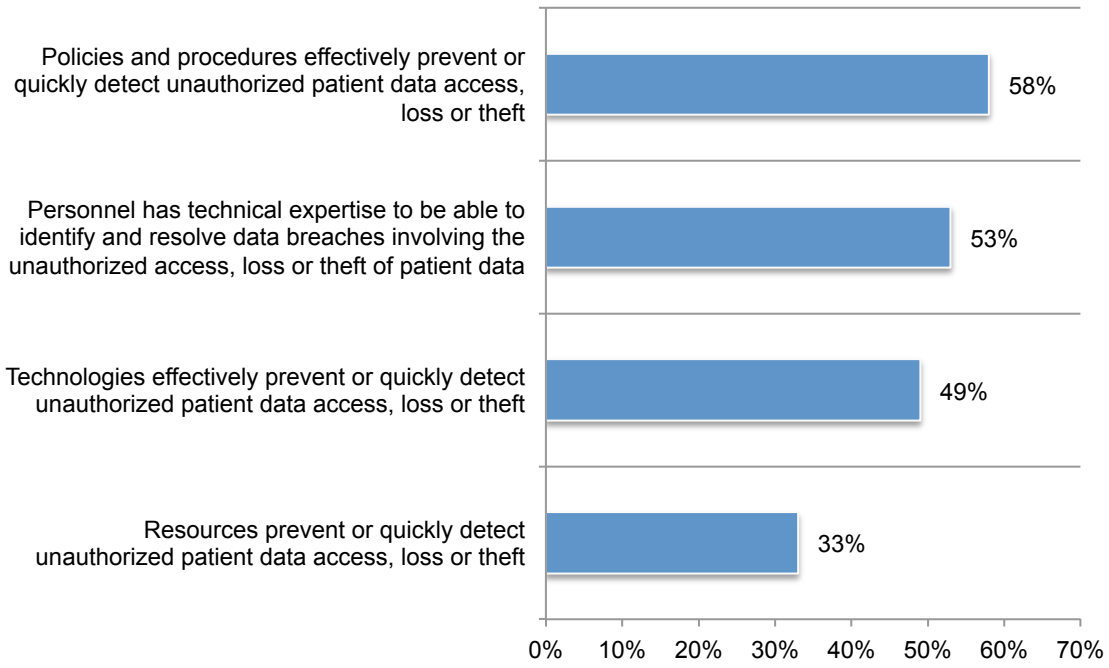
- Privacy and security of healthcare data in organizations and business associates
- Five-year trends in privacy and security practices in healthcare organizations

Privacy and security of healthcare data in organizations and business associates

To respond quickly to data breaches, organizations need to invest more in technologies. As shown in Figure 1, 58 percent of healthcare organizations agree that policies and procedures are in place to effectively prevent or quickly detect unauthorized patient data access, loss or theft. However, less than half (49 percent) agree they have sufficient technologies. Worse, only 33 percent agree they have sufficient resources to prevent or quickly detect a data breach.

Slightly more than half (53 percent) of organizations have personnel with the necessary technical expertise to be able to identify and resolve data breaches involving the unauthorized access, loss or theft of patient data.

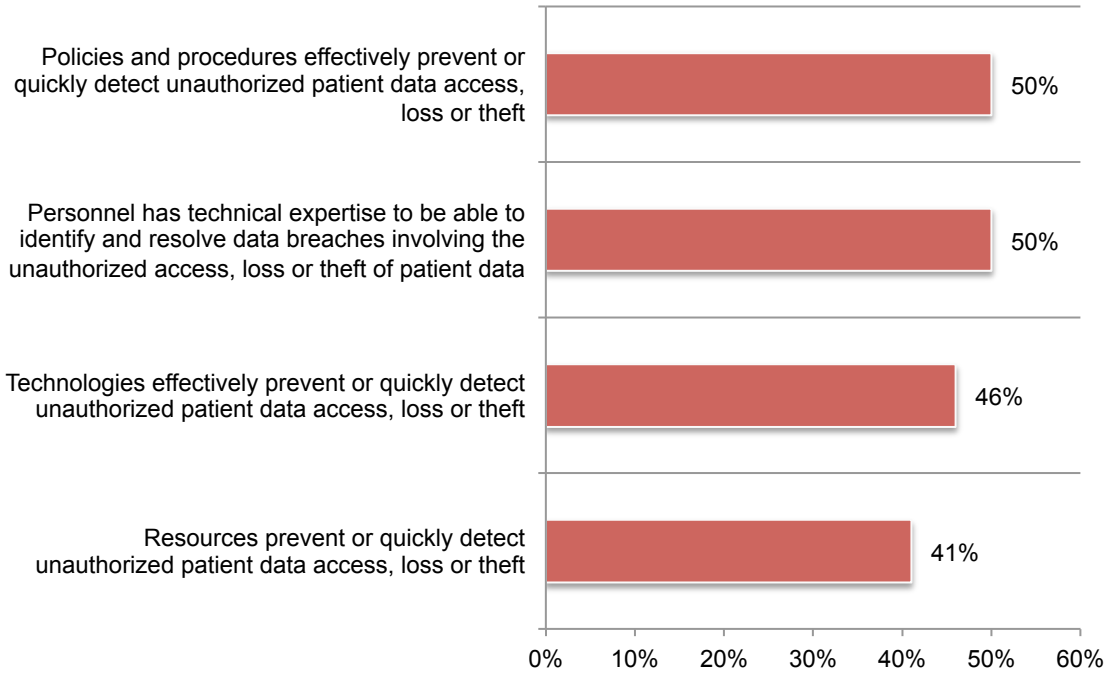
Figure 1. Healthcare organizations' perceptions about privacy and healthcare data protection



According to Figure 2, 50 percent of business associates agree that policies and procedures are in place to effectively prevent or quickly detect unauthorized patient data access, loss or theft. However, less than half (46 percent) agree they have sufficient technologies. Worse, only 41 percent agree they have sufficient resources to prevent or quickly detect a data breach.

Fifty percent say their organization has personnel with the necessary technical expertise to be able to identify and resolve data breaches involving the unauthorized access, loss or theft of patient data.

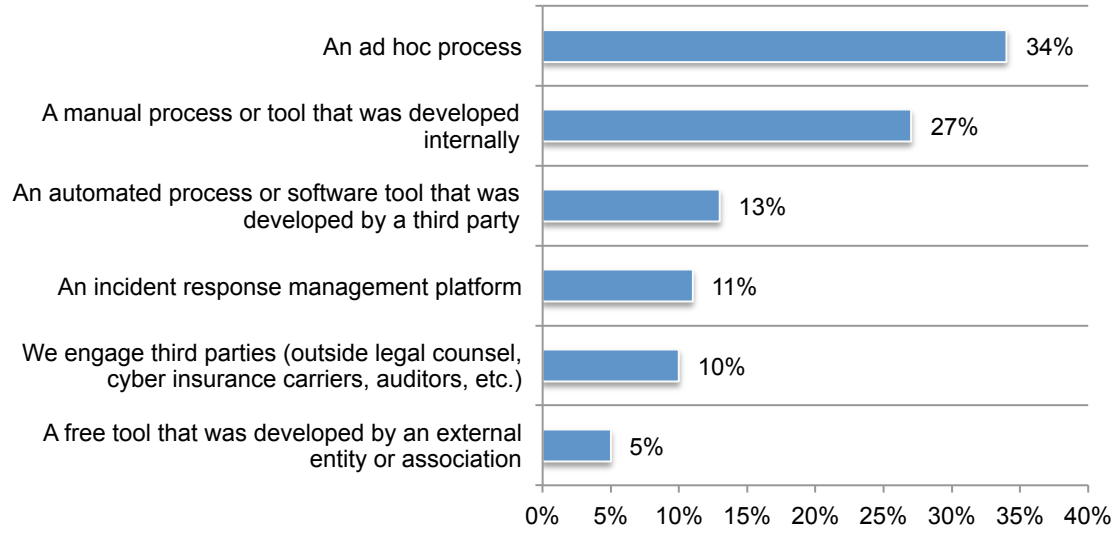
Figure 2. Business associates' perceptions about privacy and healthcare data protection



Security incidents involving electronic information are prevalent. Sixty-five percent of healthcare organizations had multiple security incidents in the past two years involving the exposure, theft or misuse of electronic information. Fifty-eight percent say they have had between 11 and 30 electronic information-based security incidents. Most involved the exposure of less than 100 PHI records.

Fifty percent of respondents say their organizations perform a 4-factor risk assessment following each security incident that involves electronic information as required under HIPAA Omnibus Final Rule to determine if an incident is a data breach that requires notification under applicable federal and state regulations. As shown in Figure 3, most often it is an ad hoc process (34 percent of respondents) and 27 percent of respondents say it is a manual process or tool that was developed internally.

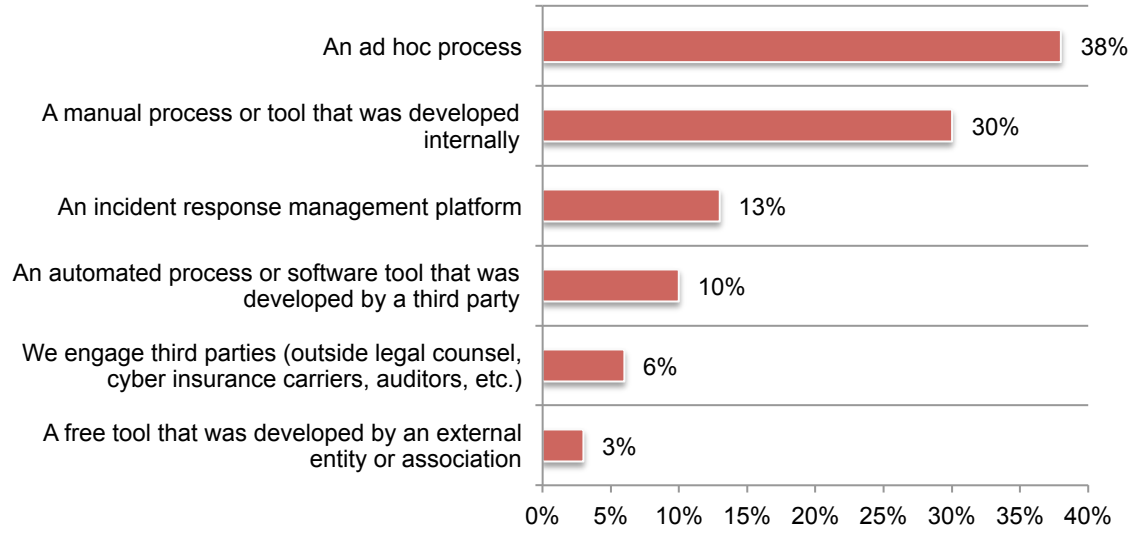
Figure 3. Assessment of risk following security incidents involving electronic documents (healthcare organizations)



Eighty-seven percent of business associates had multiple security incidents in the past two years involving the exposure, theft or misuse of electronic information. Seventy percent of respondents say they have had between 11 and 30 electronic information-based security incidents. Most involved the exposure of less than 100 PHI records.

Forty-two percent of respondents say their organizations perform a 4-factor risk assessment following each security incident that involves electronic information as required under HIPAA Omnibus Final Rule to determine if an incident is a data breach that requires notification under applicable federal and state regulations. Similar to healthcare organizations, most often the assessment process is ad hoc (38 percent of respondents) and 30 percent of respondents say it is a manual process or tool that was developed internally, according to Figure 4. The compliance officer is the person most responsible for performing the assessment.

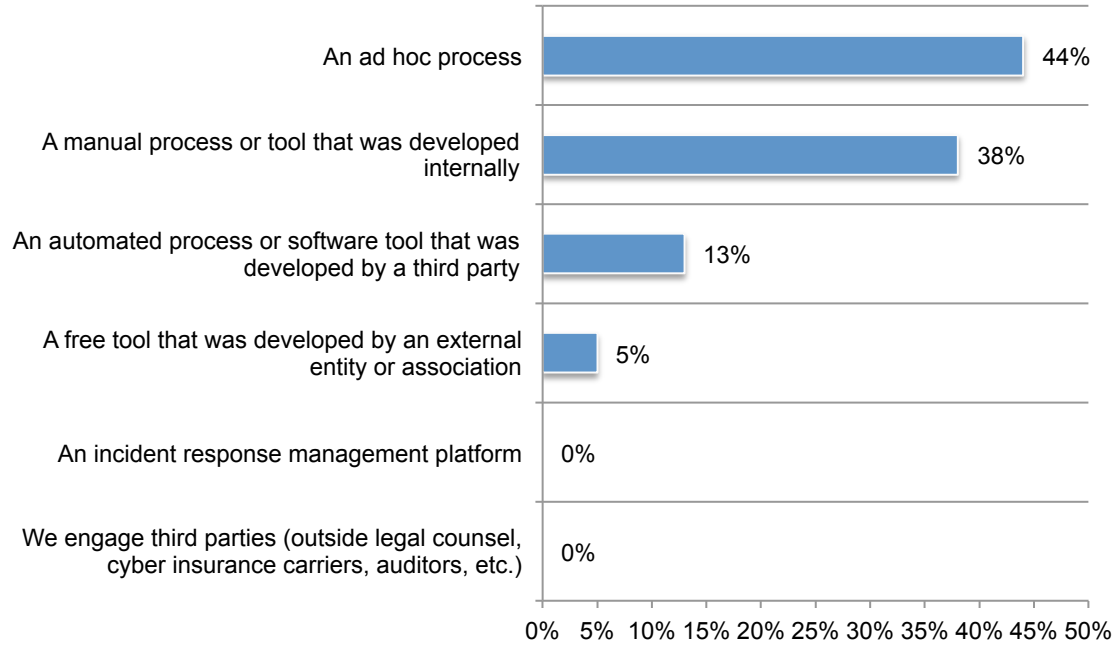
Figure 4. Assessment of risk following security incidents involving electronic documents (business associates)



Security incidents involving paper documents affect most healthcare organizations. Fifty-four percent of respondents say such a security incident occurred in their organization. Almost all (91 percent) involved less than 20 incidents in the past 24 months and most involved less than 100 PHI records.

Unlike electronic records, 4-factor risk assessments as required under HIPAA Omnibus Final Rule to determine if an incident is a data breach that requires notification under applicable federal and state regulations are rarely conducted for each security incident (20 percent of respondents) or for some security incidents (33 percent of respondents). Similar to electronic records, as shown in Figure 5, most use an ad hoc process (44 percent of respondents) or manual process (38 percent of respondents). The compliance officer is the person most responsible for performing a 4-factor risk assessment.

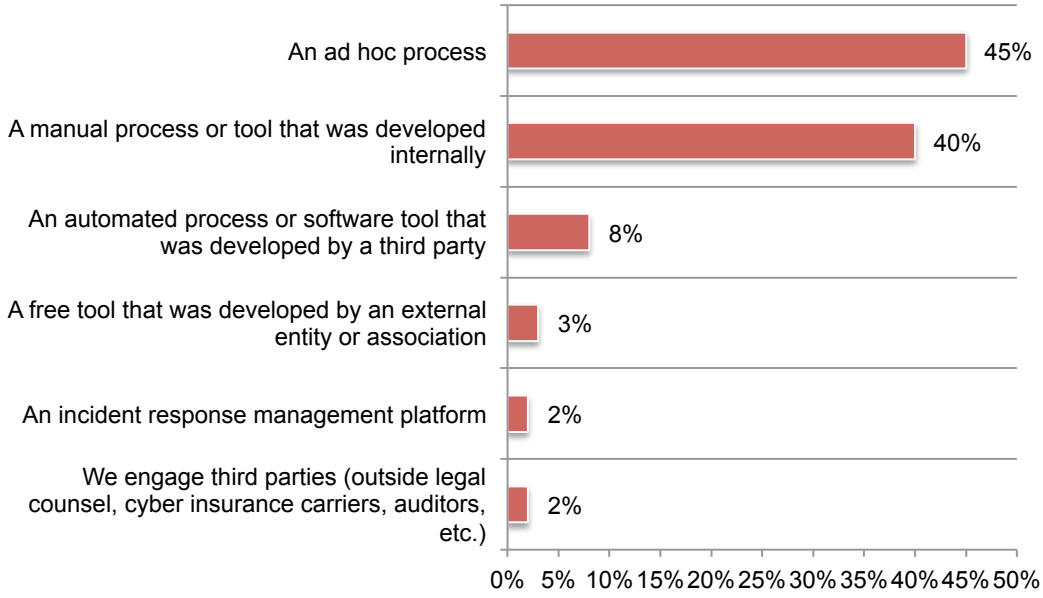
Figure 5. Assessment of risk following security incidents involving paper documents (healthcare organizations)



Forty-one percent of business associates say such a security incident occurred. Almost all (93 percent) involved less than 20 incidents in the past 24 months and most involved less than 100 PHI records.

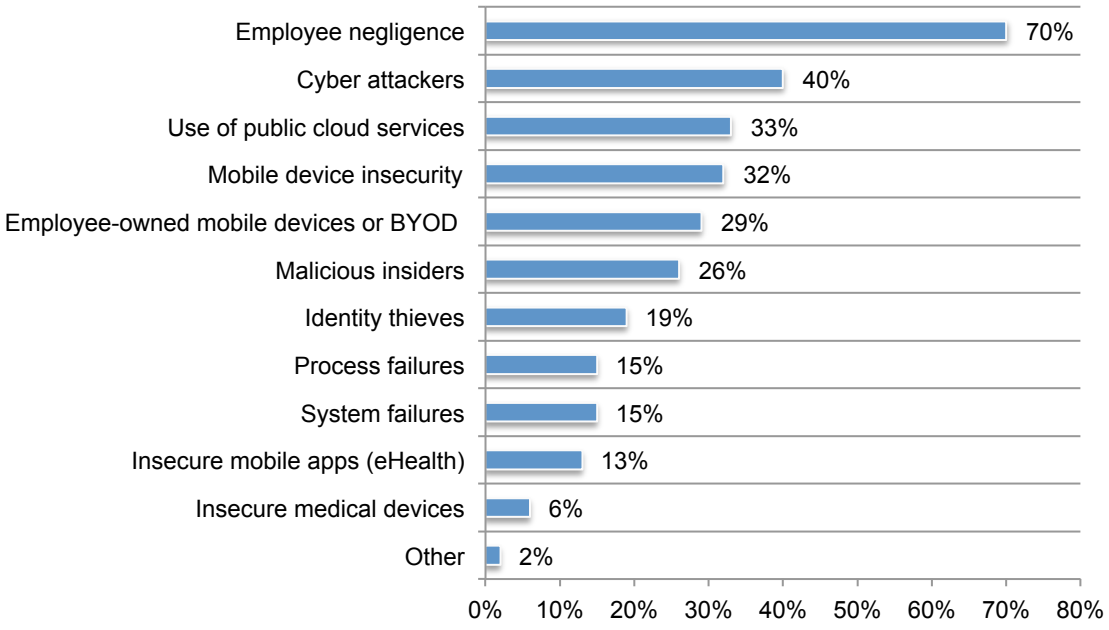
Similar to healthcare organizations, 4-factor risk assessments as required under HIPAA Omnibus Final Rule to determine if an incident is a data breach that requires notification under applicable federal and state regulations are rarely conducted for each security incident (21 percent of respondents) or for some security incidents (28 percent of respondents). According to Figure 6, similar to electronic records, most use an ad hoc process (45 percent of respondents) or manual process (40 percent of respondents). The compliance officer is the person most responsible for performing a 4-factor risk assessment.

Figure 6. Assessment of risk following security incidents involving paper documents (business associates)



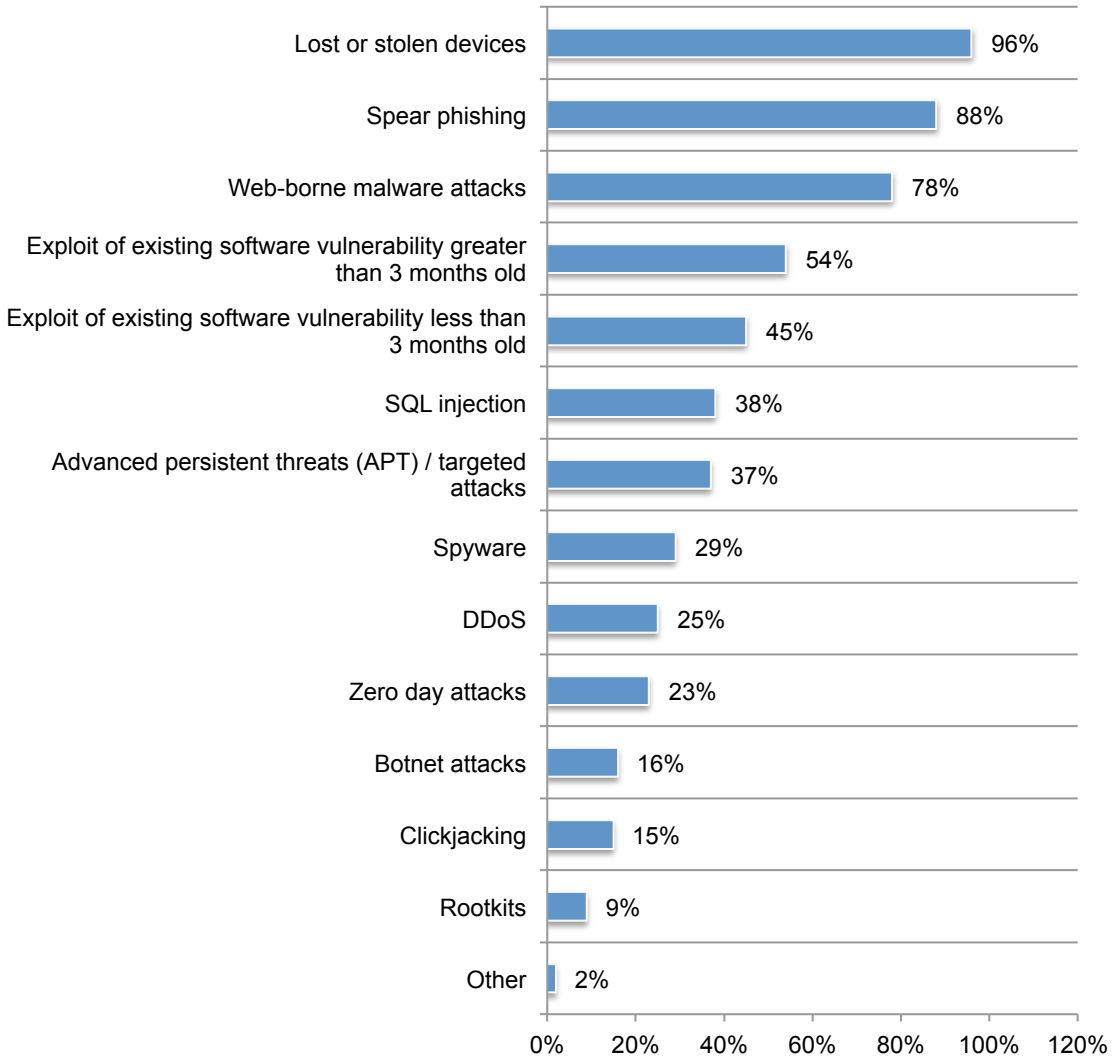
Employee negligence is the greatest concern. According to Figure 7, when healthcare organizations were asked what type of security incident worries them most, by far it is the negligent or careless employee (70 percent of respondents). This is followed by 40 percent of respondents who say it is cyber attackers and 33 percent who say it is the use of public cloud services. Insecure mobile apps and insecure medical devices are the least problematic (13 percent and 6 percent of respondents, respectively).

Figure 7. What security threats healthcare organizations worry about most
Three responses permitted



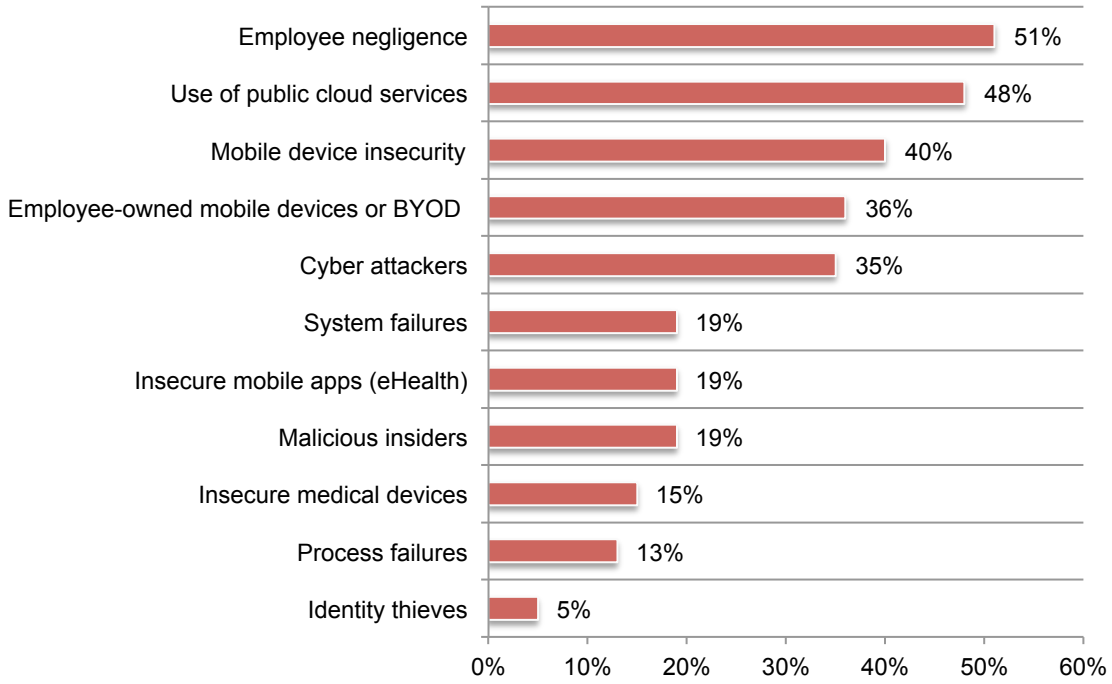
It is obvious why healthcare organizations are concerned about negligence. As shown in Figure 8, 96 percent of respondents say they had a security incident involving lost or stolen devices. This is followed by spear phishing, according to 88 percent of respondents. These incidents are also related to employees' failure to follow security procedures. Web-borne malware attacks are also a big concern with 78 percent of respondents reporting such an incident occurred in their organizations.

Figure 8. Security incidents healthcare organizations experienced
More than one response permitted



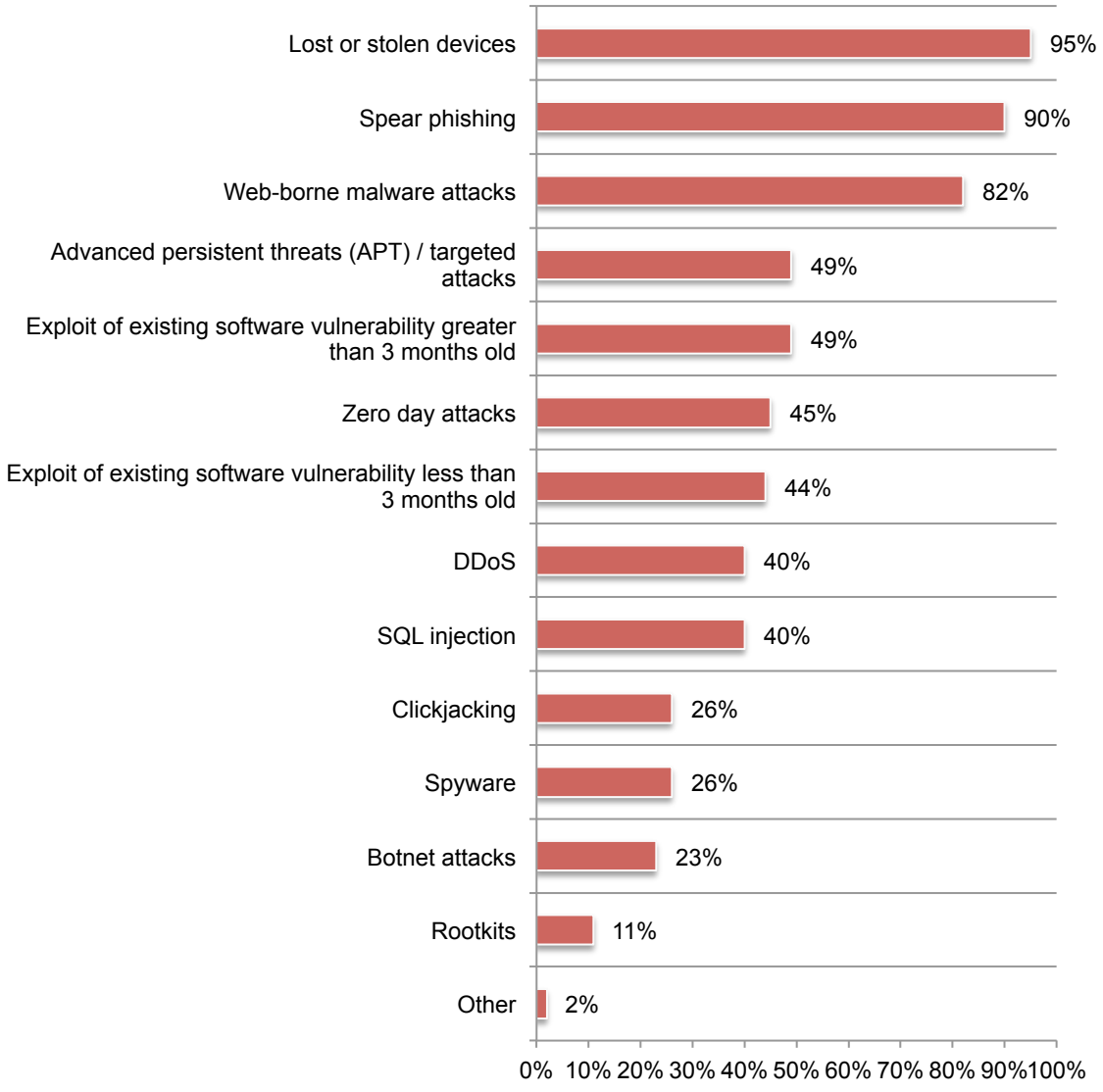
Just like healthcare **organizations**, business associates worry about employee negligence. When asked what type of security incident concerns them most, it is the negligent or careless employee (51 percent of respondents), as shown in Figure 9. This is followed by 48 percent of respondents who say it is use of cloud services and 40 percent who say it is mobile device insecurity. Process failures and identity thieves are the least problematic (13 percent and 5 percent of respondents, respectively).

Figure 9. What security threats worry business associates the most
Three responses permitted



It is obvious why organizations are concerned about negligence. As shown in Figure 10, 95 percent of respondents say they had a security incident involving lost or stolen devices. This is followed by spear phishing, according to 90 percent of respondents. These incidents are also related to employees' failure to follow security procedures. Web-borne malware attacks are also a concern with 82 percent of respondents reporting such an incident occurred in their organizations.

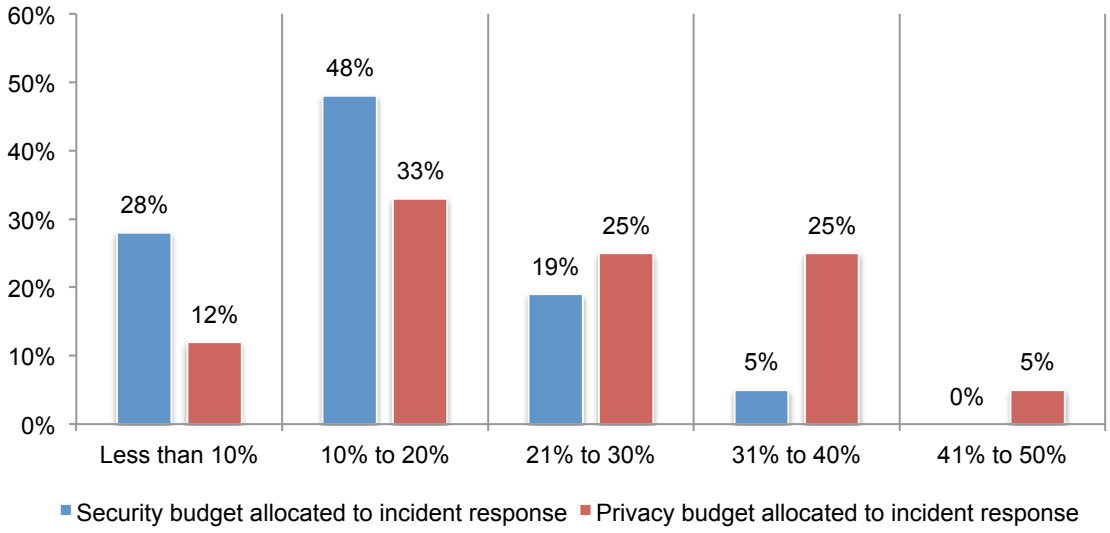
Figure 10. Security incidents business associates experienced
More than one response permitted



Most healthcare organizations have an incident response process in place. Healthcare organizations recognize the need to have a formal incident response process in place. Sixty-nine percent of organizations have a process with involvement from information technology, information security and compliance.

However, 56 percent of respondents say more funding and resources are needed to make it effective. As shown in Figure 11, 76 percent of organizations allocate 20 percent or less of the security budget allocated to incident response. Fifty-five percent of organizations allocate more than 20 percent of the privacy budget to incident response.

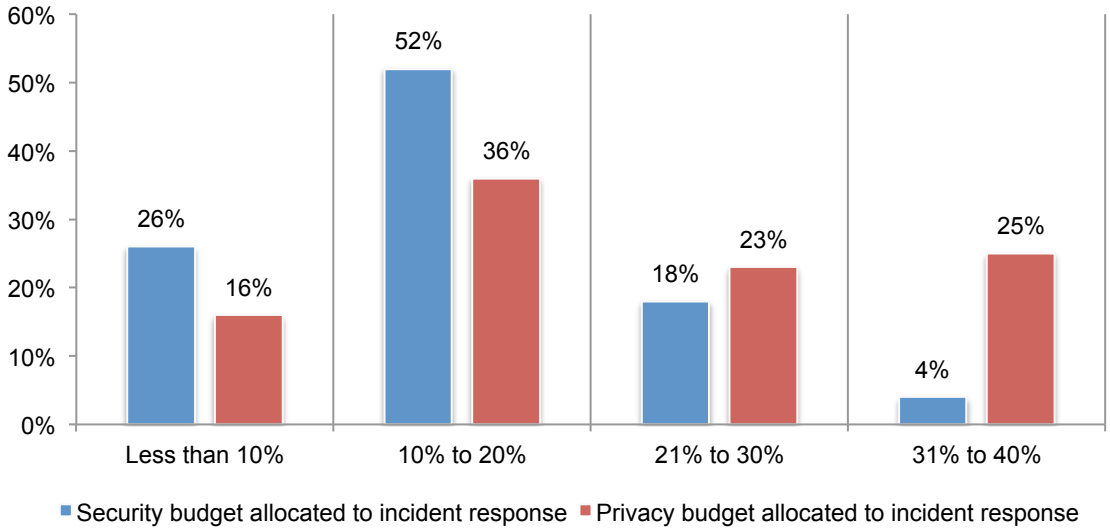
Figure 11. Percentage of security and privacy budget allocated to incident response for healthcare organizations



Business associates recognize the need to have a formal incident response process in place. Sixty-five percent of the respondents say their organizations have a process with involvement from information technology, information security and compliance.

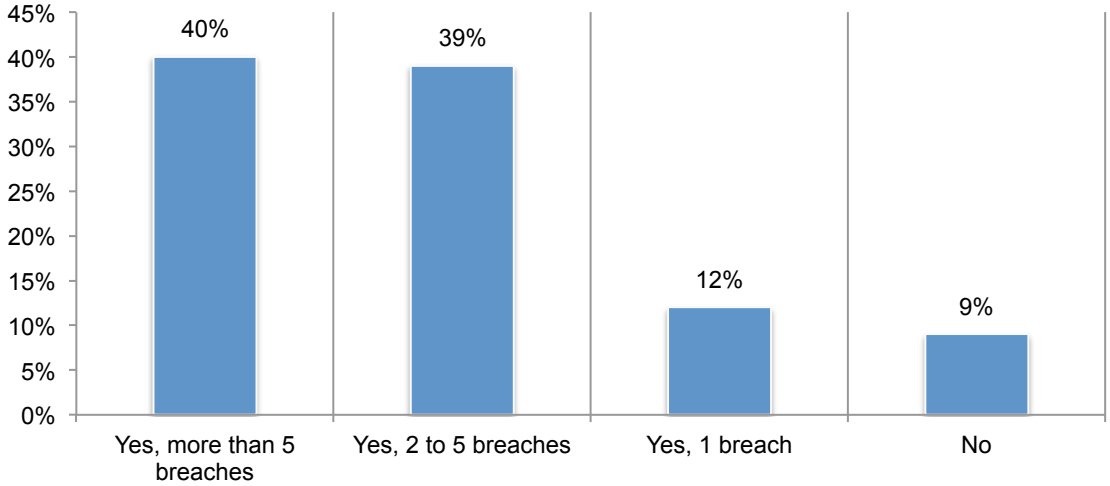
However, 59 percent of respondents say more funding and resources are needed to make it effective. Seventy-eight percent of respondents say less than 20 percent of the security budget is allocated to incident response and 52 percent of respondents allocate 20 percent or less of the privacy budget to incident response.

Figure 12. Percentage of security and privacy budget allocated to incident response for business associates



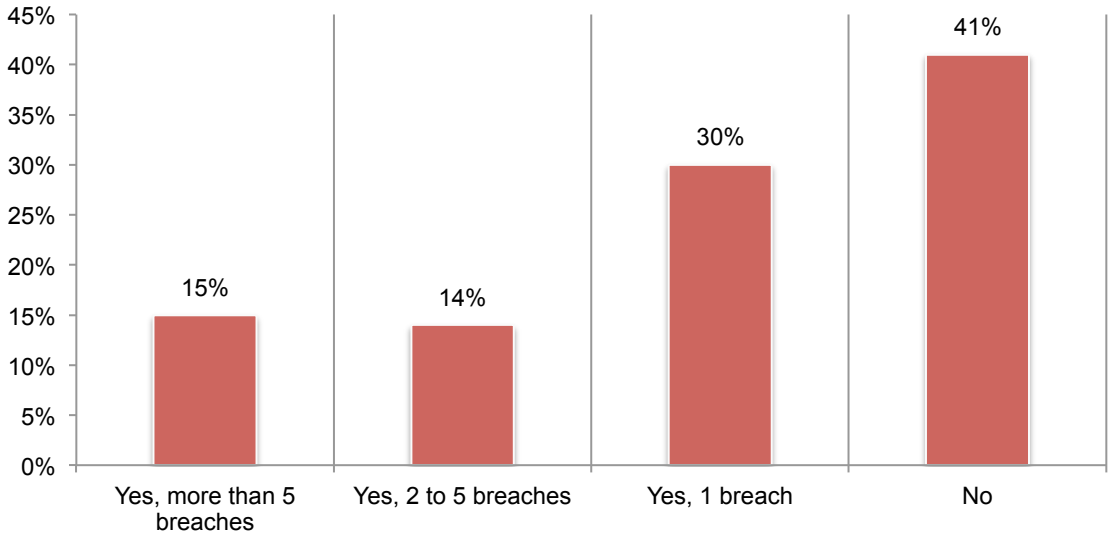
Data breaches affect all organizations. Ninety-one percent of healthcare organizations had at least one data breach involving the loss or theft of patient data in the past 24 months. According to Figure 13, 40 percent had more than 5 breaches. Moreover, less than half (49 percent) are very confident a[illegible]onfident they have the ability to detect all patient data loss or theft.

Figure 13. Has your organization suffered a data breach involving the loss or theft of patient data in the past 24 months (healthcare organizations)?



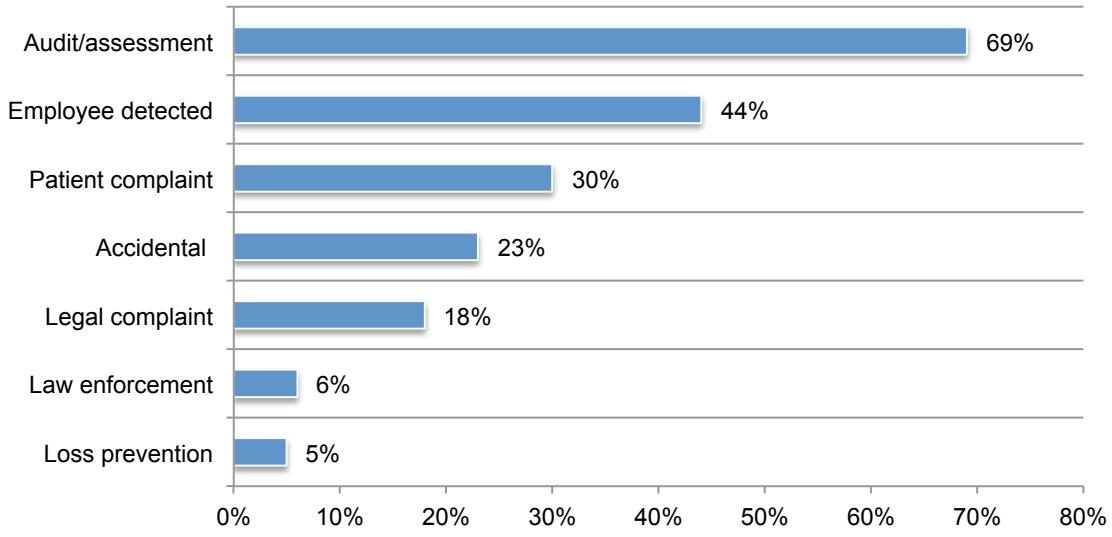
As shown in Figure 14, 59 percent of business associates had at least one data breach involving the loss or theft of patient data in the past 24 months. In fact, 29 percent say their organization had more than 2 breaches. Moreover, only 42 percent of respondents are very confident and confident they have the ability to detect all patient data loss or theft.

Figure 14. Has your organization suffered a data breach involving the loss or theft of patient data in the past 24 months (business associate)?



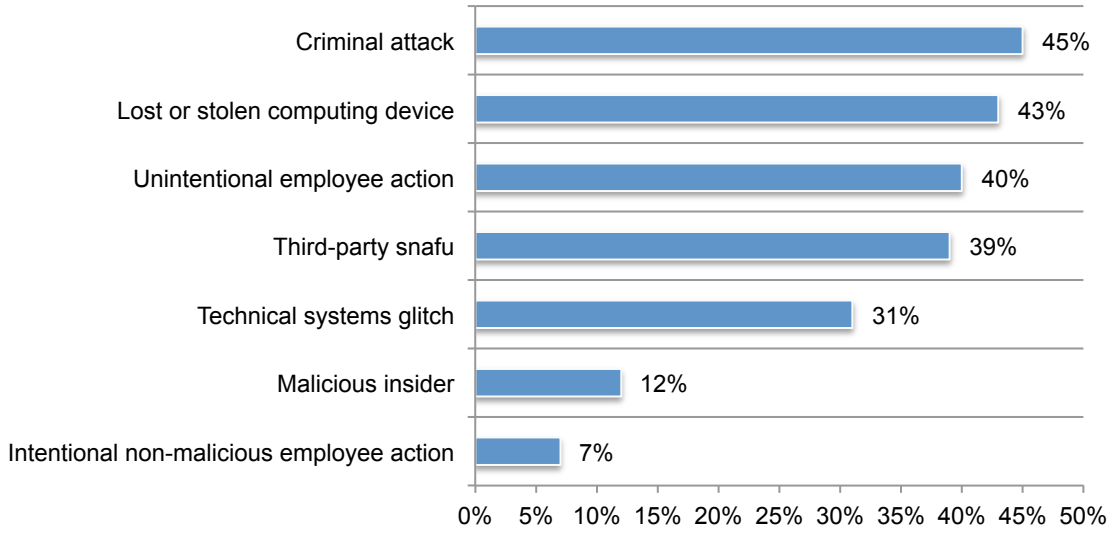
Organizations are fighting to stop data breaches from a variety of sources. In the past two years, healthcare organizations spent an average of more than $2 million to resolve the consequences of a data breach involving an average of almost more than 2,700 lost or stolen records. According to Figure 15, 69 percent of respondents say the data breach was discovered by an audit or assessment and 44 percent say an employee detected the data breach. Twenty-three percent say the data breach was discovered accidentally.

Figure 15. How the data breach was discovered (healthcare organizations)
More than one response permitted



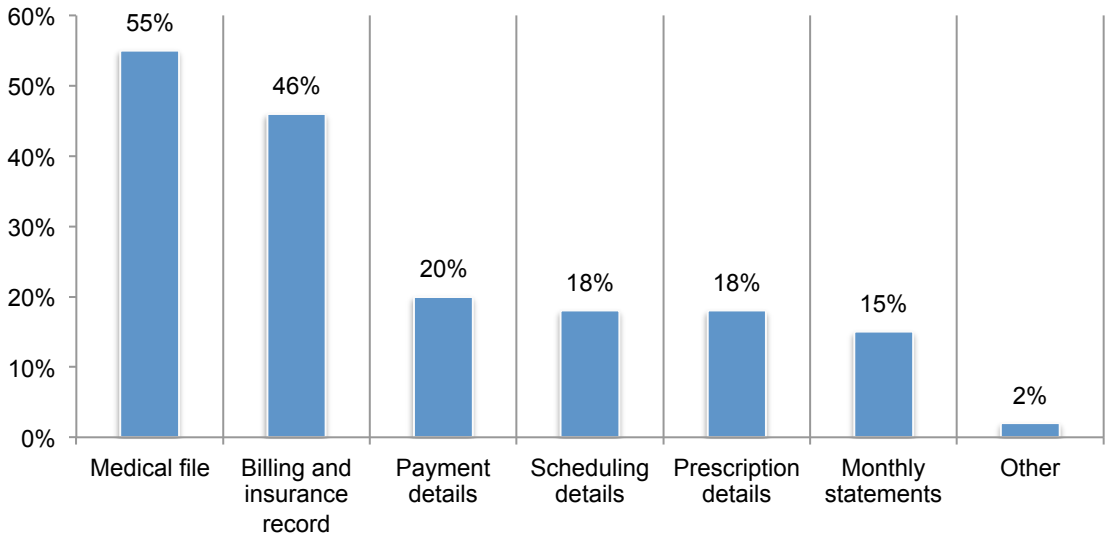
The challenge organizations face is dealing with data breaches with a variety of root causes. Figure 16 reveals that 45 percent of healthcare organizations report the breach as a criminal attack, 43 percent of respondents say it was caused by lost or stolen computing device and 40 percent respondents say it was due to unintentional employee action. Only 12 percent say it was due to a malicious insider.

Figure 16. What was the root cause of the healthcare organizations' data breach?
More than one response permitted



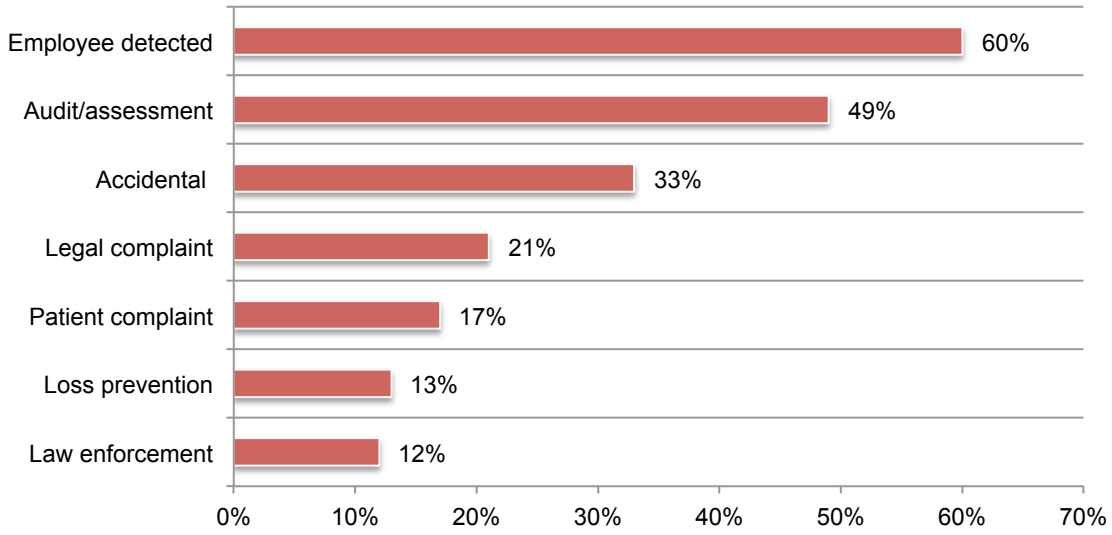
Medical files and billing and insurance records contain the most valuable patient data and most often successfully targeted (55 percent of respondents and 46 percent of respondents, respectively), as shown in Figure 17.

Figure 17. Patient data successfully targeted (healthcare organizations)



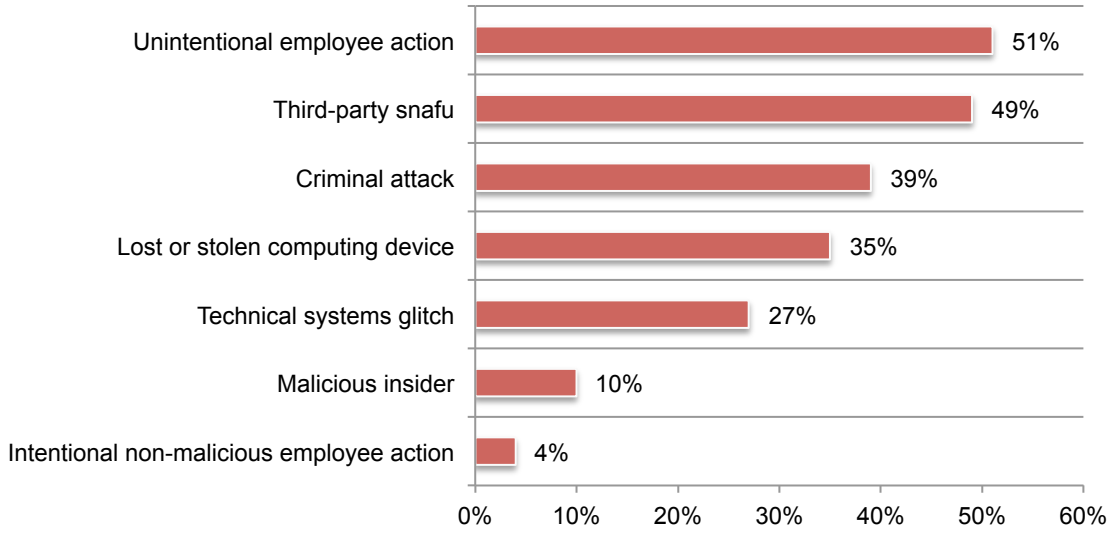
Organizations are fighting to stop data breaches from a variety of sources. In the past two years, business associates spent an average of slightly more than $1 million to resolve the consequences of a data breach involving an average of more than 5,000 lost or stolen records. According to Figure 18, 60 percent of respondents say an employee discovered the data breach and 49 percent say it was discovered through an audit or assessment. Thirty-three percent say the data breach was only discovered accidentally.

Figure 18. How the data breach was discovered (business associates)
More than one response permitted



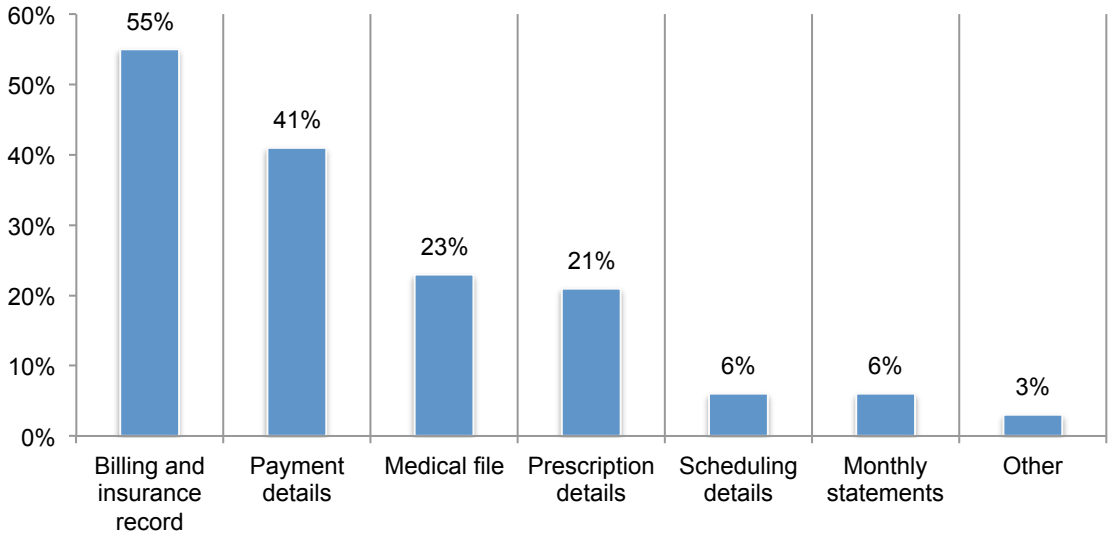
The challenge organizations face is dealing with data breaches with a variety of root causes. According to Figure 19, 51 percent of respondents say it was an unintentional employee action, 49 percent of respondents say it was caused by a third-party snafu and 35 percent respondents say it was due to a lost or stolen computing device. Only 4 percent say it was due to an intentional non-malicious employee action.

Figure 19. What was the root cause of the business associates' data breach?
More than one response permitted



Billing and insurance records contain the most valuable patient data and most often successfully targeted (55 percent of respondents). Also frequently lost or stolen are payment details (41 percent of respondents), as shown in Figure 20.

Figure 20. Patient data successfully targeted (business associates)
More than one response permitted

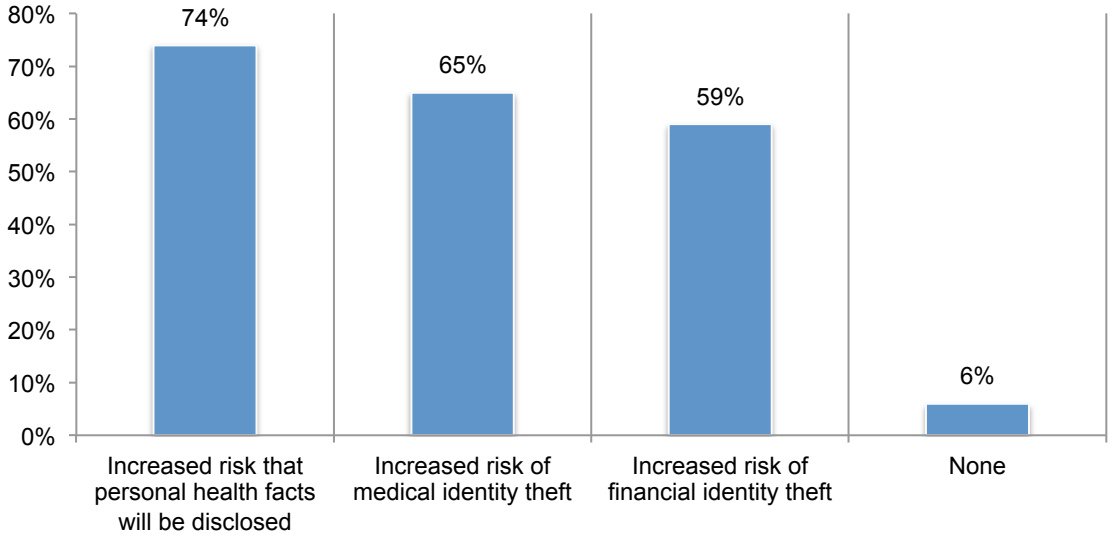


~~Organizations~~ recognize the harms patients can suffer if their records are lost or stolen. Despite the risks to patients who have had their records lost or stolen, 65 percent of ~~healthcare~~ respondents do not offer protection services. Only 19 percent offer credit monitoring and 10 percent offer other identity monitoring.

As shown in Figure 21, 74 percent of healthcare respondents say there is an increased risk that personal health facts will be disclosed and 65 percent believe patients who have had their records lost or stolen are more likely to become victims of medical identity theft. Fifty-nine percent of respondents say the risk of financial identity theft increases.

Sixty-seven percent of healthcare respondents say they are not aware or are unsure of any medical identity theft affecting their patients. Of the 33 percent who say they know about medical identity theft, the root cause most often was unintentional employee action (50 percent of respondents) followed by intentional but non-malicious employee action (17 percent of respondents).

Figure 21. Harms patients actually suffer if their records are lost or stolen (healthcare organizations)
More than one response permitted

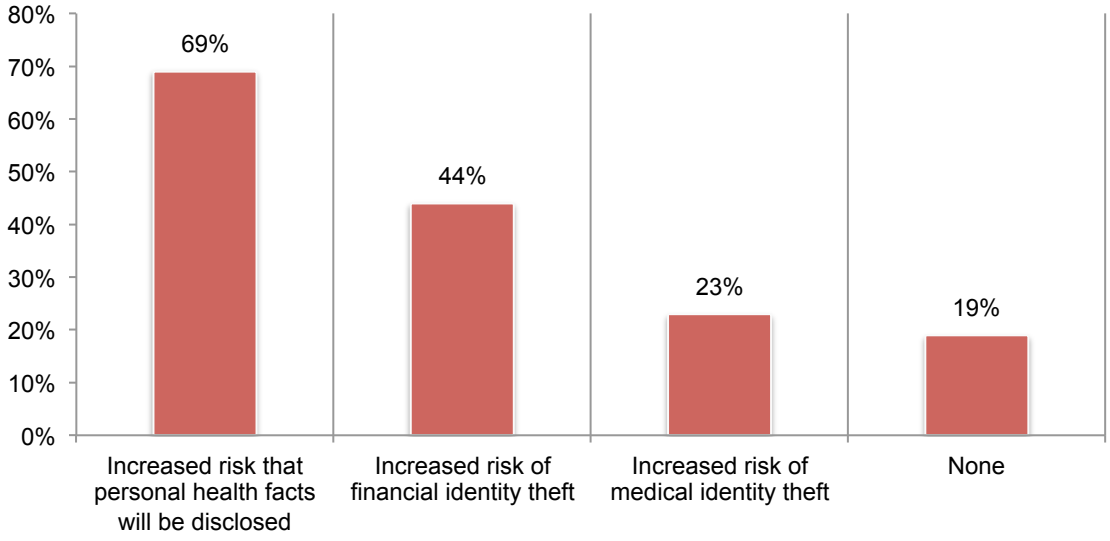


Despite the risks to patients who have had their records lost or stolen, 63 percent of BA respondents do not offer protection services. Only 14 percent offer credit monitoring and 9 percent offer other identity monitoring.

According to Figure 22, 69 percent of BA respondents say there is an increased risk that personal health facts will be disclosed and 44 percent believe patients who have had their records lost or stolen are more likely to become victims of financial identity theft. Twenty-three percent of respondents say the risk of medical identity theft increases.

Seventy-five percent of BA respondents say they are not aware or are unsure of any medical identity theft affecting their patients. Of the 25 percent who say they know about medical identity theft, the root cause most often was the intentional but non-malicious employee action (30 percent of respondents). Twenty-two percent say it was due to unintentional employee action and malicious insiders (both 22 percent).

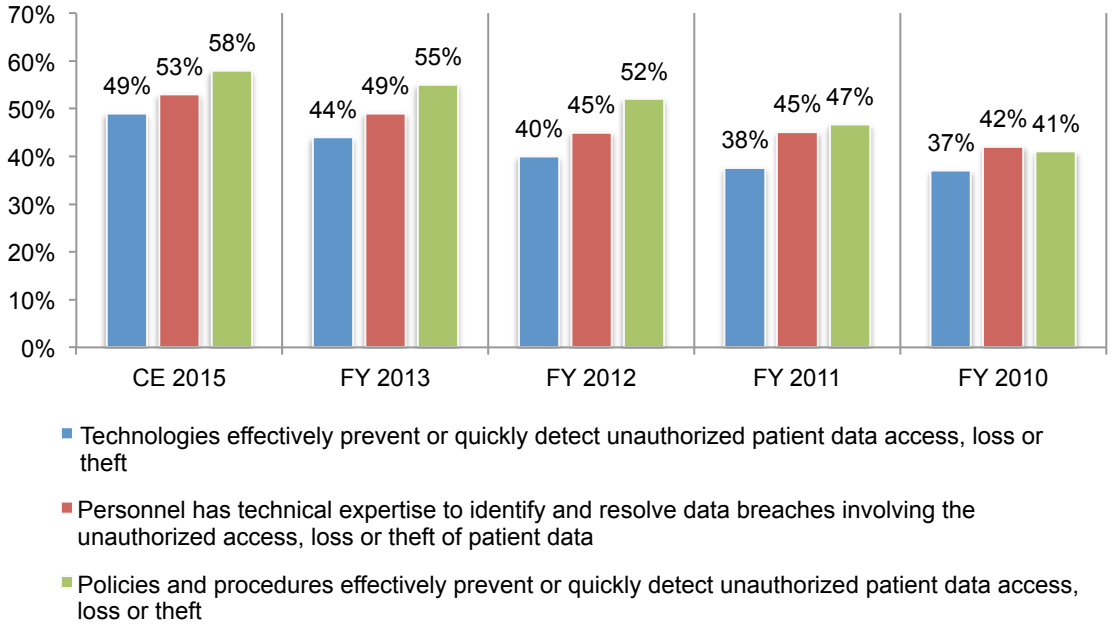
Figure 22. Harms patients actually suffer if their records are lost or stolen (business associates)
More than one response permitted



~~Healthcare organizations: five-year trends in practices~~

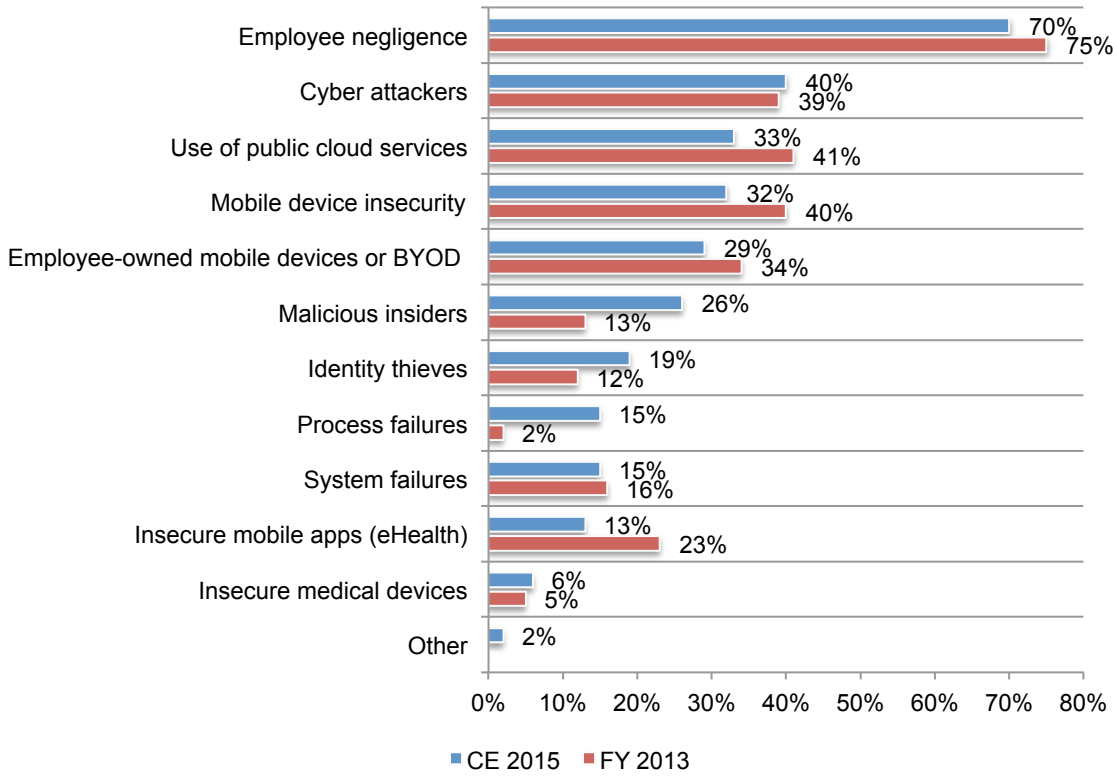
Healthcare organizations are slowly but steadily increasing their technologies and resources. Since first conducting the study in 2010, the percentage of respondents who believe their organization has personnel with the technical expertise to be able to identify and resolve data breaches involving the unauthorized access, loss or theft of patient data increased from 42 percent to 53 percent. Other changes include the increase in sufficient technologies (37 percent to 49 percent of respondents) and sufficient policies and procedures (41 percent to 58 percent).

Figure 23. Trends in privacy and security of healthcare data
Strongly agree and agree response combined



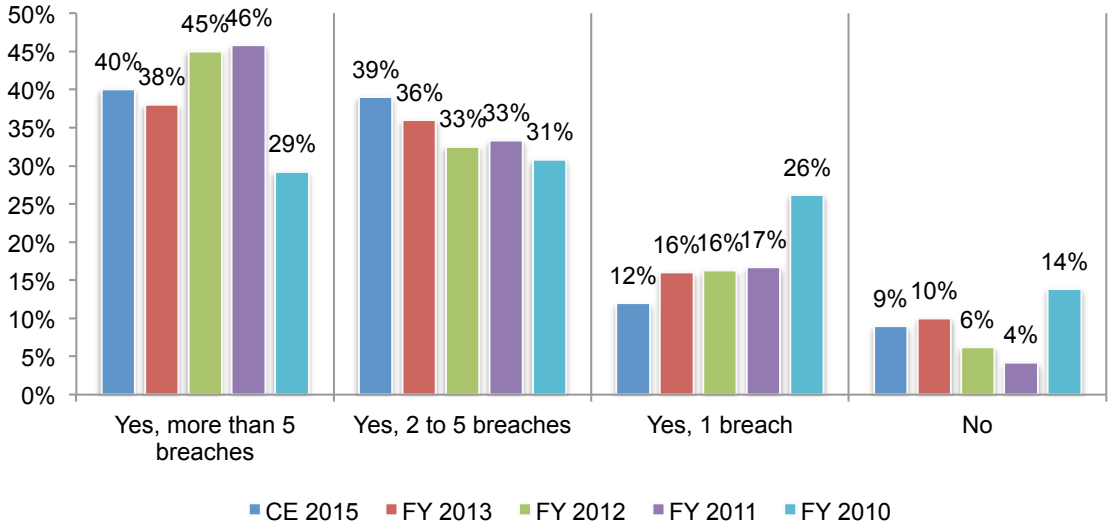
Employee negligence is a risk that must be dealt with. As shown in Figure 24**,** in the last study, 75 percent of healthcare organizations cited employee negligence as the biggest security threat. This year, 70 percent say it is a threat they worry most about. The risk of insecure mobile apps has declined as well as BYOD, mobile device insecurity and use of public cloud services.

Figure 24. Trends in security threats facing healthcare organizations
Three responses permitted



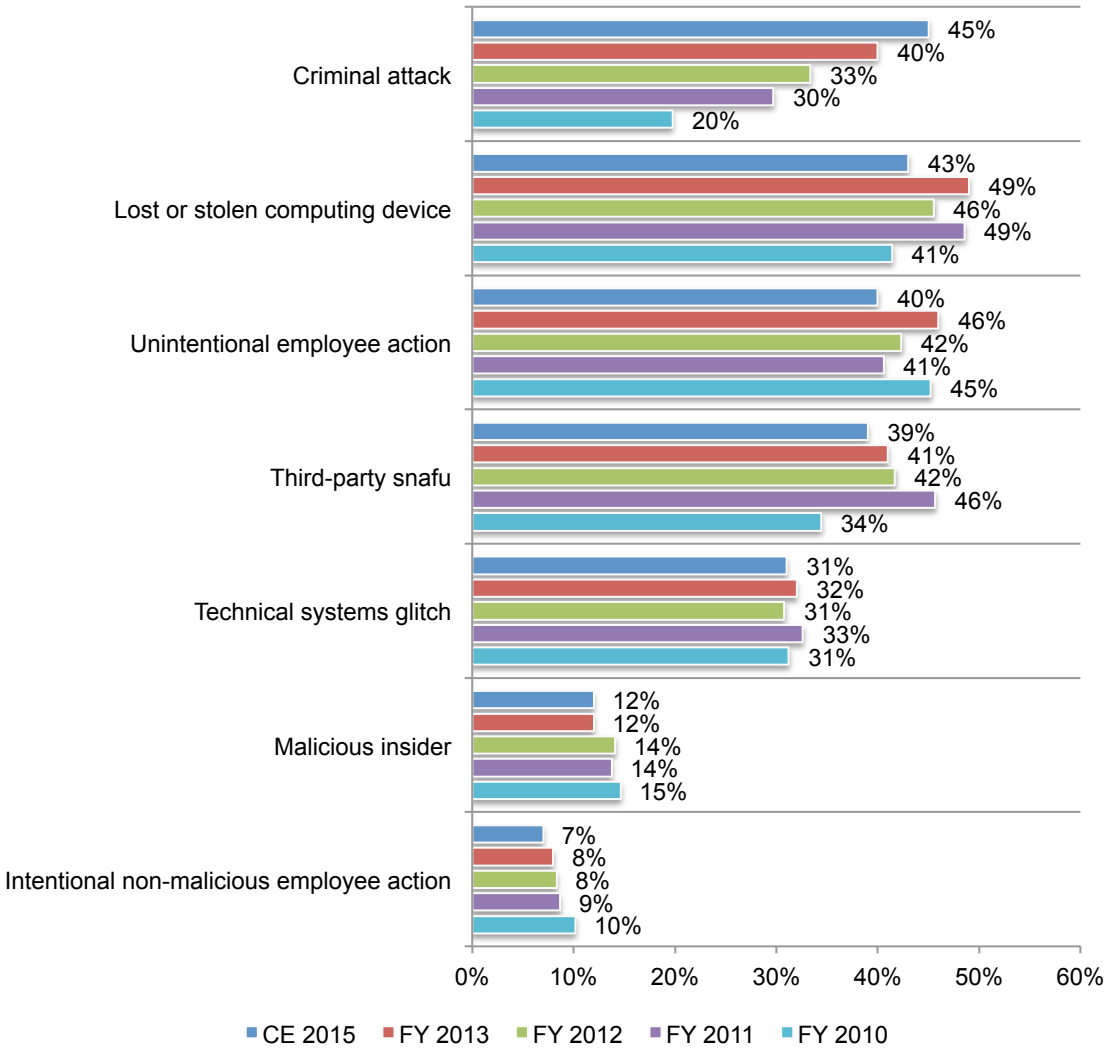
Most organizations have multiple data breaches and lack confidence in the ability to detect all patient data loss or theft. Since 2010, the percentage of respondents who said their organization had multiple breaches increased from 60 percent to 79 percent. Confidence in the ability to detect the loss or theft of all patient data increased. The level of confidence increased from 42 percent of healthcare organizations in 2010 to 49 percent of healthcare organizations in this year's study.

Figure 25. Trends in data breach incidents



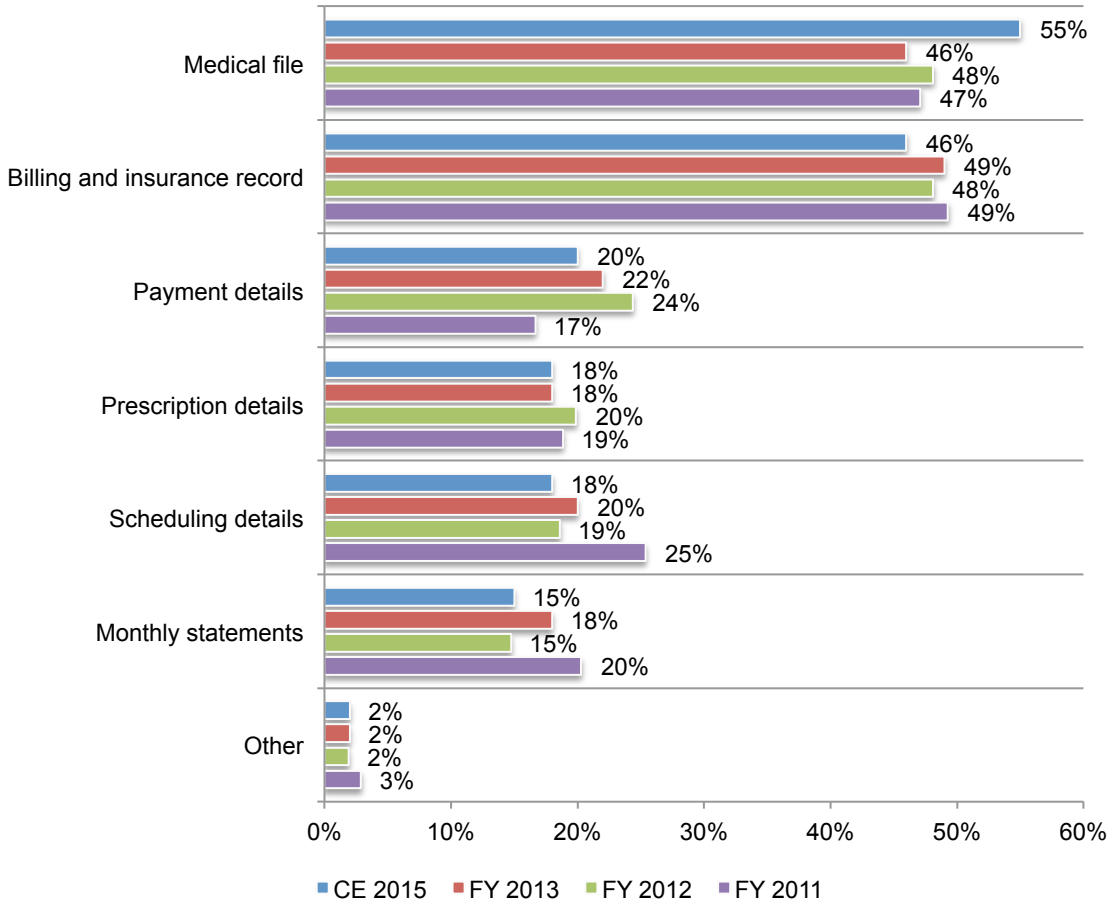
The most often reported root cause of a data breach shifts from lost or stolen computing devices to criminal attacks. For the first time, criminal attacks are the number one type of data breach (45 percent of respondents) followed by lost or stolen computing devices (43 percent), according to Figure 26. In previous years, the lost or stolen device was consistently the top root cause (with the exception of 2010).

Figure 26. Trends in the nature of the incident
More than one response permitted



Mor[illegible]artphones and tablets are the types of device[illegible]mpromised or stolen. In previous years it was the desktop or laptop. Medical files and billing and insurance records continue to be the types of patient data most often lost or stolen. More data breaches are discovered through audits and assessments followed by employee detections.

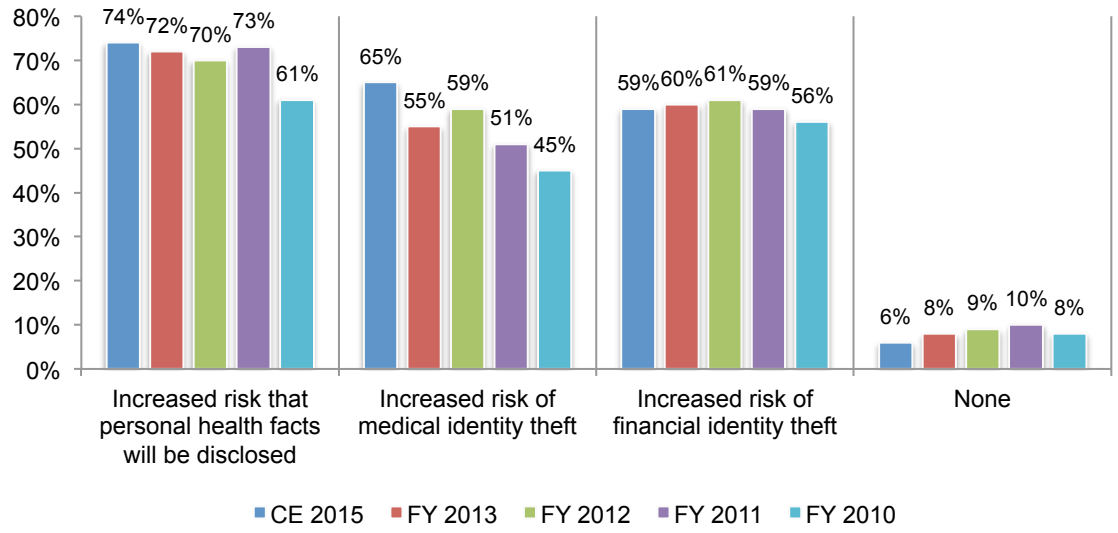
Figure 27. Trends in the type of patient data lost or stolen
More than one response permitted



The economic impact of a data breach stays consistent. Since 2010, there has not been much variance in the average economic impact of a data breach over the past two years. In 2010 it was $2.1 million and in 2015 it was $2.1 million as well.

Most respondents continue to believe a data breach increases the risk that a patient's personal health facts will be disclosed. In 2010, 61 percent believed disclosure of personal health facts was the biggest risk. In this year's report 74 percent believe this is the case. Awareness of the risk of medical identity theft has increased significantly from 45 percent in 2010 to 65 percent of respondents in this year's report.

Figure 28. Trends in perceptions about data breach victims
More than one response permitted



Conclusion

Healthcare organizations and business associates face a rapidly changing threat landscape. Cyber criminals recognize two critical facts of the healthcare industry: 1) healthcare organizations manage a treasure trove of financially lucrative personal information and 2) healthcare organizations do not have the resources, processes, and technologies to prevent and detect attacks and adequately protect patient data. While the findings reveal a slow but steady increase in technologies, the pace of investments is not fast enough to keep up with the threats to achieve a stronger security posture.

Another challenge for the protection of patient information is the need to address two serious but different root causes of security incidents and data breaches: employee negligence and hackers. One requires intensive employee training and awareness programs and the other calls for investments in technologies and security expertise. Innovative solutions are required to achieve both goals.

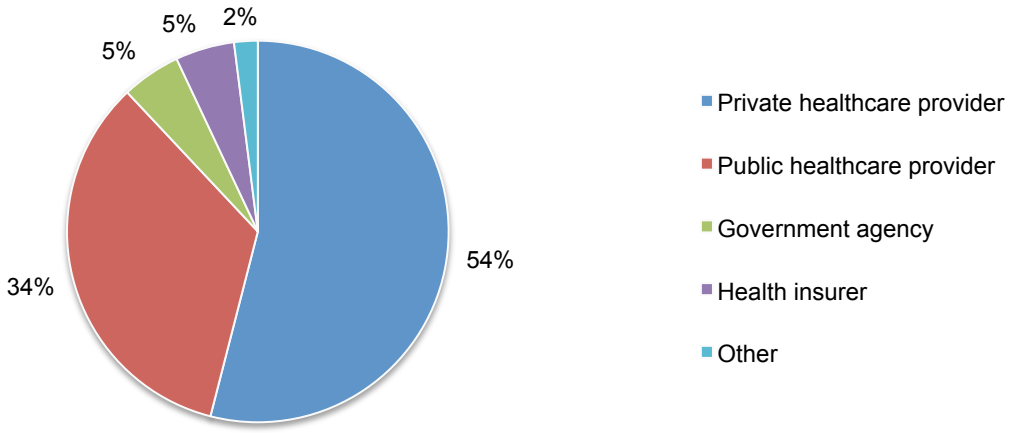
Part 3. Benchmark Methods

Table 1 summarizes the responses completed over a four-week period from February 18, 2015 to March 20, 2015. A total of 525 covered entities and 466 business associates were selected for participation and contacted by the researcher. One hundred and thirteen covered entities and 137 business associates agreed to complete the benchmark survey. The final number of covered entities that actually participated was 90 and 88 business entities completed the benchmark instrument.

Table 1. Benchmark sampling response	CE	BA
Organizations contacted	525	466
Organizations agreeing to participate	113	137
Organizations participating	90	88
Participation rate	17%	19%

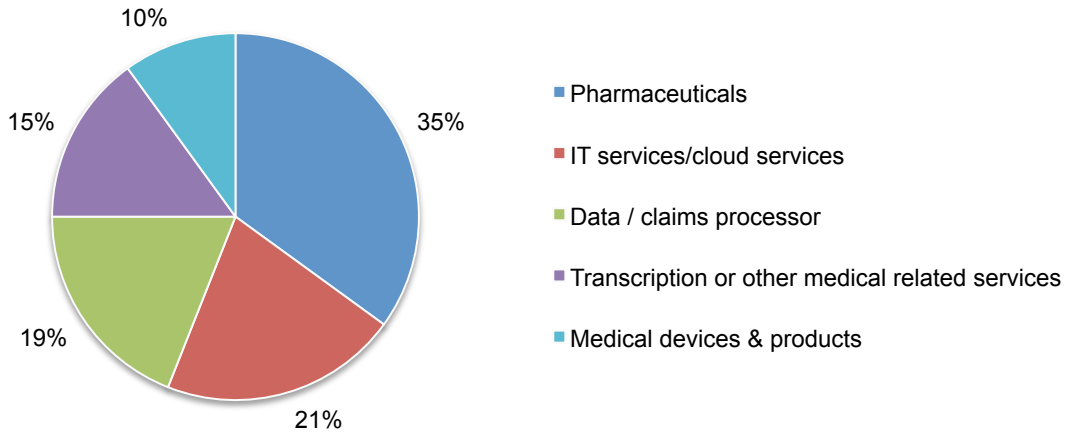
Pie Chart 1 reports the type of category that best describes the respondent's role and their organization. More than half (54 percent) reported they are a private healthcare provider followed by 34 percent that responded public healthcare provider.

Pie Chart 1. Type of covered entity



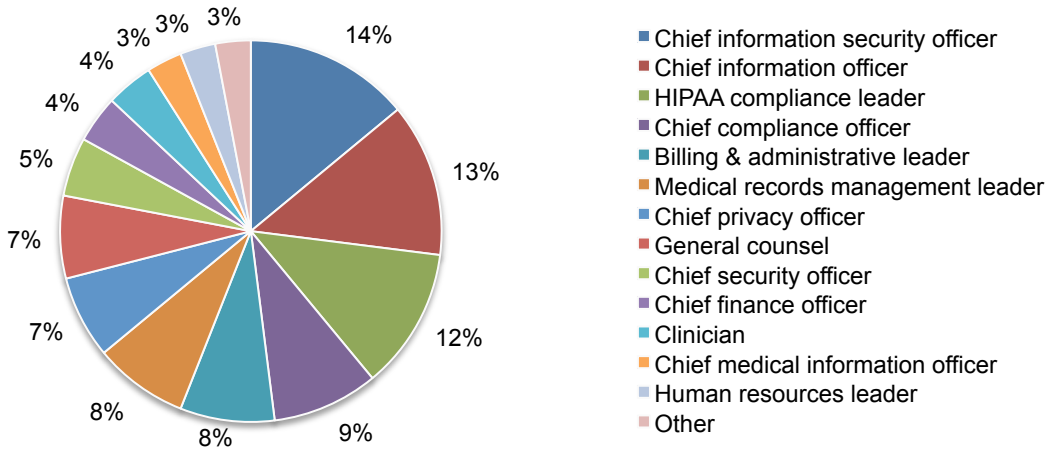
Pie Chart 2 reports the type of category that best describes the respondent's role and their organization. Thirty-five percent of the business associates reported pharmaceuticals as their primary role or organization. Another 21 percent identified IT services/cloud services.

Pie Chart 2. Type of business associate



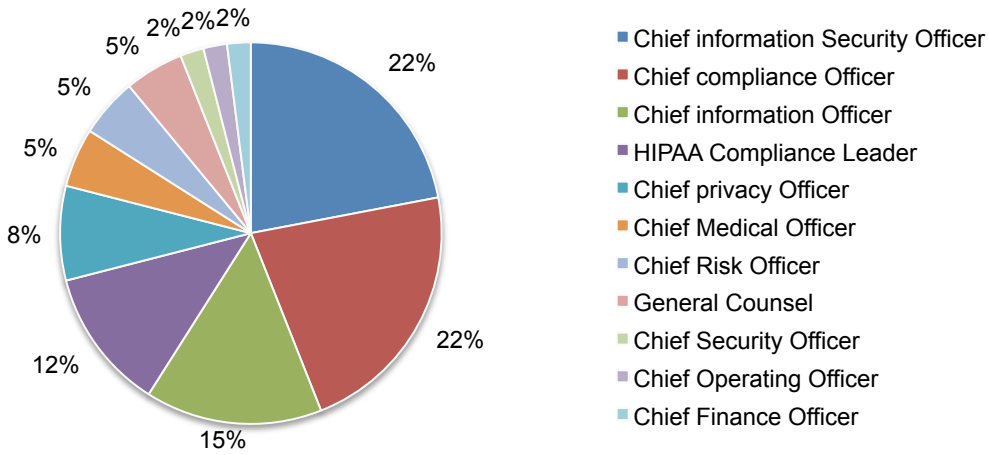
As shown in Pie Chart 3, the primary role for the covered entity is the chief information security officer (14 percent) followed by the chief information officer (13 percent) and HIPAA compliance leader (12 percent).

Pie Chart 3. What best describes the covered entity's role or the role of the supervisor?



Pie Chart 4 reports the primary role for the business associate. Twenty-two percent responded chief information security officer, and an additional 22 percent responded chief compliance officer. Fifteen percent of respondents reported their role as chief information officer.

Pie Chart 4. What best describes the business associate's role or the role of the supervisor?



Figures 29 and 30 identify the department or function for the covered entity and business associate. Both organizations reported compliance (98 percent) as their primary department or function. Another 74 percent of CE and 90 percent of BA respondents identified information technology as their primary function.

Figure 29. What best describes your department or function?

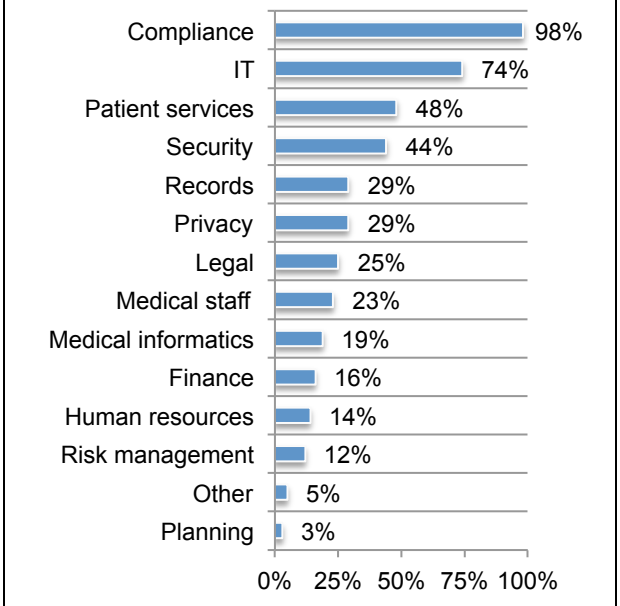
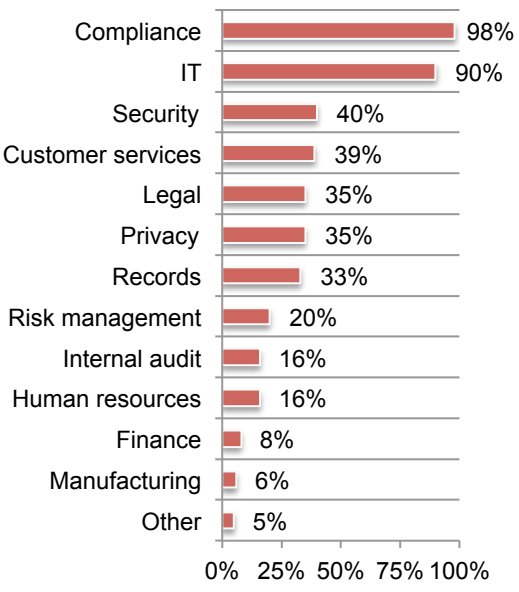


Figure 30. What best describes your department function?



Appendix: Detailed Results

The following tables provide the frequency of all benchmark survey questions completed by 90 covered entities and 88 business associates. All field research was completed over a four-week period from February 18, 2015 to March 20, 2015.

Benchmark study response	CE	BA
Organizations contacted	525	466
Organizations agreeing to participate	113	137
Organizations participating	90	88
Participation rate	17%	19%

Screening Question

S1. Is your organization a covered entity or business associate subject to HIPAA?	CE	BA
Covered entity	100%	0%
Business associate	0%	100%
Neither (Stop)	0%	0%
Total	100%	100%

Part I: Organizational characteristics

Q1. [If S1 = covered entity] Please select the category that best describes your role and your organization.		
Q1a. What best describes your organization:	CE	BA
Public healthcare provider	34%	
Private healthcare provider	54%	
Government agency	5%	
Health insurer	5%	
Healthcare clearinghouse	0%	
Other	2%	
Total	100%	

Q1b. Please indicate the region of the United States where you are located.	CE	BA
Northeast	21%	
Mid-Atlantic	19%	
Midwest	16%	
Southeast	12%	
Southwest	13%	
Pacific-West	19%	
Total	100%	

Q1c. What best describes your role or the role of your supervisor?	CE	BA
Chief security officer	5%	
Chief information security officer	14%	
Chief information officer	13%	
Chief privacy officer	7%	
Chief compliance officer	9%	
Chief medical officer	2%	
Chief clinical officer	1%	
Chief risk officer	0%	
Chief medical information officer	3%	
Chief finance officer	4%	
Chief development officer	0%	
General counsel	7%	
HIPAA compliance leader	12%	
Clinician	4%	
Billing & administrative leader	8%	
Medical records management leader	8%	
Human resources leader	3%	
Total	100%	
Total number of individual interviews	395	
Average number of interviews per organization	4.39	

Q1d. What best describes your department or function?	CE	BA
Compliance	98%	
Privacy	29%	
Information technology (IT)	74%	
Security	44%	
Legal	25%	
Finance	16%	
Marketing	0%	
Medical informatics	19%	
Medical staff	23%	
Patient services	48%	
Records management	29%	
Risk management	12%	
Development (foundation)	0%	
Planning	3%	
Human resources	14%	
Other	5%	
Total	439%	

Q1e. What best describes your organization's privacy and security functions? Please select one.	CE	BA
Privacy and security functions are completely separate	32%	
Privacy and security functions overlap in some places (hybrid)	49%	
Privacy and security functions are combined	19%	
Total	100%	

Q2. [If S1 = business associate] Please select the category that best describes your role and your organization.		
Q2a. What best describes your organization:	CE	BA
Data / claims processor		19%
IT services/cloud services		21%
Medical devices & products		10%
Pharmaceuticals		35%
Government agency		0%
Transcription or other medical related services		15%
Other		0%
Total		100%

Q2b. Please indicate the region of the United States where you are located.	CE	BA
Northeast		19%
Mid-Atlantic		20%
Midwest		16%
Southeast		13%
Southwest		13%
Pacific-West		19%
Total		100%

Q2c. What is your organization's global headcount?	CE	BA
Less than 100		0%
100 to 500		4%
501 to 1,000		24%
1,001 to 5,000		32%
5,001 to 10,000		23%
10,001 to 25,000		12%
More than 25,000		5%
Total		100%

Q2d. What best describes your role or the role of your supervisor?	CE	BA
Chief Security Officer		2%
Chief information Security Officer		22%
Chief information Officer		15%
Chief privacy Officer		8%
Chief compliance Officer		22%
Chief Medical Officer		5%
Chief Risk Officer		5%
Chief Operating Officer		2%
Chief Finance Officer		2%
General Counsel		5%
HIPAA Compliance Leader		12%
Total		100%
Total number of individual interviews		388
Average number of interviews per organization		4.41

Q2e. What best describes your department or function?	CE	BA
Compliance		98%
Privacy		35%
Information technology (IT)		90%
Security		40%
Legal		35%
Finance		8%
Sales / marketing		0%
Logistics		0%
Manufacturing		6%
Customer services		39%
Records management		33%
Risk management		20%
Human resources		16%
Internal audit		16%
Other		5%
Total		441%

Part 2. Attributions. Please rate your opinion about the statements contained in Q3 to Q8 using the scale provided below each item.		
Q3. My organization has sufficient technologies that effectively prevent or quickly detect unauthorized patient data access, loss or theft.	CE	BA
Strongly agree	19%	18%
Agree	30%	28%
Unsure	28%	32%
Disagree	15%	13%
Strongly disagree	8%	9%
Total	100%	100%

Q4. My organization has sufficient resources to prevent or quickly detect unauthorized patient data access, loss or theft.	CE	BA
Strongly agree	15%	18%
Agree	18%	23%
Unsure	35%	35%
Disagree	26%	19%
Strongly disagree	6%	5%
Total	100%	100%

Q5. My organization has personnel who have technical expertise to be able to identify and resolve data breaches involving the unauthorized access, loss or theft of patient data.	CE	BA
Strongly agree	23%	21%
Agree	30%	29%
Unsure	23%	29%
Disagree	18%	17%
Strongly disagree	6%	4%
Total	100%	100%

Q6. Our organization's security budget is sufficient to curtail or minimize data breach incidents.	CE	BA
Strongly agree	16%	18%
Agree	21%	19%
Unsure	35%	36%
Disagree	19%	21%
Strongly disagree	9%	6%
Total	100%	100%

Q7. My organization has personnel who are knowledgeable about HITECH and states' data breach notification laws.	CE	BA
Strongly agree	24%	18%
Agree	25%	19%
Unsure	39%	28%
Disagree	12%	25%
Strongly disagree	0%	10%
Total	100%	100%

Q8. My organization has sufficient policies and procedures that effectively prevent or quickly detect unauthorized patient data access, loss or theft.	CE	BA
Strongly agree	26%	21%
Agree	32%	29%
Unsure	19%	24%
Disagree	19%	21%
Strongly disagree	4%	5%
Total	100%	100%

Part 3: Incident response

Q9. What security threats is your organization most concerned about? Select the top three.	CA	BA
Employee-owned mobile devices or BYOD	29%	36%
Mobile device insecurity	32%	40%
Use of public cloud services	33%	48%
Insecure medical devices	6%	15%
Employee negligence	70%	51%
Malicious insiders	26%	19%
Cyber attackers	40%	35%
Identity thieves	19%	5%
Insecure mobile apps (eHealth)	13%	19%
System failures	15%	19%
Process failures	15%	13%
Other	2%	0%
Total	300%	300%

Q10. Which of these types of incidents did your organization experience? Please check all that apply.	CE	BA
Zero day attacks	23%	45%
Exploit of existing software vulnerability less than 3 months old	45%	44%
Exploit of existing software vulnerability greater than 3 months old	54%	49%
SQL injection	38%	40%
Spyware	29%	26%
Botnet attacks	16%	23%
Clickjacking	15%	26%
Rootkits	9%	11%
DDoS	25%	40%
Web-borne malware attacks	78%	82%
Advanced persistent threats (APT) / targeted attacks	37%	49%
Spear phishing	88%	90%
Lost or stolen devices	96%	95%
Other	2%	2%
Total	555%	622%

Q11a. In the past 24 months, did your organization have a security incident involving the exposure, theft or misuse of electronic information?	CE	BA
Yes	65%	87%
No (skip to Q14a)	35%	13%
Total	100%	100%

Q11b. If yes, how many electronic information-based security incidents did your organization experience over the past 24 months?	CE	BA
1 to 10	36%	18%
11 to 20	35%	29%
21 to 30	23%	41%
31 to 40	6%	9%
41 to 50	0%	3%
More than 50	0%	0%
Total	100%	100%

Q12. What is the average number of PHI records exposed in each security incident involving electronic information?	CE	BA
Less than 10	55%	42%
10 to 100	35%	28%
101 to 1,000	6%	21%
1,001 to 5,000	2%	5%
5,001 to 10,000	1%	2%
10,001 to 100,000	1%	1%
More than 100,000	0%	1%
Total	100%	100%

Q13a. Does your organization perform a 4-factor risk assessment following a security incident that involves electronic information as required under HIPAA Omnibus Final Rule to determine if an incident is a data breach that requires notification under applicable federal and state regulations?	CE	BA
Yes, for each security incident	50%	42%
Yes, for some security incidents	23%	24%
No	20%	24%
Unsure	7%	10%
Total	100%	100%

Q13b. If yes, how does your organization perform a 4-factor risk assessment for electronic incidents?	CE	BA
We engage third parties (outside legal counsel, cyber insurance carriers, auditors, etc.)	10%	6%
An ad hoc process	34%	38%
A manual process or tool that was developed internally	27%	30%
An automated process or software tool that was developed by a third party	13%	10%
An incident response management platform	11%	13%
A free tool that was developed by an external entity or association	5%	3%
Total	100%	100%

Q13c. If yes, who is responsible for performing a 4-factor risk assessment for electronic incidents?	CE	BA
General Counsel	6%	9%
Chief Privacy Officer	10%	4%
Chief Information Officer	11%	13%
Chief Information Security Officer	19%	18%
Compliance Officer	40%	34%
Internal Audit	2%	9%
Chief Security Officer	4%	3%
Chief Risk Officer	6%	8%
Records Management	2%	0%
Other	0%	2%
Total	100%	100%

Q14a. In the past 24 months, did your organization have a security incident involving the exposure, theft, or misuse of paper documents?	CE	BA
Yes	54%	41%
No (skip to Q19a)	46%	59%
Total	100%	100%

Q14b. If yes, in the past 24 months how many paper-based security incidents did your organization experience?	CE	BA
1 to 10	68%	75%
11 to 20	23%	18%
21 to 30	5%	4%
31 to 40	4%	3%
41 to 50	0%	0%
More than 50	0%	0%
Total	100%	100%

Q15. What is the average number of PHI records exposed in incidents involving paper documents?	CE	BA
Less than 10	73%	55%
10 to 100	25%	40%
101 to 1,000	2%	5%
1,001 to 5,000	0%	0%
5,001 to 10,000	0%	0%
10,001 to 100,000	0%	0%
More than 100,000	0%	0%
Total	100%	100%

Q16. Does your organization perform a 4-factor risk assessment following a paper-based security incident as required under HIPAA Omnibus Final Rule to determine if an incident is a data breach that requires notification under applicable federal and state regulations?	CE	BA
Yes, for each security incident	20%	21%
Yes, for some security incidents	33%	28%
No	40%	42%
Unsure	7%	9%
Total	100%	100%

Q17. If yes, how does your organization perform a 4-factor risk assessment for paper-based security incidents?	CE	BA
We engage third parties (outside legal counsel, cyber insurance carriers, auditors, etc.)	0%	2%
An ad hoc process	44%	45%
A manual process or tool that was developed internally	38%	40%
An automated process or software tool that was developed by a third party	13%	8%
An incident response management platform	0%	2%
A free tool that was developed by an external entity or association	5%	3%
Total	100%	100%

Q18. If yes, which function is responsible for performing a 4-factor risk assessment for paper-based security incidents?	CE	BA
General Counsel	9%	6%
Chief Privacy Officer	9%	5%
Chief Information Officer	4%	6%
Chief Information Security Officer	19%	20%
Compliance Officer	45%	40%
Internal Audit	0%	5%
Chief Security Officer	6%	4%
Chief Risk Officer	5%	8%
Records Management	3%	0%
Other	0%	6%
Total	100%	100%

Q19a. Does your organization have an incident response process in place?	CE	BA
Yes	69%	65%
No (Go to Q25)	31%	35%
Total	100%	100%

Q19b. Who is involved in the incident response process? Please check all that apply.	CE	BA
Legal	18%	38%
Compliance	79%	69%
Internal Audit	13%	28%
Privacy Office	58%	51%
Information Technology	88%	91%
Information Security	84%	95%
Human Resources	47%	24%
Security	26%	43%
Risk Management	30%	20%
Corporate Communications	27%	39%
Records Management	5%	0%
Other	0%	3%
Total	475%	498%

Q20. What percentage of your organization's **security** budget is allocated to incident response? Please include personnel, services and technology costs/investments in your estimate? Your best guess is welcome.	CE	BA
Less than 10%	28%	26%
10% to 20%	48%	52%
21% to 30%	19%	18%
31% to 40%	5%	4%
41% to 50%	0%	0%
More than 50%	0%	0%
Total	100%	100%

Q21. How has this percentage changed over the past 24 months?	CE	BA
Increased	33%	35%
Decreased	11%	9%
Stayed the same	50%	48%
Cannot determine	6%	8%
Total	100%	100%

Q22. What percentage of your organization's **privacy** budget is allocated to incident response? Please include personnel, services and technology costs/investments in your estimate? Your best guess is welcome.	CE	BA
Less than 10%	12%	16%
10% to 20%	33%	36%
21% to 30%	25%	23%
31% to 40%	25%	25%
41% to 50%	5%	0%
More than 50%	0%	0%
Total	100%	100%

Q23. How has this percentage changed over the past 24 months?	CE	BA
Increased	44%	45%
Decreased	5%	9%
Stayed the same	45%	38%
Cannot determine	6%	8%
Total	100%	100%

Q24. Do you believe your incident response process has adequate funding and resources?	CE	BA
Yes	44%	41%
No	56%	59%
Total	100%	100%

Part 4: Data Breach

Q25. Has your organization suffered a data breach involving the loss or theft of patient data in the past 24 months as defined above?	CE	BA
No	9%	41%
Yes, 1 breach	12%	30%
Yes, 2 to 5 breaches	39%	14%
Yes, more than 5 breaches	40%	15%
Total	100%	100%

Q26. How confident are you that your organization has the ability to detect **all** patient data loss or theft?	CE	BA
Very confident	16%	13%
Confident	33%	29%
Little confidence	31%	34%
No confidence	20%	24%
Total	100%	100%

Q27. Two separate data breaches over the past two years.	CE	BA
Number of breaches reported	361	304
Number of observed incidents used in the analysis of Q27	170	161

Q27a. Approximate number of compromised records	CE	BA
< 10	3%	0%
10 to 100	50%	54%
101 to 1,000	24%	15%
1,001 to 5,000	15%	15%
5,001 to 10,000	6%	11%
10,001 to 100,000	1%	3%
> 100,000	1%	2%
Total	100%	100%
Extrapolated average number of lost or stolen records over two years	2,710	5,237

Q27b. Nature of the breach	CE	BA
Unintentional employee action	40%	51%
Intentional non-malicious employee action	7%	4%
Technical systems glitch	31%	27%
Criminal attack	45%	39%
Malicious insider	12%	10%
Third-party snafu	39%	49%
Lost or stolen computing device	43%	35%
Total	217%	215%

Q27c. Type of device compromised or stolen	CE	BA
Desktop or laptop	26%	32%
Smartphone	29%	23%
Tablet	29%	29%
Notebook	0%	0%
Server	2%	3%
USB drive	14%	13%
Total	100%	100%

Q27d. Type of patient data lost or stolen	CE	BA
Medical file	55%	23%
Billing and insurance record	46%	55%
Scheduling details	18%	6%
Prescription details	18%	21%
Payment details	20%	41%
Monthly statements	15%	6%
Other	2%	3%
Total	174%	155%

Q27e. How the data breach was discovered	CE	BA
Accidental	23%	33%
Loss prevention	5%	13%
Patient complaint	30%	17%
Law enforcement	6%	12%
Legal complaint	18%	21%
Employee detected	44%	60%
Audit/assessment	69%	49%
Total	195%	205%

Q27f. Offer of protection services	CE	BA
None offered	65%	63%
Credit monitoring	19%	14%
Other identity monitoring	10%	9%
Insurance	0%	0%
Identity restoration	6%	7%
Financial incentives (i.e., gift cards)	0%	7%
Other	0%	0%
Total	100%	100%

Q28. In your opinion (best guess), what best describes the lifetime economic value, on average, of one patient or customer to your organization?	CE	BA
Less than $10,000	11%	69%
$10,001 to $50,000	33%	16%
$50,001 to $100,000	18%	3%
$100,001 to $200,000	19%	1%
$200,001 to $500,000	6%	0%
$500,001 to $1 million	2%	0%
More than $1 million	1%	0%
Cannot determine	10%	11%
Total	100%	100%
Average lifetime value of one patient or customer	110,989	16,584

Q29. In your opinion (best guess), what best describes the economic impact of data breaches incidents experienced by your organization over the past two years?	CE	BA
Less than $10,000	4%	3%
$10,001 to $50,000	4%	5%
$50,001 to $100,000	6%	21%
$100,001 to $200,000	9%	27%
$200,001 to $500,000	21%	15%
$500,001 to $1 million	24%	12%
More than $1 million	27%	12%
Cannot determine	5%	5%
Total	100%	100%
Average economic impact of data breach over the past two years	2,134,800	1,032,126

Q30. In your opinion, what harms do patients actually suffer if their records are lost or stolen?	CE	BA
Increased risk of financial identity theft	59%	44%
Increased risk of medical identity theft	65%	23%
Increased risk that personal health facts will be disclosed	74%	69%
None	6%	19%
Total	204%	155%

Q31a. Are you aware of any cases of medical identity theft that affected your patients or customers during the past 24 months?	CE	BA
Yes	33%	25%
No	50%	60%
Unsure	17%	15%
Total	100%	100%

Q31b. If yes, what were the root causes of the medial identity theft?	CE	BA
Unintentional employee action	50%	22%
Intentional non-malicious employee action	17%	30%
Technical system glitches/authentication failure	0%	0%
Criminal attack	7%	9%
Malicious insider	13%	22%
Third-party snafu	10%	13%
Stolen computing device	3%	4%
Unsure	0%	0%
Total	100%	100%

Part 5: Cloud Services

Q32. What best describes your organization's use of cloud services?	CE	BA
No use of cloud services (skip to Q36a)	5%	0%
Light use of cloud services	15%	11%
Moderate use of cloud services	40%	52%
Heavy use of cloud services	40%	37%
Total	100%	100%

Q33. What cloud applications or services does your organization presently use? Please select all that apply.	CE	BA
Peer-to-peer communications (such as Skype)	37%	35%
Social media applications (such as Facebook, LinkedIn, Twitter, etc.)	33%	41%
Business applications (such as SalesForce.com, webmail, HR, etc.)	56%	63%
Document sharing and collaboration (such as Dropbox, Google Docs, etc.)	47%	51%
Infrastructure applications (online backup, security, archiving, etc.)	36%	30%
Services such as identity management, payments and others	33%	38%
Solution stacks such as Java, PHP, Python, ColdFusion and others	18%	25%
Backup & storage	49%	48%
Other	2%	3%
Total	311%	334%

Q34. What types of information does your organization process and/or store in a public cloud environment? Please select all that apply.	CE	BA
Patient medical records	35%	33%
Patient billing information	35%	36%
Clinical trial and other research information	3%	4%
Employee information including payroll data	50%	51%
Administrative and scheduling information	32%	15%
Accounting and financial information	50%	39%
Email applications	60%	45%
Productivity applications	47%	49%
None of the above	25%	19%
Other	3%	4%
Total	340%	295%

Q35. What types of information does your organization consider **too sensitive** to be processed and/or stored in a public cloud environment? Please select all that apply.	CE	BA
Patient medical records	50%	44%
Patient billing information	47%	36%
Clinical trial and other research information	56%	67%
Employee information including payroll data	23%	18%
Administrative and scheduling information	19%	18%
Accounting and financial information	29%	36%
Email applications	9%	10%
Productivity applications	12%	15%
None of the above	38%	41%
Other	3%	4%
Total	286%	289%

Part 6. General Questions

Q36a. Does your organization use (or plan to use) big data analytics involving the use of health information (PHI)?	CE	BA
Yes, presently doing so	23%	30%
Yes, plan to do so within the next 12 months	43%	45%
Yes, plan to do so in more than 12 months	15%	10%
No plans	19%	15%
Total	100%	100%

Q36b. If yes, how concerned is your organization about preserving the privacy of health information when using this technology?	CE	BA
Very concerned	18%	20%
Concerned	32%	37%
Not concerned	50%	43%
Total	100%	100%

Q37a. Does your organization use (or plan to use) patient lifestyle data (such fitness programs, eating habits, stress levels, etc.) to comply with healthcare regulations and insurance requirements?	CE	BA
Yes, presently doing so	35%	21%
Yes, plan to do so within the next 12 months	33%	39%
Yes, plan to do so in more than 12 months	12%	17%
No plans	20%	23%
Total	100%	100%

Q37b. If yes, how concerned is your organization about preserving the privacy of health information when collecting and using lifestyle data?	CE	BA
Very concerned	20%	20%
Concerned	33%	36%
Not concerned	47%	44%
Total	100%	100%

Q38a. How does the Affordable Care Act (a.k.a. Obamacare) affect the privacy and security of patient information?	CE	BA
Significantly increases risk	32%	28%
Increases risk	29%	26%
No impact on risk	18%	29%
Decreases risk	8%	7%
Significantly decreases risk	6%	5%
Cannot determine	7%	5%
Total	100%	100%

Q38b. If you believe the Affordable Care Act increases the risk to the privacy of health information, what are your primary concerns? Please select all that apply.	CE	BA
Patient registration on insecure websites	65%	56%
Patient data on insecure databases	75%	80%
Insecure exchange of patient data between healthcare providers and government	88%	68%
Other	4%	3%
Total	232%	207%

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.