Ponemon INSTITUTE

Sixth Annual Benchmark Study on Privacy & Security of Healthcare Data

Sponsored by ID Experts

Independently conducted by Ponemon Institute LLC

Publication Date: May 2016

Sixth Annual Benchmark Study on Privacy & Security of Healthcare Data

Presented by Ponemon Institute, May 2016

Part 1. Executive Summary

The Sixth Annual Benchmark Study on Privacy & Security of Healthcare Data reveals that the majority of healthcare organizations represented in this study have experienced multiple data breaches. Despite the increased frequency of breaches, the study found that many organizations lack the money and resources to manage data breaches caused by evolving cyber threats, preventable mistakes, and other dangers.

For the second year, the study has been expanded beyond healthcare organizations to include business associates. Represented in this study are 91 covered entities[1] (hereafter referred to as healthcare organizations) and 84 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 patient data and data breaches—including causes and top threat concerns—as well as their management of data breach response.

Data breaches in healthcare are increasingly costly and frequent, and continue to put patient data at risk. Based on the results of this study, we estimate that data breaches could be costing the healthcare industry $6.2 billion.[2] Nearly 90 percent of healthcare organizations represented in this study had a data breach in the past two years, and nearly half, or 45 percent had more than five data breaches in the same time period. The majority of these breaches were small, containing fewer than 500 records.

According to the findings of this research, over the past two years the average cost of a data breach for healthcare organizations is estimated to be more than $2.2 million. No healthcare organization, regardless of size, is immune from data breach. Over the past two years, the average cost of a data breach to BAs represented in this research is more than $1 million. Despite this, about half of all organizations have little or no confidence that they can detect all patient data loss or theft. Although there's been a slight increased investment over last year in technology, privacy and security budgets, and personnel with technical expertise, the majority of healthcare organizations still don't have sufficient security budget to curtail or minimize data breach incidents.

For the second year in a row, criminal attacks are the leading cause of data breaches in healthcare. In fact, 50 percent of healthcare organizations say the nature of the breach was a criminal attack and 13 percent say it was due to a malicious insider.

In the case of BAs, 41 percent say a criminal attacker caused the breach and nine percent say it

---

[1] Covered entities are defined in the HIPAA rules as (1) health plans, (2) health care clearinghouses, and (3) health care providers who electronically transmit any health information in connection with transactions for which HHS has adopted standards. Business associates provide services or activities to a covered entity that involve the use or disclosure of individually identifiable health information. For a more complete description visit:
http://privacyruleandresearch.nih.gov/pr_06.asp.

[2] This is based on multiplying $1,112,771.50 (50% of the average two year cost of a data breach experienced by the 91 healthcare organizations in this research) x 5,627 (the total number of registered U.S. hospitals per the AHA).

was due to a malicious insider. Indeed, cyber attacks remain a primary concern for healthcare organizations. In 2016, ransomware, malware, and denial-of-service (DOS) attacks are the top cyber threats facing healthcare organizations. Healthcare organizations and BAs alike are also significantly concerned about employee negligence, mobile device insecurity, use of public cloud services, and employee-owned mobile devices or BYOD—all threats to sensitive and confidential information. On the wireless front, there is a growing concern over the security of mobile apps (eHealth), up to 19 percent for healthcare organizations.

The research found that many healthcare organizations and their business associates are negligent in the handling of patient information. While external threats dominate, internal problems such as mistakes—unintentional employee actions, third-party snafus, and stolen computing devices—are equally a problem and account for a significant percentage of data breaches. In fact, 36 percent of healthcare organizations and 55 percent of BAs named unintentional employee action as a breach cause.

Healthcare organizations and business associates differ slightly on which of these internal problems is a larger threat to patient data. For example, 41 percent of healthcare organizations say third parties cause breaches while 52 percent of business associates blame third-party snafus. This brings up the issue of accountability when it comes to protecting patient information.

Despite these differences, the vast majority of all respondents agree that healthcare organizations are more vulnerable to data breach than other industries. More than half of covered entities in the survey say they are not vigilant in ensuring partners and third parties protect patient information. The majority of both healthcare organizations and BAs have not invested in the technologies necessary to mitigate a data breach, nor have they hired enough skilled IT security practitioners. In addition, 59 percent of healthcare organizations and 60 percent of BAs don't think or are unsure that their organization's security budget is sufficient to curtail or minimize data breaches. Similarly, more than half of healthcare organizations, or 56 percent, do not believe their incident response process has adequate funding and resources.

Patients are suffering the effects of data breach. Thirty-eight percent of healthcare organizations and 26 percent of BAs are aware of medical identity theft cases affecting patients and customers. However, a significant number of respondents—62 percent of healthcare organizations and 74 percent of BAs—are not aware or are unsure if this crime has affected their patients or customers. However, the majority of healthcare professionals believe that patients affected by data breach are at greater risk for financial and medical identity theft and having their personal health information exposed. Case in point: medical files, billing and insurance records, and payment details top the list of the type of patient data that is typically breached, accessed without authorization, lost, or stolen. Approximately two-thirds of all respondents don't offer any protection services for breach victims, nor do the majority have a process in place for correcting errors in victims' medical records.

Since 2010, this study has tracked privacy and security trends of patient data at healthcare organizations. The annual economic impact of a data breach has risen over the past six years, as has the frequency of data breaches. Criminal attacks and internal threats are the leading cause of data breaches. Evolving cyber attack threats such as ransomware and malware are of primary concern for 2016. At the same time, internal issues such as employee negligence, third-party snafus, and stolen computing devices continue to put patient data at risk.

Recent big healthcare data breaches have increased the healthcare industry's awareness of the growing threats to patient data, resulting in more focus on their security practices and implementing the appropriate policies and procedures, however the research indicates that it is not enough to curtail or minimize data breaches. According to the findings, half of these organizations still don't have the people or the budget to detect or manage data breaches.

Summary of key findings

- **Privacy and security of patient data in healthcare organizations and business associates**

Healthcare organizations and business associates believe they are more vulnerable than other industries to a data breach. An overwhelming majority of healthcare organizations (69 percent) and business associates (63 percent) believe they are at greater risk than other industries for a data breach. The top reasons for healthcare organizations are a lack of vigilance in ensuring their partners and other third parties protect patient information (51 percent) and not enough skilled IT security practitioners (44 percent). In contrast, business associates say their vulnerabilities are due to employees' negligence in handling patient information (54 percent) and a lack of technologies to mitigate a data breach (50 percent).

Recent well-publicized data breaches in healthcare have put the industry on alert. Sixty-seven percent of healthcare organizations and 62 percent of business associates say these data breaches affected their security practices. Both types of organizations are taking the same steps: more vigilance in ensuring their partners and other third parties safeguard patient information, more investments in technologies to mitigate a data breach and increased employee training.

Healthcare organizations continue to depend mainly upon policies and expertise to respond to data breaches. Sixty-three percent of respondents agree that policies and procedures are in place to effectively prevent or quickly detect unauthorized patient data access, loss or theft. This is an increase from 58 percent in the 2015 study. Fifty-seven percent of respondents say they have the personnel with technical expertise to be able to identify and resolve data breaches involving the unauthorized access, loss or theft of patient data and this is an increase from 53 percent in 2015.

More than half (54 percent of respondents) believes their organizations have technologies to effectively prevent or quickly detect unauthorized patient data access, loss or theft. This is an increase from 49 percent of respondents in 2015. Also, agreement that organizations have resources to prevent or quickly detect unauthorized patient data access, loss or theft has increased from 33 percent of respondents to 37 percent of respondents.

Business associates also rely upon policies and procedures. Fifty-three 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. In addition, business associates are making progress in strengthening the security posture of their organizations. Fifty-one percent of respondents say their organizations have technologies to effectively prevent or quickly detect unauthorized patient data access, loss or theft. This is an increase from 46 percent of respondents in 2015.

Fifty-one percent of respondents 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. This is virtually unchanged since 2015.

Employee negligence continues to be the greatest concern. When healthcare organizations were asked what type of security incident worries them most, by far it is the negligent or careless employee (69 percent of respondents). Forty-five percent of respondents say it is cyber attackers and 30 percent say it is the use of insecure mobile devices. These findings are virtually unchanged since 2015.

Employee negligence is a concern for business associates as well. When asked what type of security incident concerns them most, it is the negligent or careless employee (53 percent of respondents). This is followed by 46 percent of respondents who say it is use of cloud services and 36 percent who say it is cyber attackers. These findings are similar to last year's study.

Healthcare and business associates are most concerned about denial of service (DoS) attacks. Almost half of respondents in both organizations (48 percent) worry about DoS attacks against their organizations. This is followed by ransomware and malware.

The majority of organizations assess vulnerabilities to a data breach, but it is a rare event. Sixty percent of respondents in healthcare organizations and 54 percent of respondents in business associates say their organizations assess vulnerabilities to a data breach. However, it is most often done on an annual basis (41 percent and 33 percent, respectively) or ad hoc (no regular schedule) (43 and 35 percent, respectively).

Healthcare organizations continue to put incident response processes in place. Healthcare organizations recognize the need to have a formal incident response process in place. Seventy-one percent of organizations have a process with involvement from information technology, information security and compliance, an increase from 69 percent of respondents in last year's study. The majority of respondents (51 percent) say their healthcare organizations have the in-house expertise to respond effectively to a data breach.

Of the healthcare organizations that have an incident response plan and the necessary expertise, the majority (56 percent) says more funding and resources are needed to make it effective. Seventy-seven percent of organizations (17 percent + 60 percent) allocate 20 percent or less of the security budget allocated to incident response. Forty-one percent of organizations (11 percent + 30 percent) allocate less than 20 percent of the privacy budget to incident response.

Business associates recognize the need to have a formal incident response process in place. Sixty-four percent of the respondents say their organizations have a process with involvement from information technology, information security and compliance. However, only 46 percent of respondents say they have the in-house expertise to respond effectively to a data breach.

Of the healthcare organizations that have an incident response plan and the necessary expertise, there is not enough funding and resources needed to make incident response effective (59 percent). Sixty-three percent of respondents say less than 20 percent of the security budget is allocated to data breach response and 52 percent of respondents allocate 20 percent or less of the privacy budget to incident response.

Despite concerns about the vulnerability of these organizations to a data breach, budgets do not budge. Healthcare organizations report budgets have decreased (10 percent) or stayed the same (52 percent). Similarly, most business associates must deal with budgets that decrease (11 percent) or stay the same (50 percent).

Information technology is held ultimately accountable for the data breach incident response process. Accountability for the data breach incident response process is dispersed throughout the organization. However, both healthcare organizations (30 percent of respondents) and business associates (41 percent of respondents) say information technology is the function most accountable for the data breach response process. Corporate compliance is more likely to be held accountable in healthcare organizations.

Healthcare organizations are more likely than business associates to engage a third party. To help with incident response**,** 40 percent of respondents say their healthcare organizations hire a third party, and they are mainly outside legal counsel (65 percent of respondents) followed by a forensic/IT security provider (48 percent). Thirty-three percent of respondents in business associates say their organizations hire a third party. Similarly, business associates tend to hire legal counsel and forensic/IT security provider.

- **Data breaches in healthcare organizations and business associates**

Data breaches affect all organizations. Eighty-nine percent of healthcare organizations had at least one data breach involving the loss or theft of patient data in the past 24 months. Forty-five percent had more than 5 breaches. Sixty-one 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, 28 percent say their organization had more than 2 breaches.

Healthcare organizations are more confident than business associates in their ability to detect all patient data loss or theft. Healthcare organizations and business associates are both relatively confident they can determine if patient data was stolen or lost. If patient data was lost or stolen, 53 percent of healthcare organizations (18 percent + 35 percent) and 45 percent of business associates (15 percent + 30 percent) are very confident or confident they would be able to detect the loss or theft.

Healthcare 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 $2.2 million to resolve the consequences of a data breach involving an average of 3,128 lost or stolen records. Seventy-four percent of respondents say the data breach was discovered by an audit or assessment, an increase from 69 percent in last year's study. Forty-seven percent say an employee detected the data breach. Patient complaints revealed the data breach, according to 31 percent of respondents.

Criminal attacks are the root cause of most data breaches. The challenge healthcare organizations face is dealing with data breaches with many possible root causes. Fifty percent of healthcare organizations report the root cause of the breach was a criminal attack, 41 percent of respondents say it was caused by a third-party snafu and 39 percent of respondents say it was due to a stolen computing device. Only 13 percent say it was due to a malicious insider.

Successful attacks targeting medical files and billing and insurance records increased. These contain the most valuable patient data and most often successfully targeted (64 percent of respondents and 45 percent of respondents, respectively).

Business associates 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 5,887 lost or stolen records. Fifty-eight percent of respondents say an employee discovered the data breach and 50 percent say it was discovered through an audit or assessment. Thirty-five percent say the data breach was only discovered accidentally.

Business associates face the challenge of dealing with data breaches due to many different root causes. Fifty-five percent of respondents say it was an unintentional employee action, 52 percent of respondents say it was caused by a third-party snafu and 41 percent of respondents say it was due to a criminal attack. Only 6 percent say it was due to an intentional non-malicious employee action.

Billing and insurance records are at risk in business associates. In contrast to healthcare organizations, billing and insurance records are most often successfully targeted (56 percent of respondents) in business associates. Also frequently lost or stolen are payment details (45 percent of respondents).

Healthcare 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, only 19 percent of respondents in healthcare say they have a process in place to correct errors in victim's medical records. Similar to last year's study, 79 percent of respondents say there is an increased risk that personal health facts will be disclosed and 61 percent believe patients who have had their

records lost or stolen are more likely to become victims of financial identity theft. Sixty-six percent of respondents say the risk of medical identity theft increases.

According to healthcare organizations, most medical identity theft is preventable through employee training. Sixty-two percent of respondents say they are not aware or are unsure of any medical identity theft affecting their patients. Of the 38 percent who say they know about medical identity theft, the root cause most often was unintentional employee action (48 percent of respondents) followed by intentional but non-malicious employee action (15 percent of respondents).

Business associates 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, only 11 percent of respondents in business associates say they have a process in place to correct errors in victim's medical records. Sixty-seven percent of respondents say there is an increased risk that personal health facts will be disclosed and 46 percent of respondents say the risk of financial identity theft increases.

Insiders in business associates are the main root cause of medical identity theft. Seventy-four percent of BA respondents say they are not aware or are unsure of any medical identity theft affecting their patients. Of the 26 percent who say they know about medical identity theft, the root cause most often was the intentional but non-malicious employee action (33 percent of respondents). Unintentional employee action and malicious insiders (both 20 percent) were also considered a root cause.

Following a data breach, should credit monitoring or medical identity theft protection be provided? Fifty-six percent of healthcare organization respondents and 52 percent of business associate respondents say victims of data breaches should be protected. Most respondents believe credit monitoring or medical identity theft protection should be offered for a minimum of two to three years. However, 64 percent of healthcare organizations and 67 percent of business associates don't offer any protection services for victims whose information has been breached.

- **Data breach insurance for healthcare organizations and business associates**

To minimize the financial consequences, some healthcare organizations have purchased data breach insurance policies. One-third of healthcare organizations have a data breach insurance policy and 29 percent of business associates have a cyber breach insurance policy. Fifty-seven percent of healthcare organizations and 52 percent of business associates say they purchase up to $5 million in coverage. Insurance typically covers external attacks by cyber criminals (56 percent of healthcare respondents and 57 percent of business associates) and incidents affecting business partners, vendors or other third parties that have access to the organizations information assets (48 percent of healthcare respondents and 52 percent of business associates).

Legal defense and forensics and investigative costs are most often covered under these policies. Seventy-one percent of healthcare respondents and 73 percent of business associates say their insurance will cover legal defense costs and 65 percent of healthcare respondents and 68 percent of business associate respondents say forensics and investigative costs are covered. Brand damages and communication costs to regulators are rarely covered.

Cyber insurers most often provide credit monitoring and identity protection services. When asked what services the cyber insurer provides in addition to cost coverage, most respondents (78 percent of healthcare and 80 percent of business associates) say their organization provides credit-monitoring services and identity protection services for data breach victims (74 percent of healthcare respondents and 79 percent of business associates).

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 following three topics:

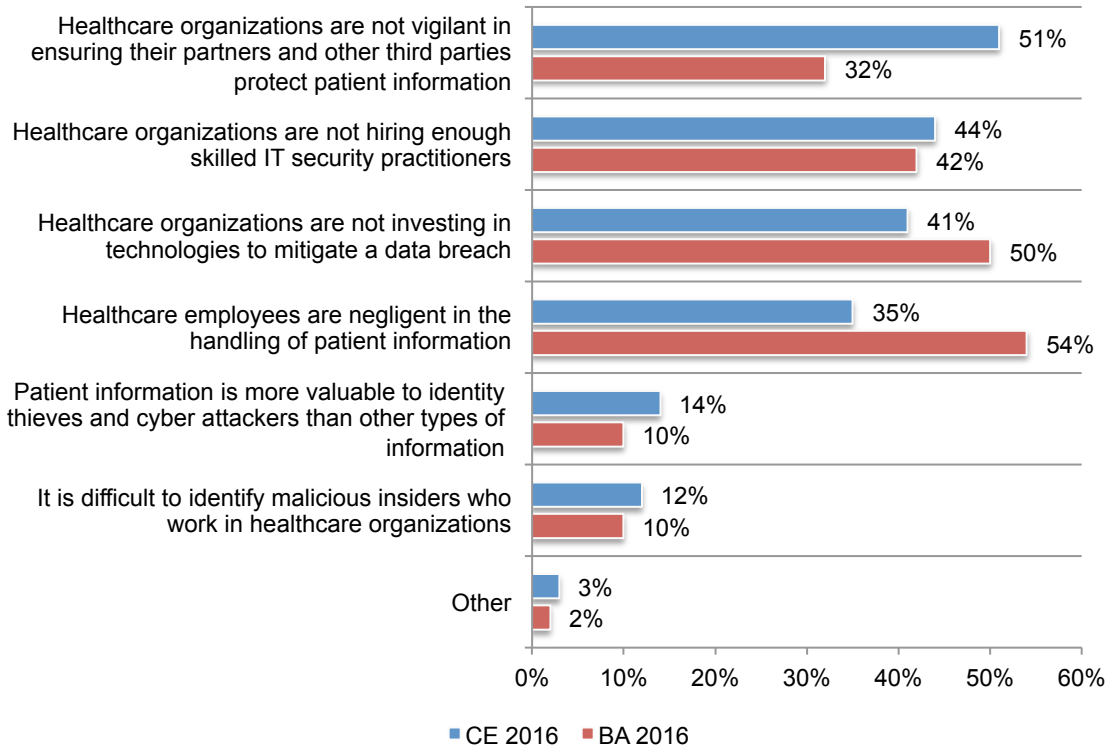
- Privacy and security of patient data in healthcare organizations and business associates
- Data breaches in healthcare organizations and business associates
- Data breach insurance for healthcare organizations and business associates

Privacy and security of patient data in healthcare organizations and business associates

Healthcare organizations and business associates believe they are more vulnerable to a data breach than other industries. An overwhelming majority of healthcare organizations (69 percent) and business associates (63 percent) believe they are at greater risk for a data breach than other industries.

As shown in Figure 1, the top reasons for healthcare is that these organizations do not believe they are vigilant in ensuring their partners and other third parties protect patient information (51 percent) and they are not hiring enough skilled IT security practitioners (44 percent). In contrast, business associates say their employees are negligent in handling patient information (54 percent) and they are not investing in technologies to mitigate a data breach (50 percent).

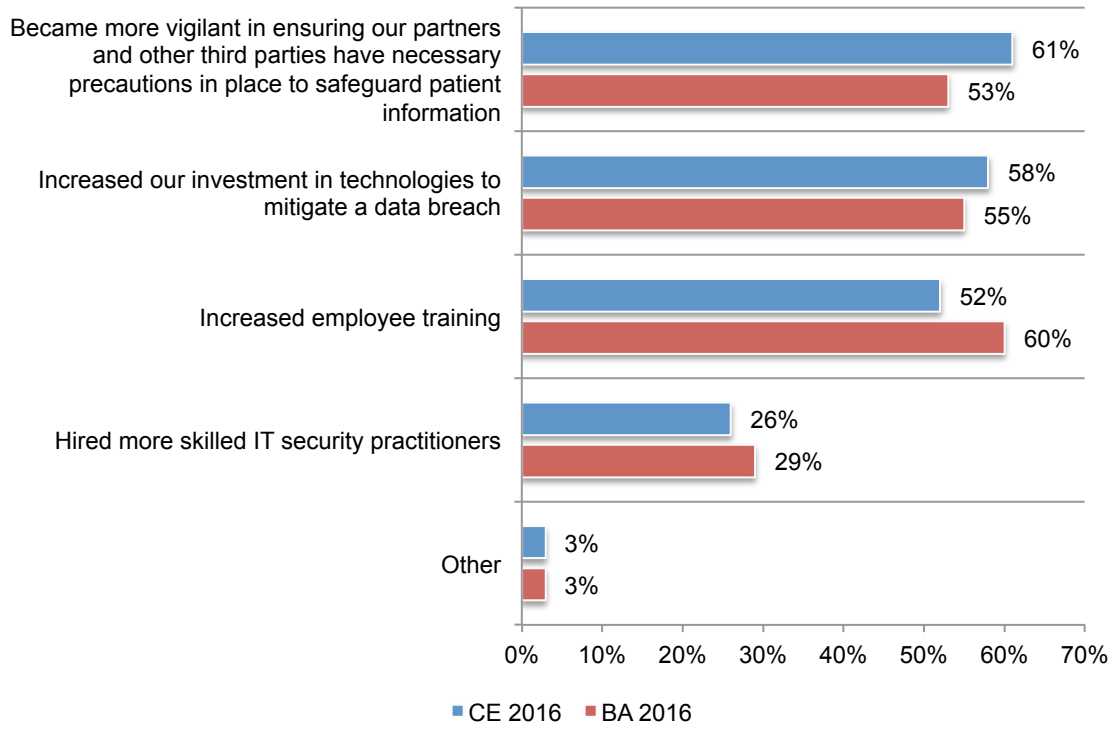
Figure 1. Reasons why healthcare and business associates believe they have a target on their backs
Two choices permitted



Recent well-publicized data breaches in healthcare have put the industry on alert. Sixty-seven percent of healthcare organizations and 62 percent of business associates say these data breaches affected their security practices.

As shown in Figure 2, both types of organizations are taking the same steps: more vigilance in ensuring their partners and other third parties safeguard patient information, more investments in technologies to mitigate a data breach and increased employee training.

Figure 2. How have recent healthcare data breaches affected your security practices?
Two choices permitted

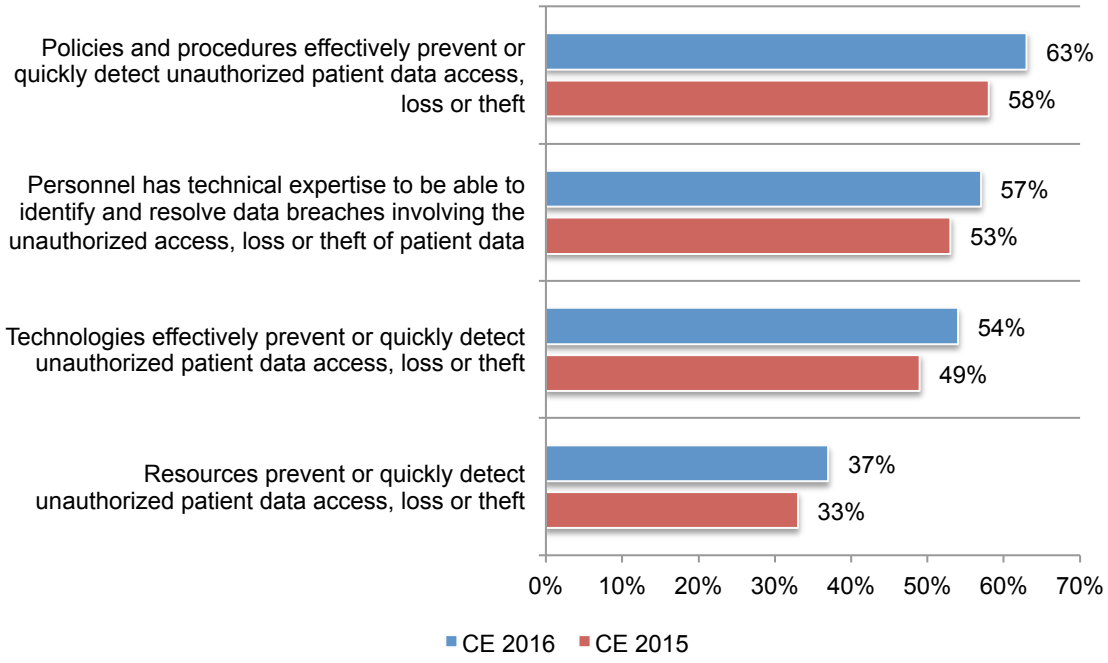


Healthcare organizations depend mainly upon policies and expertise to respond to data breaches. As shown in Figure 3, 63 percent of respondents agree that policies and procedures are in place to effectively prevent or quickly detect unauthorized patient data access, loss or theft. This is an increase from 58 percent in the 2015 study. Fifty-seven percent of respondents say they have the personnel with technical expertise to be able to identify and resolve data breaches involving the unauthorized access, loss or theft of patient data and this is an increase from 53 percent in 2015.

On a positive note, more than half (54 percent of respondents) believe their organizations have technologies to effectively prevent or quickly detect unauthorized patient data access, loss or theft. This is an increase from 49 percent of respondents in 2015. Also agreement that organizations have resources to prevent or quickly detect unauthorized patient data access, loss or theft has increased from 33 percent of respondents to 37 percent of respondents.

Figure 3. Healthcare organizations' perceptions about privacy and healthcare data protection

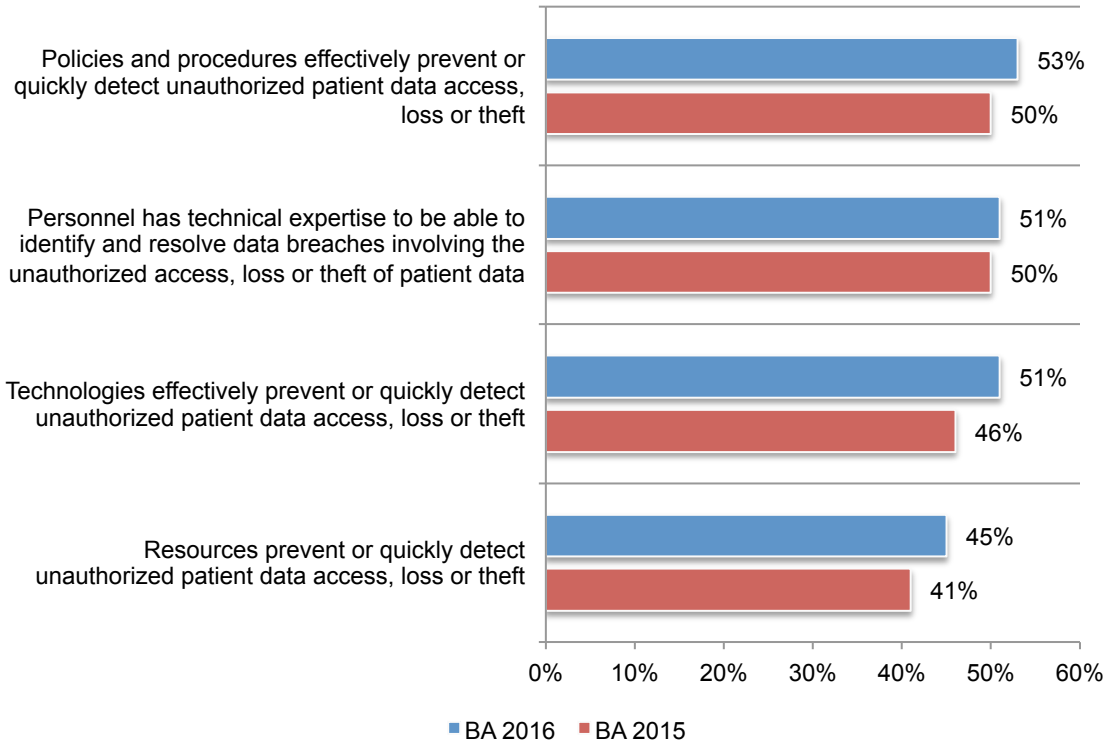
Strongly agree and agree responses combined



According to Figure 4, 53 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. In addition, business associates are making progress in strengthening the security posture of their organizations. Fifty-one percent of respondents say their organizations have technologies to effectively prevent or quickly detect unauthorized patient data access, loss or theft. This is an increase from 46 percent of respondents in 2015.

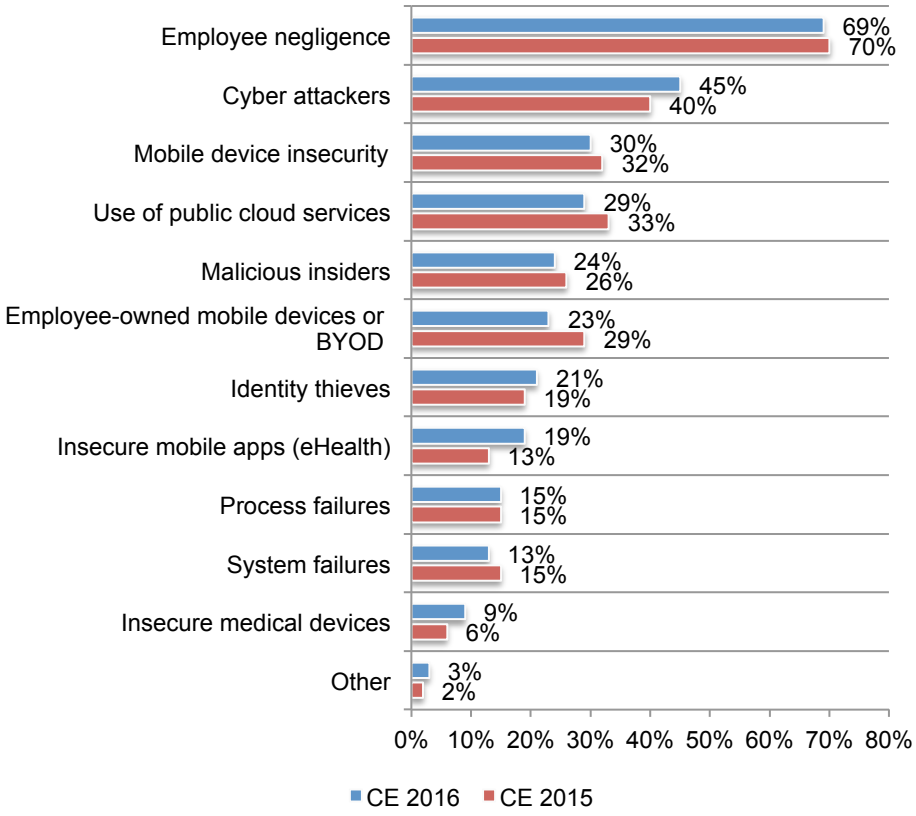
Fifty-one percent of respondents say their organization has personnel with the necessary technical expertise to be able to identify and resolve data breaches involving the unauthorized access, loss or theft of patient data. This is virtually unchanged since 2015.

Figure 4. Business associates' perceptions about privacy and healthcare data protection
Strongly agree and agree responses combined



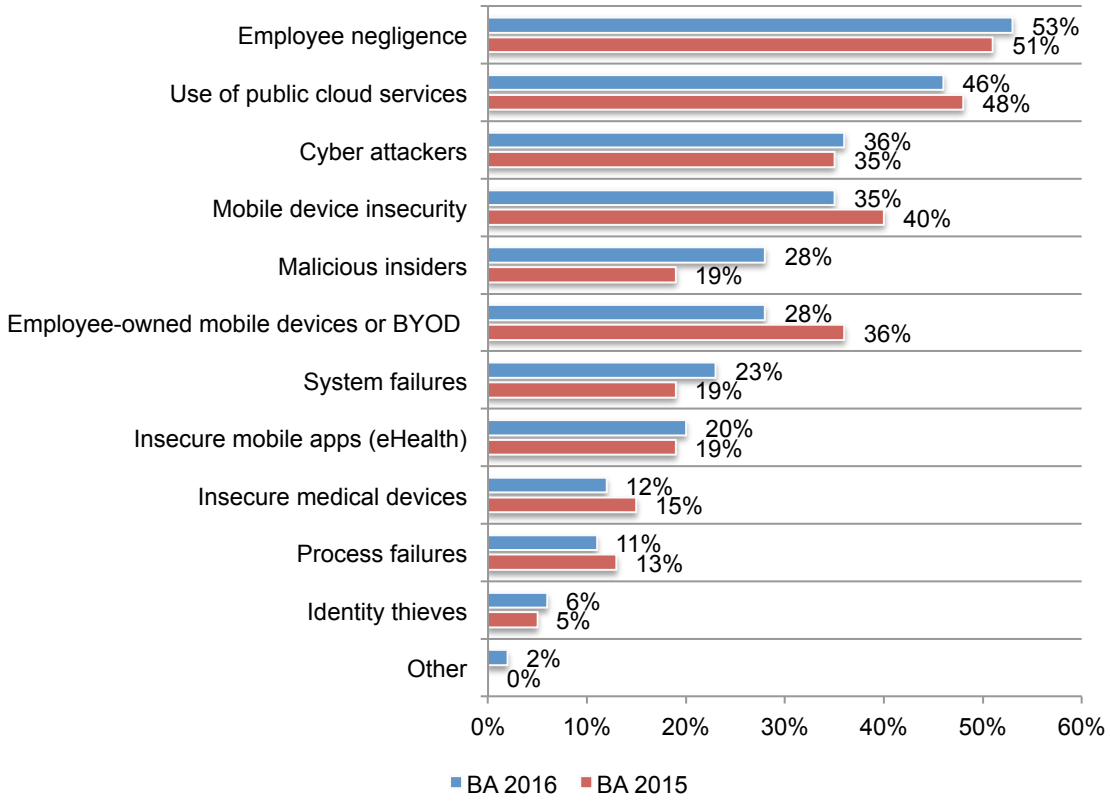
Employee negligence continues to be the greatest concern. According to Figure 5, when healthcare organizations were asked what type of security incident worries them most, by far it is the negligent or careless employee (69 percent of respondents). Forty-five percent of respondents say it is cyber attackers and 30 percent say it is the use of insecure mobile devices. These findings are virtually unchanged since 2015. Insecure medical devices and system failures are the least problematic (9 percent and 13 percent of respondents, respectively).

Figure 5. Security threats healthcare organizations worry about most
Three responses permitted



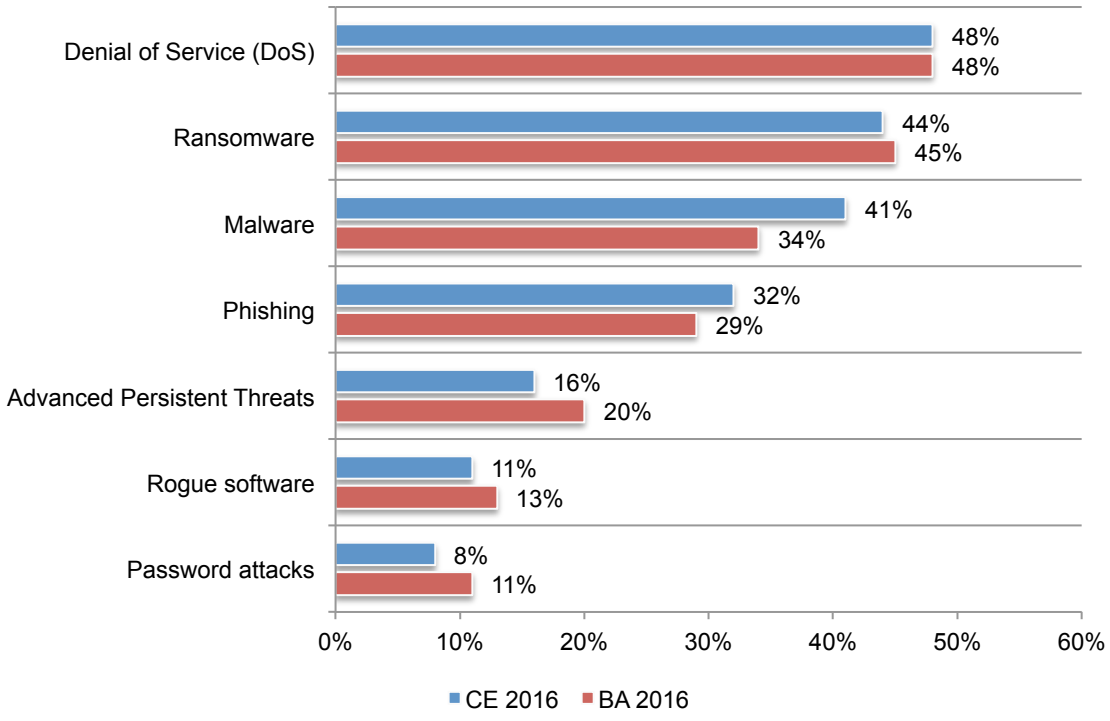
Employee negligence is a concern for business associates as well. When asked what type of security incident concerns them most, it is the negligent or careless employee (53 percent of respondents), as shown in Figure 6. This is followed by 46 percent of respondents who say it is use of cloud services and 36 percent who say it is cyber attackers. These findings are similar to last year's study. Process failures and identity thieves are the least problematic (11 percent and 6 percent of respondents, respectively).

Figure 6. What security threats worry business associates the most
Three responses permitted



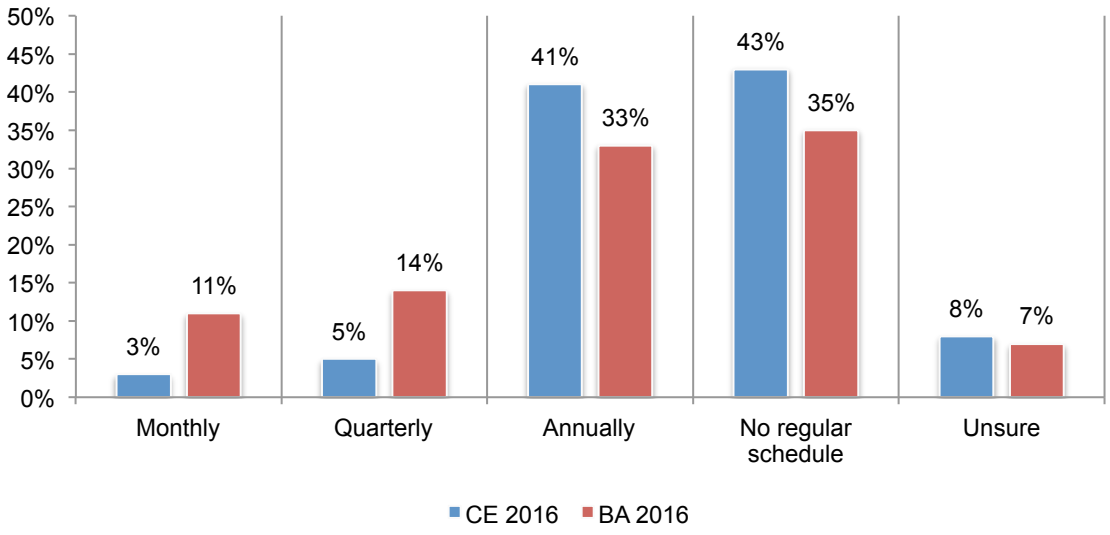
Healthcare and business associates are most concerned about denial of service (DoS) attacks. As shown in Figure 7, almost half of respondents (48 percent) worry about DoS attacks against their organizations. This is followed by ransomware and malware.

Figure 7. Cyber attacks organizations are most concerned about
Two responses permitted



The majority of organizations assess vulnerabilities to a data breach, but it is a rare event. Sixty percent of respondents in healthcare organizations and 54 percent of respondents in business associates say their organizations assess vulnerabilities to a data breach. However, it is most often done on an annual basis (41 percent and 33 percent, respectively) or ad hoc (no regular schedule) (43 and 35 percent, respectively), as shown in Figure 8.

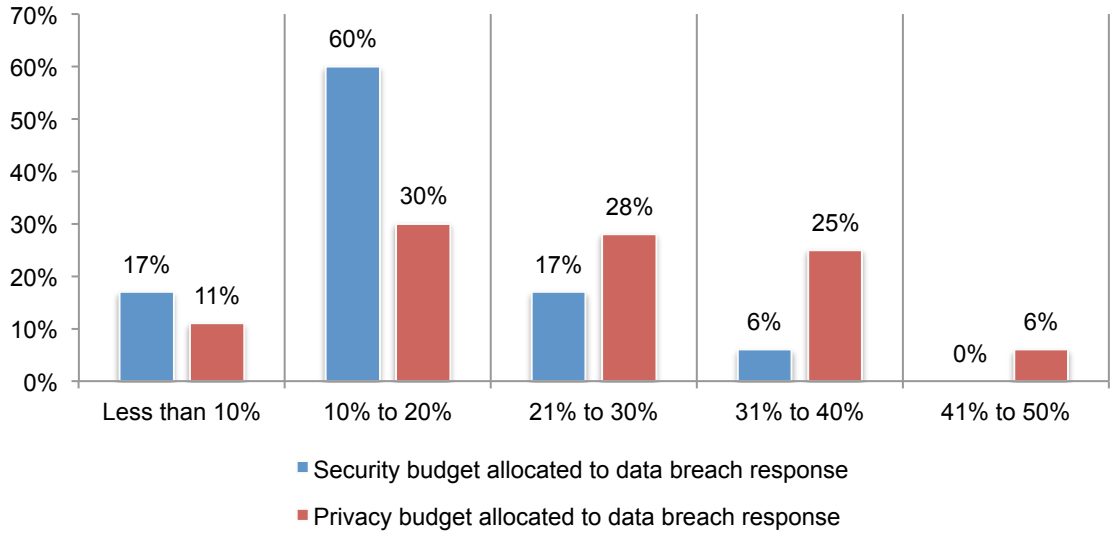
Figure 8. How often do you assess vulnerabilities to a data breach?



Healthcare organizations continue to put incident response processes in place. Healthcare organizations recognize the need to have a formal incident response process in place. Seventy-one percent of organizations have a process with involvement from information technology, information security and compliance, an increase from 69 percent of respondents in last year's study. The majority of respondents (51 percent) say their healthcare organizations have the in-house expertise to respond effectively to a data breach.

Of the healthcare organizations that have an incident response plan and the necessary expertise, the majority (56 percent) say more funding and resources are needed to make it effective. As shown in Figure 9, 77 percent of organizations (17 percent + 60 percent) allocate 20 percent or less of the security budget allocated to incident response Forty-one percent of organizations (11 percent + 30 percent) allocate less than 20 percent of the privacy budget to incident response.

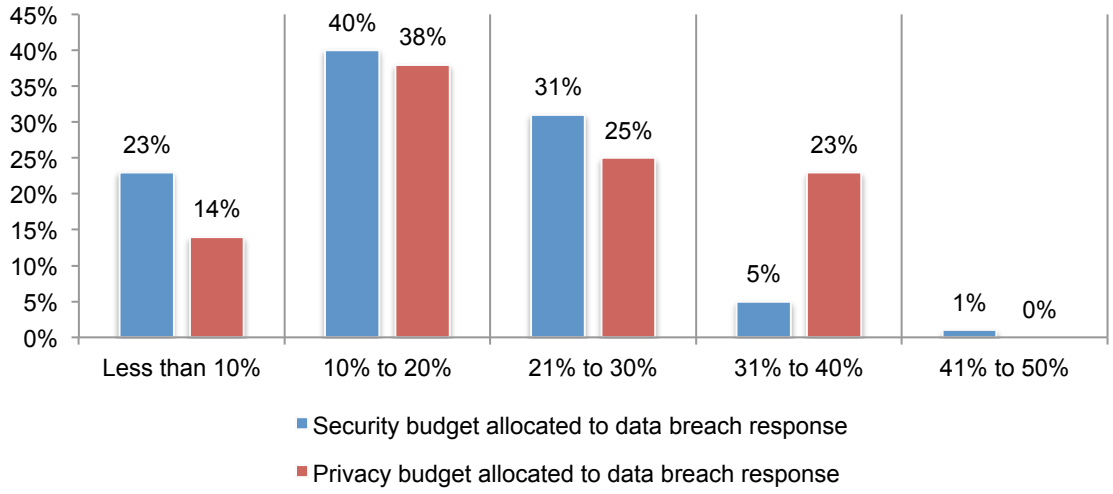
Figure 9. Percentage of security and privacy budget allocated to incident response for healthcare organizations



Business associates recognize the need to have a formal incident response process in place. Sixty-four percent of the respondents say their organizations have a process with involvement from information technology, information security and compliance. However, only 46 percent of respondents say they have the in-house expertise to respond effectively to a data breach.

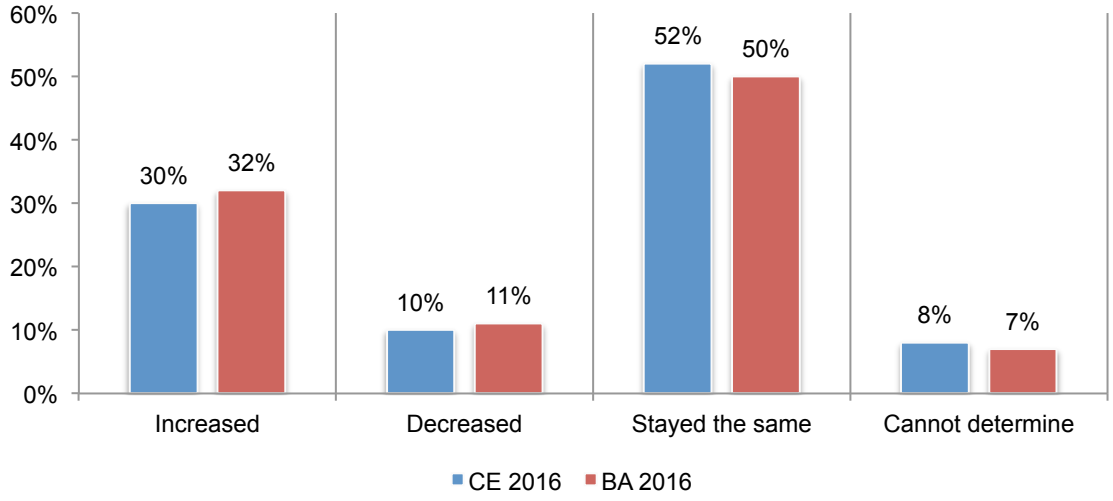
Of the healthcare organizations that have an incident response plan and the necessary expertise, there is not enough funding and resources needed to make incident response effective (59 percent). As shown in Figure 10, 63 percent of respondents say less than 20 percent of the security budget is allocated to data breach response and 52 percent of respondents allocate 20 percent or less of the privacy budget to incident response.

Figure 10. Percentage of security and privacy budget allocated to incident response for business associates



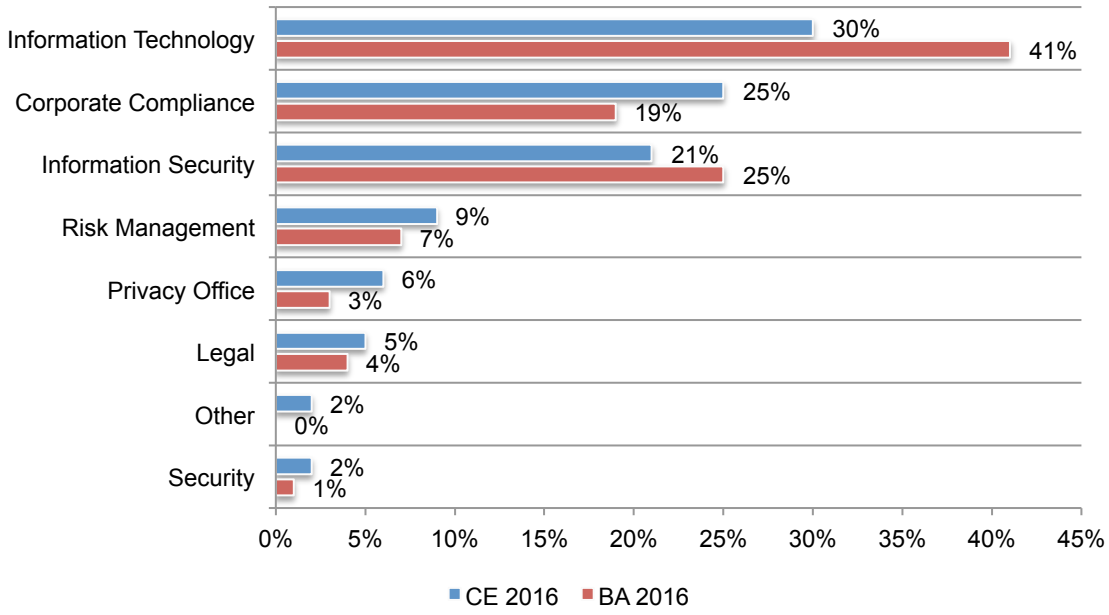
Despite concerns about the vulnerability of these organizations to a data breach, budgets do not budge. As shown in Figure 11, healthcare organizations report budgets have decreased (10 percent) or stayed the same (52 percent). Similarly, most business associates must deal with budgets that decrease (11 percent) or stay the same (50 percent).

Figure 11. How has this percentage changed over the past 24 months?



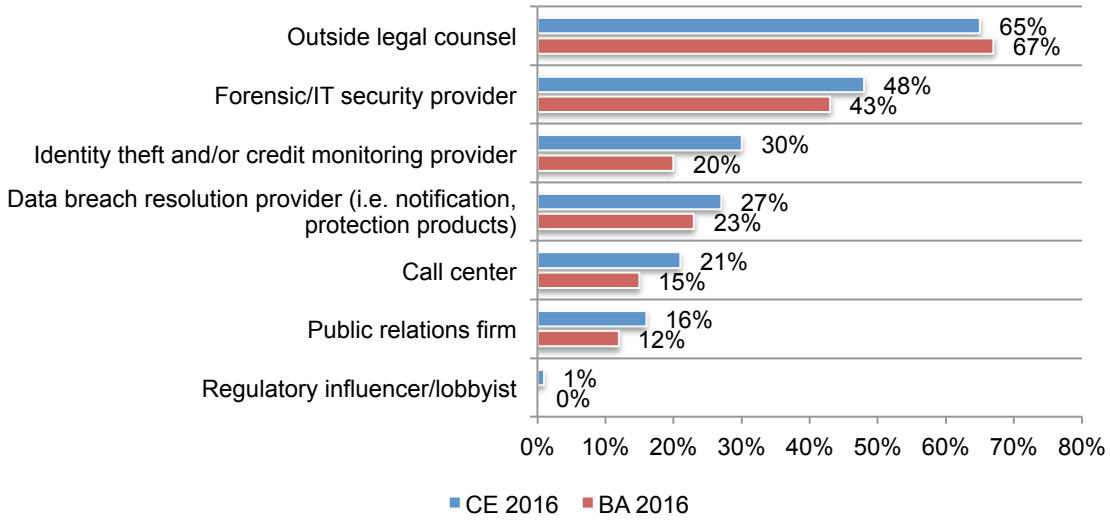
Information technology is ultimately accountable for data breach incident response. Accountability for the data breach incident response process is dispersed throughout the organization, as shown in Figure 12. However, both healthcare organizations (30 percent) and business associates (41 percent) say IT is the function most accountable for the data breach response process. Corporate compliance is more likely to be held accountable in healthcare organizations.

Figure 12. Which department is ultimately accountable for the data breach incident response?



Healthcare organizations are more likely than business associates to engage a third party. To help with incident response**,** 40 percent of respondents say their healthcare organizations hire a third party, and they are mainly outside legal counsel (65 percent of respondents) followed by a forensic/IT security provider (48 percent). Thirty-three percent of respondents in business associates say their organizations hire a third party. Similarly, business associates tend to hire legal counsel and forensic/IT security provider, as shown in Figure 13.

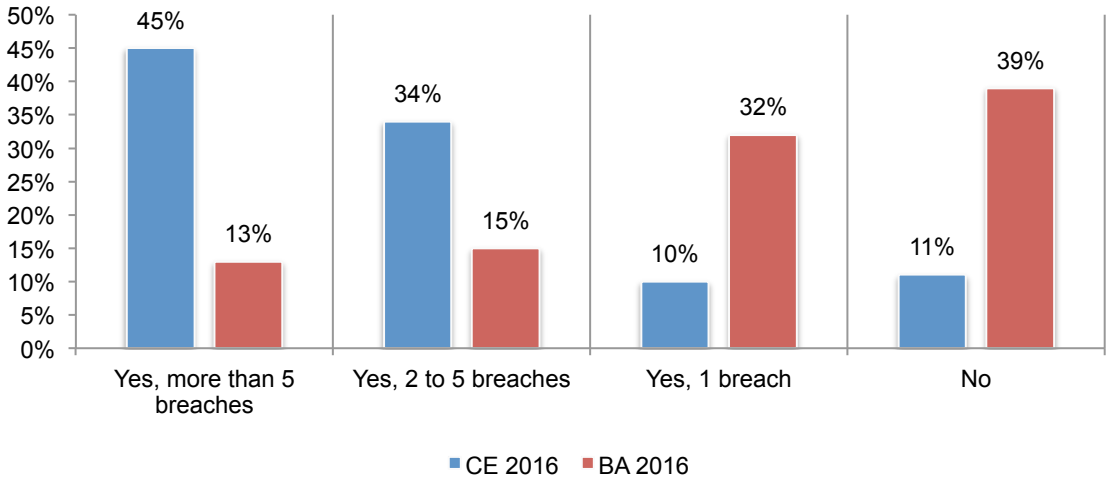
Figure 13. What type of third party providers do you hire?



Data breaches in healthcare organizations and business associates

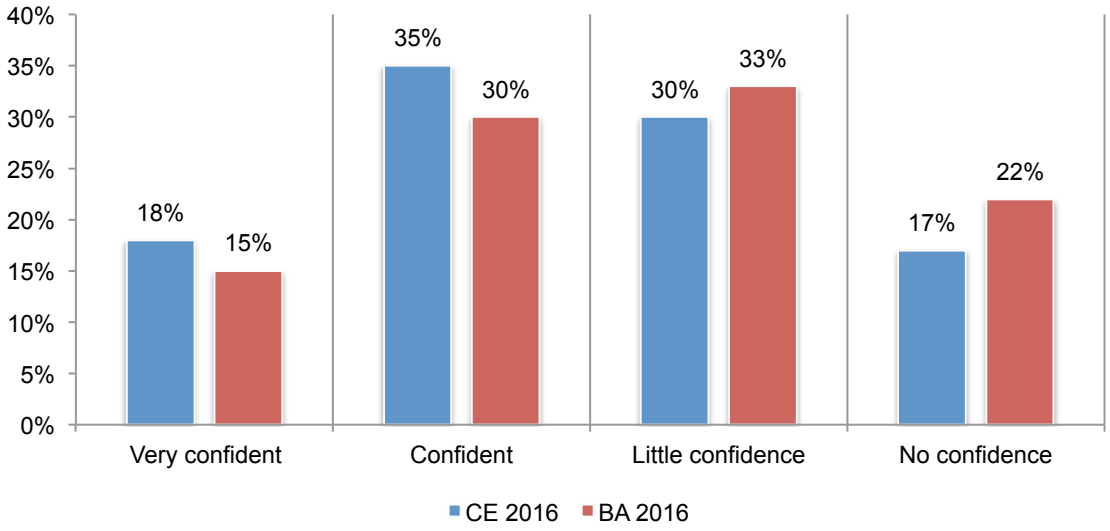
Data breaches affect all organizations. Eighty-nine percent of healthcare organizations had at least one data breach involving the loss or theft of patient data in the past 24 months. According to Figure 14, 45 percent had more than five breaches. Sixty-one percent of business associates had at least one data breach involving the loss or theft of patient data in the past 24 months. In fact, 28 percent say their organization had more than two breaches.

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



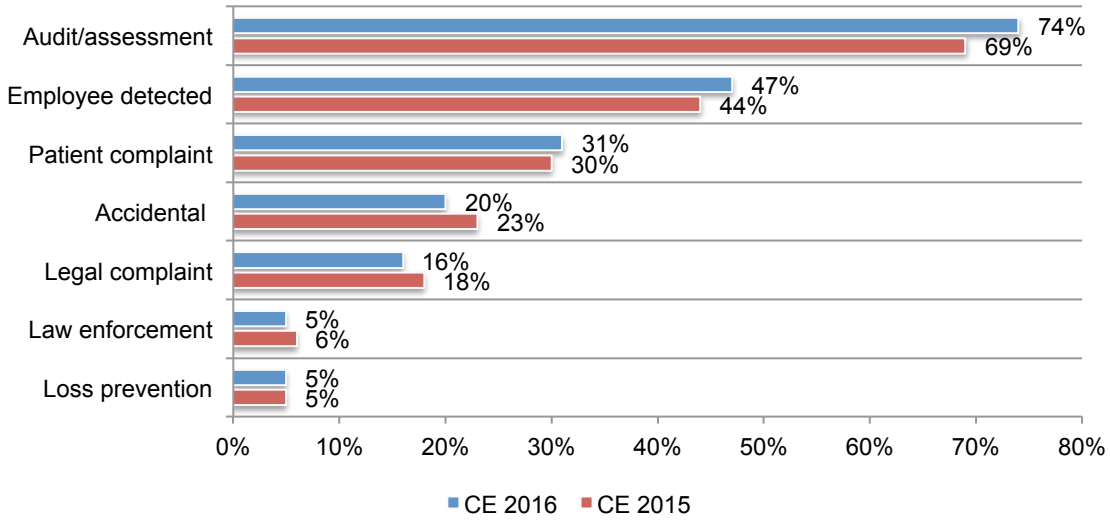
Healthcare organizations are more confident than business associates in their ability to detect all patient data loss or theft. As shown in Figure 15, healthcare organizations and business associates are both relatively confident they can determine if patient data was stolen or lost. Fifty-three percent of healthcare organizations (18 percent + 35 percent) and 45 percent of business associates (15 percent + 30 percent) are very confident or confident.

Figure 15. How confident are you that your organization has the ability to detect all patient data loss or theft?



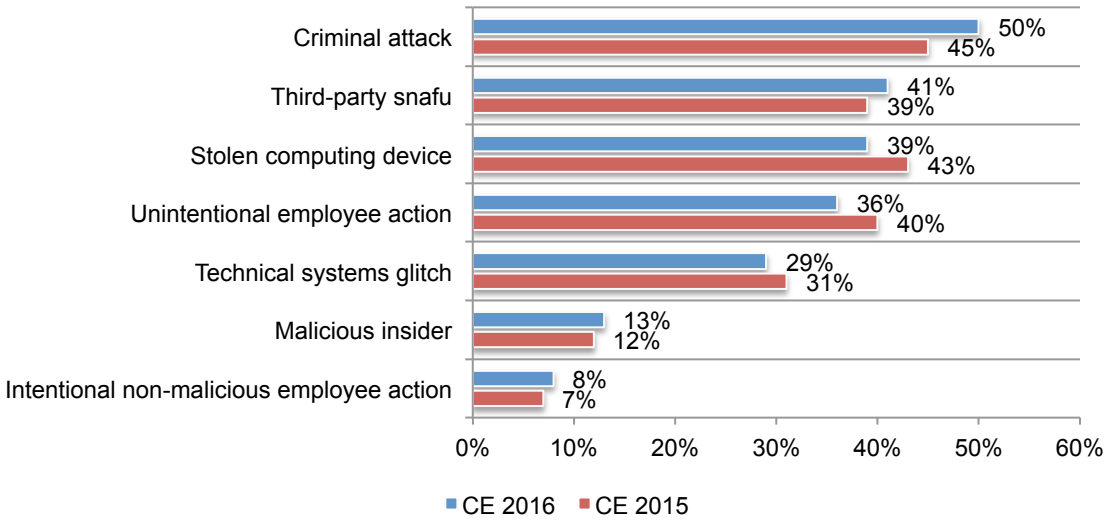
Organizations are fighting to stop data breaches from a variety of sources. In the past two years, healthcare organizations spent an average of more than $2.2 million to resolve the consequences of a data breach involving an average of 3,128 lost or stolen records. According to Figure 16, 74 percent of respondents say the data breach was discovered by an audit or assessment, an increase from 69 percent in last year's study. Forty-seven percent say an employee detected the data breach. Patient complaints revealed the data breach, according to 31 percent of respondents.

Figure 16. How the data breach was discovered (healthcare organizations)
More than one response permitted



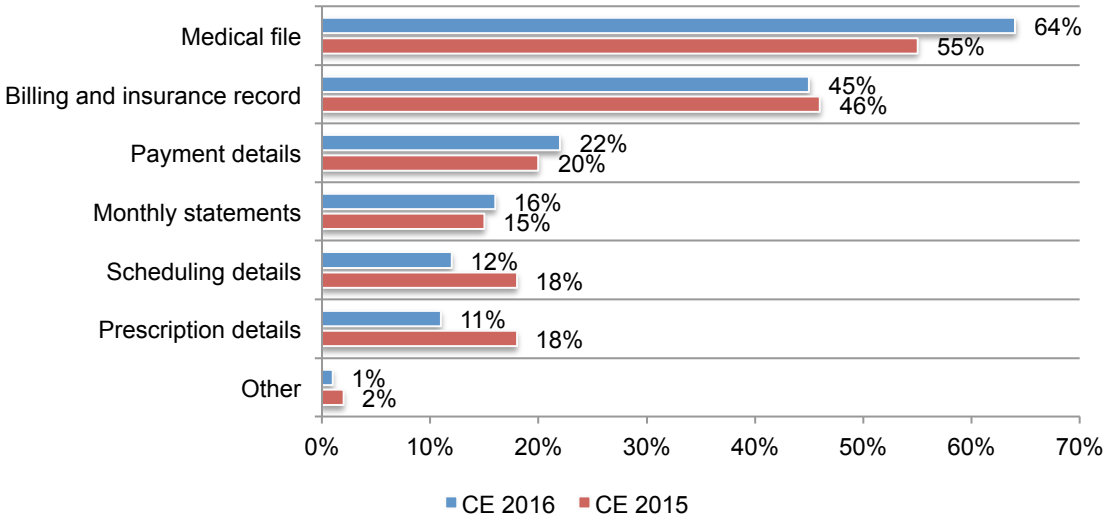
Criminal attacks are the main cause of data breaches. The challenge organizations face is dealing with data breaches with many possible root causes. Figure 17 reveals that 50 percent of healthcare organizations report the root cause of the breach was a criminal attack, 41 percent of respondents say it was caused by a third-party snafu and 39 percent of respondents say it was due to a stolen computing device. Only 13 percent say it was due to a malicious insider.

Figure 17. What was the root cause of the healthcare organizations' data breach?
More than one response permitted



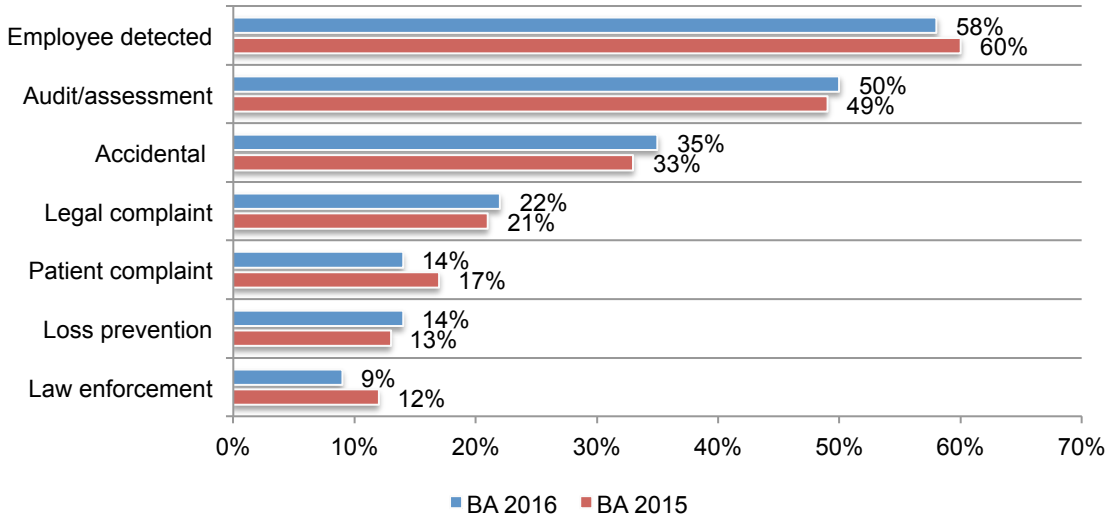
Successful attacks targeting medical files and billing and insurance records increased. These contain the most valuable patient data and most often successfully targeted (64 percent of respondents and 45 percent of respondents, respectively), as shown in Figure 18.

Figure 18. Patient data successfully targeted (healthcare organizations)
More than one response permitted



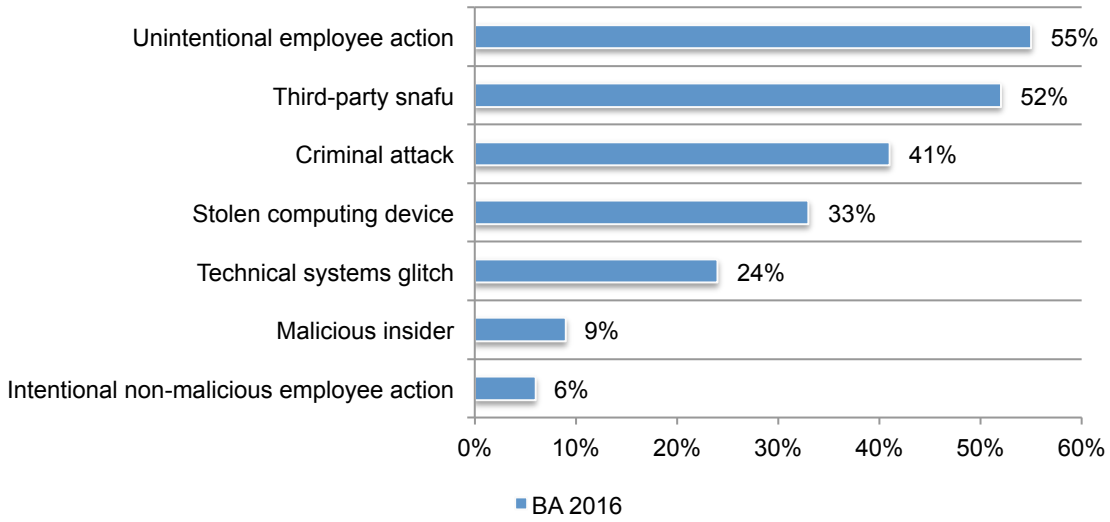
Business associates are fighting to stop data breaches from a variety of sources. In the past two years, business associates spent an average of slightly more than $1 million to resolve the consequences of a data breach involving an average of 5,887 lost or stolen records. According to Figure 19, 58 percent of respondents say an employee discovered the data breach and 50 percent say it was discovered through an audit or assessment. Thirty-five percent say the data breach was only discovered accidentally.

Figure 19. How the data breach was discovered (business associates)
More than one response permitted



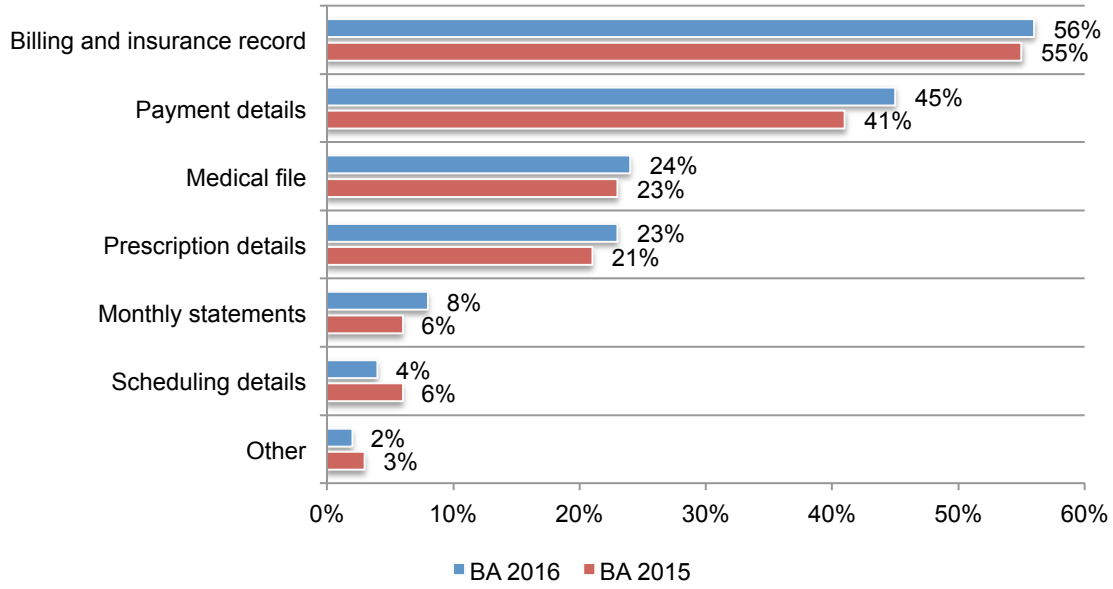
Business associates face the challenge of dealing with data breaches due to many different root causes. According to Figure 20, 55 percent of respondents say it was an unintentional employee action, 52 percent of respondents say it was caused by a third-party snafu and 41 percent of respondents say it was due to a criminal attack. Only six percent say it was due to an intentional non-malicious employee action.

Figure 20. What was the root cause of the business associates' data breach?
More than one response permitted



Billing and insurance records are at risk in business associates. In contrast to healthcare organizations, billing and insurance records are most often successfully targeted (56 percent of respondents) in business associates. Also frequently lost or stolen are payment details (45 percent of respondents), as shown in Figure 21.

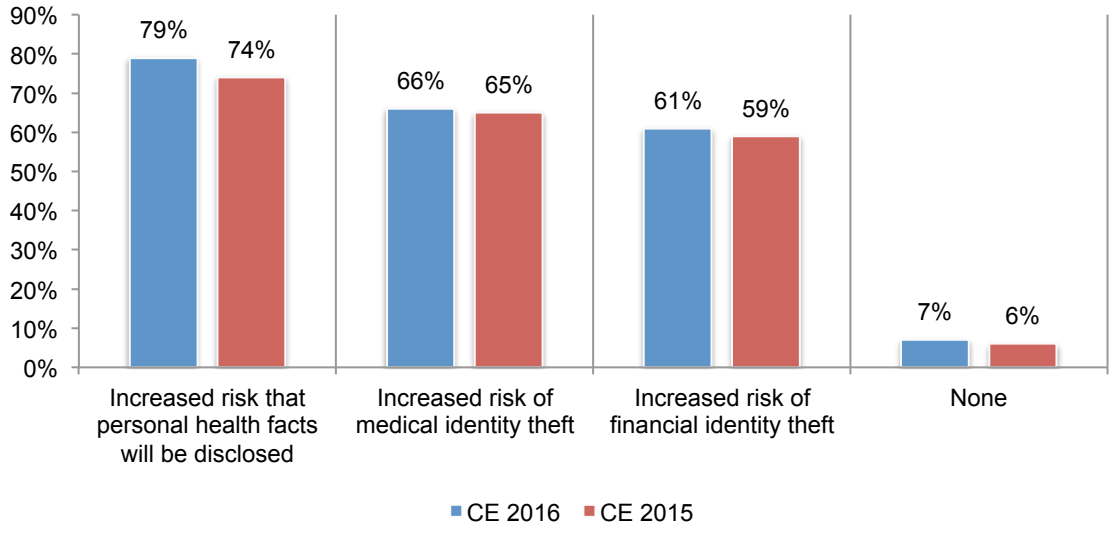
Figure 21. Patient data successfully targeted (business associates)
More than one response permitted



Healthcare 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, only 19 percent of respondents in healthcare say they have a process in place to correct errors in victim's medical records.

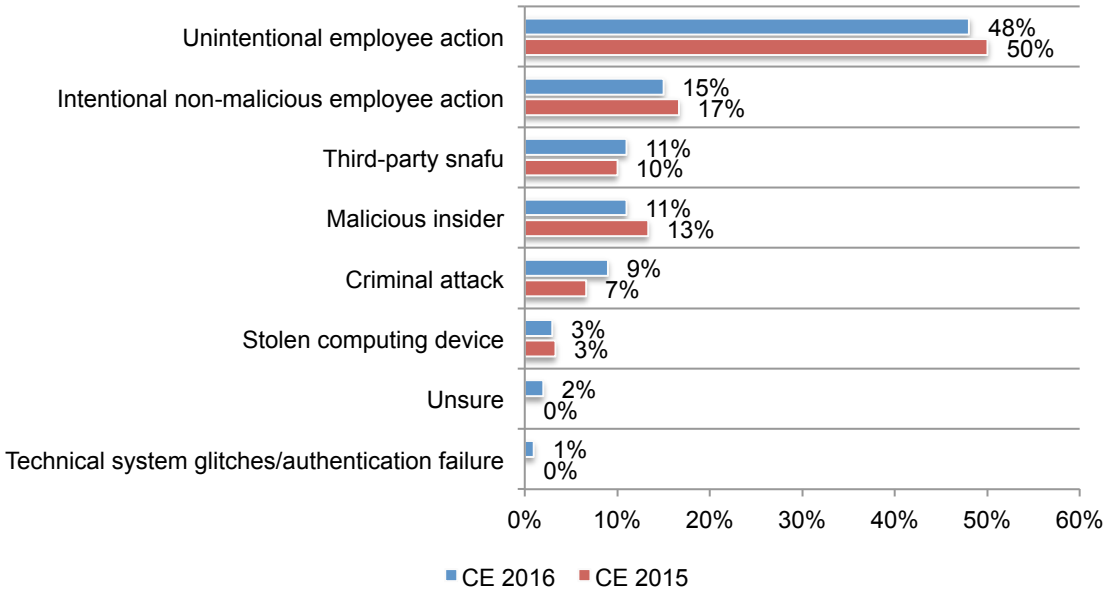
As shown in Figure 22, similar to last year's study, 79 percent of respondents say there is an increased risk that personal health facts will be disclosed and 61 percent believe patients who have had their records lost or stolen are more likely to become victims of financial identity theft. Sixty-six percent of respondents say the risk of medical identity theft increases.

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



According to healthcare organizations, most medical identity theft is preventable through employee training. Sixty-two percent of respondents say they are not aware or are unsure of any medical identity theft affecting their patients. As shown in Figure 23, of the 38 percent who say they know about medical identity theft, the root cause most often was unintentional employee action (48 percent of respondents) followed by intentional but non-malicious employee action (15 percent of respondents).

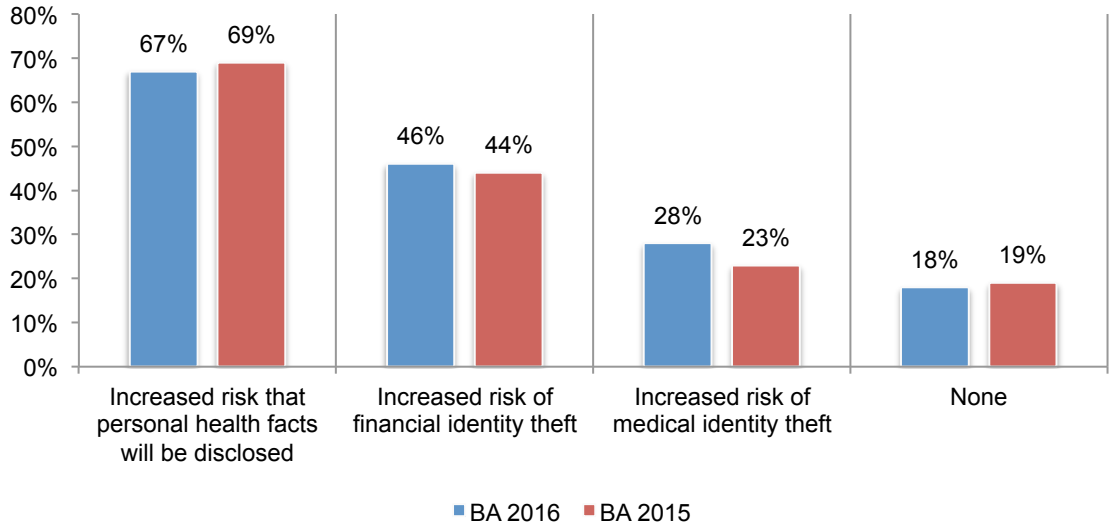
Figure 23. What was the root cause of the medical identity theft?



Business associates 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, only 11 percent of respondents in business associates say they have a process in place to correct errors in victim's medical records.

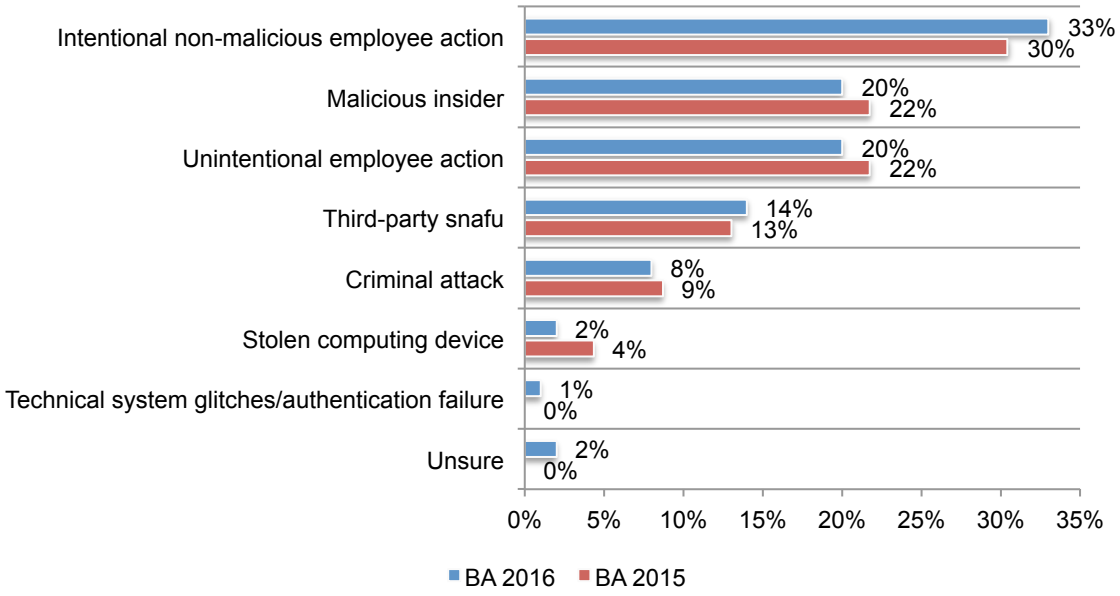
As shown in Figure 24, 67 percent of respondents say there is an increased risk that personal health facts will be disclosed and 46 percent of respondents say the risk of financial identity theft increases.

Figure 24. Harms patients actually suffer if their records are lost or stolen (business associates)
More than one response permitted



Insiders in business associates are the main root cause of medical identity theft. Seventy-four percent of BA respondents say they are not aware or are unsure of any medical identity theft affecting their patients. Of the 26 percent who say they know about medical identity theft, the root cause most often was the intentional but non-malicious employee action (33 percent of respondents). Unintentional employee action and malicious insiders were both considered the root cause in 20 percent of the cases, as shown in Figure 25.

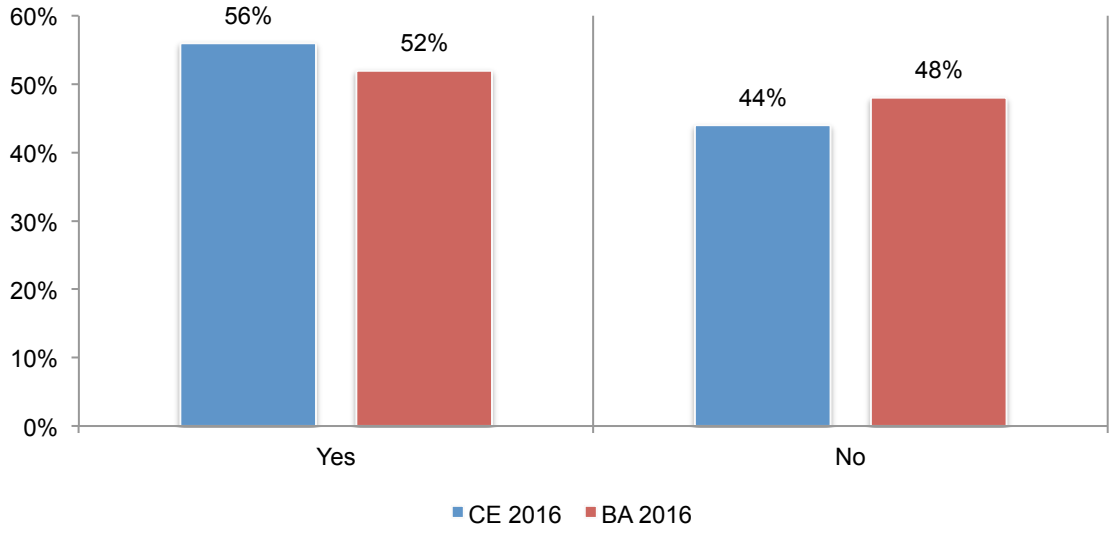
Figure 25. What was the root cause of the medical identity theft?



Following a data breach, should credit monitoring or medical identity theft protection be provided? As shown in Figure 26, 56 percent of respondents in healthcare organizations and 52 percent of respondents in business associates say victims of data breaches should be protected. Most respondents believe credit monitoring or medical identity theft protection should be offered for a minimum of two to three years.

Employees do not receive the same amount of protection. Only 17 percent of respondents in healthcare organizations and 15 percent of respondents in business associates say they provide employees with identity theft protection services. Only 24 percent of healthcare organizations and 22 percent of business associates plan to offer this protection in the future.

Figure 26. Do you believe credit monitoring or medical identity theft protection should be provided?

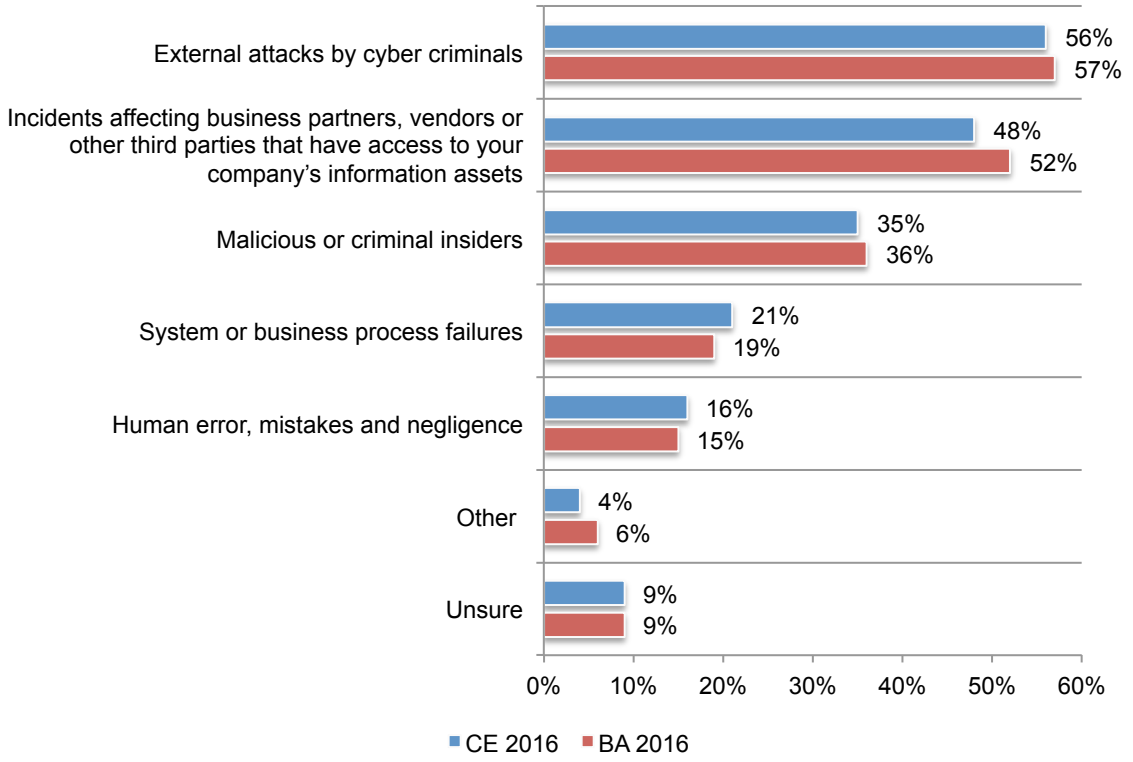


Data breach insurance for healthcare organizations and business associates

To minimize the financial consequences, some healthcare organizations have purchased data breach insurance policies. One-third of healthcare organizations have a data breach insurance policy and 29 percent of business associates have a cyber breach insurance policy.

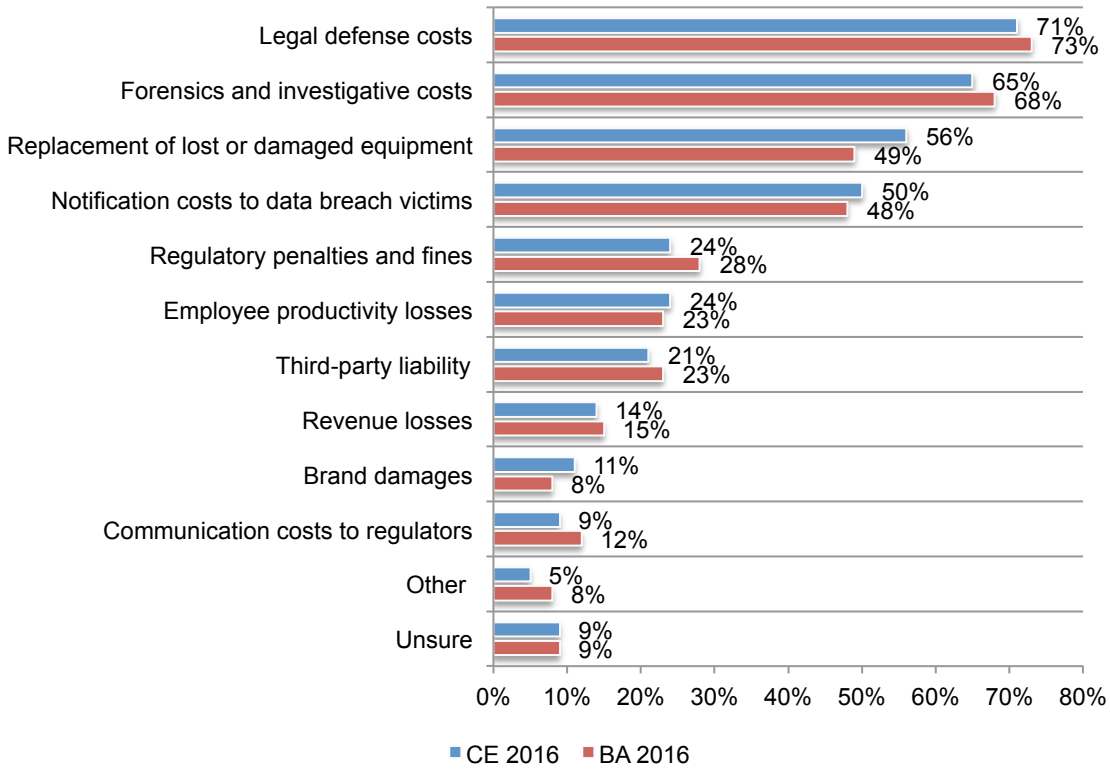
Fifty-seven percent of healthcare organizations and 52 percent of business associates say they purchase up to $5 million in coverage. According to Figure 27, insurance typically covers external attacks by cyber criminals (56 percent of healthcare respondents and 57 percent of business associates) and incidents affecting business partners, vendors or other third parties that have access to the organization's information assets (48 percent of respondents and 52 percent of business associates).

Figure 27. What types of incidents does your organization's data breach insurance cover?
More than one choice permitted



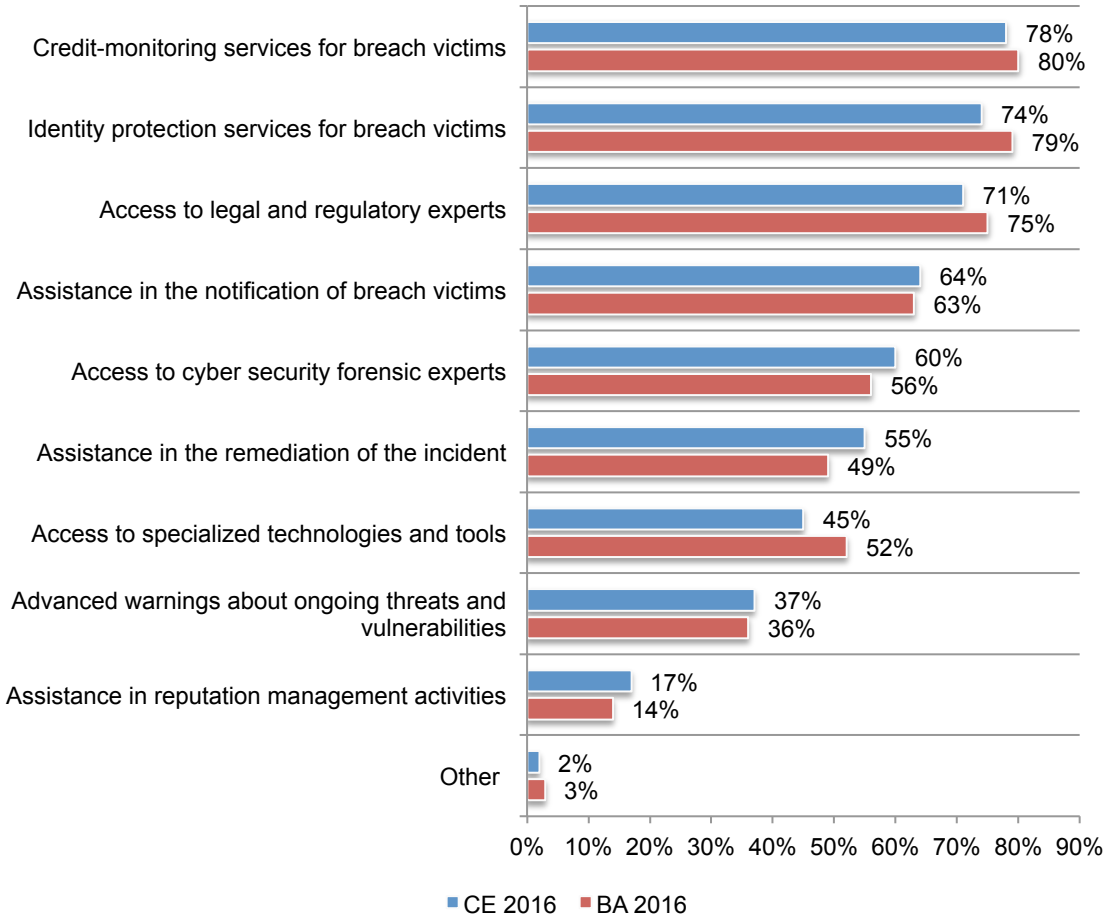
Legal defense and forensics and investigative costs are most often covered under these policies. According to Figure 28, 71 percent of healthcare respondents and 73 percent of business associates say their insurance will cover legal defense costs and 65 percent of healthcare respondents and 68 percent of business associates say forensics and investigative costs are covered. Brand damages and communication costs to regulators are rarely covered.

Figure 28. What coverage does data breach insurance provide?
More than one choice permitted



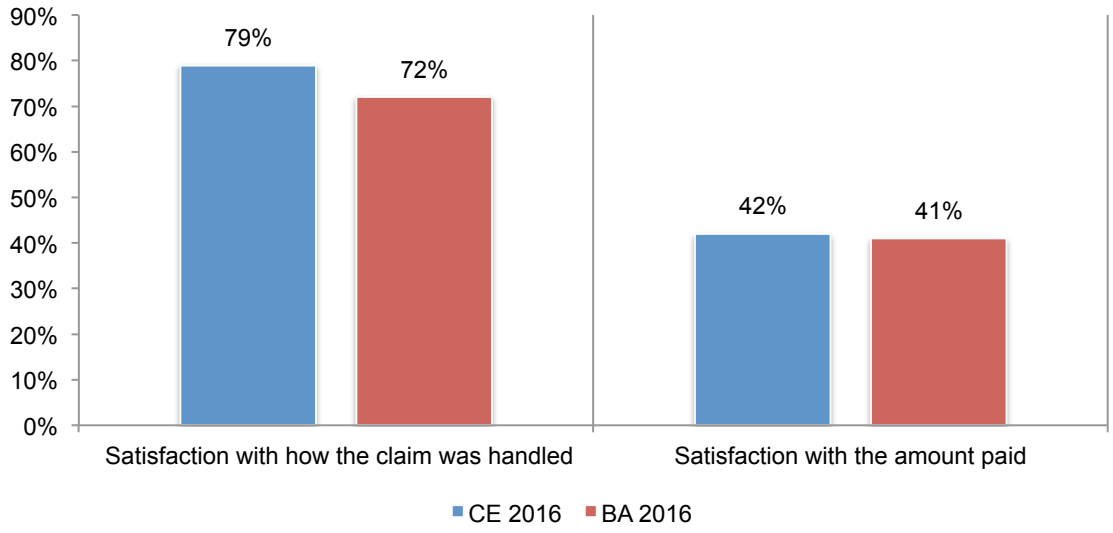
Cyber insurers most often provide credit monitoring and identity protection services. When asked what services the cyber insurer provides in addition to cost coverage, most respondents (78 percent of healthcare and 80 percent of business associates) say their organization provides credit-monitoring services and identity protection services for data breach victims (74 percent of healthcare respondents and 79 percent of business associates), as shown in Figure 29.

Figure 29. What services does the cyber insurer provide?
More than one choice permitted



Are healthcare organizations and business associates satisfied with their cyber insurer? Thirty-five percent of healthcare respondents and 31 percent of business associates say their organizations submitted a claim following a data breach or security incident. As shown in Figure 30, most respondents (79 percent of healthcare and 72 percent of business associates) were very satisfied with how the claim was handled. However, 42 percent of healthcare respondents and 41 percent of business associates say they were satisfied with the amount paid.

Figure 30. How satisfied was your organization with the claim process and amount paid?
7+ on a scale of 1 = not satisfied to 10 = highly satisfied



Part 3. Benchmark Methods

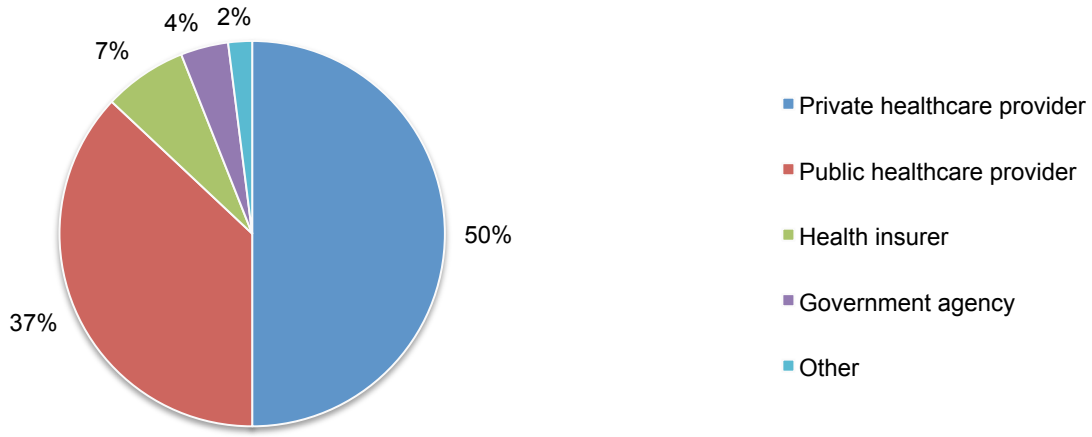
Table 1 summarizes the responses completed over a four-week period from March 2016 to April 2016. A total of 516 covered entities and 474 business associates were selected for participation and contacted by the researcher. One hundred and seventeen covered entities and 130 business associates agreed to complete the benchmark survey.

The final number of covered entities that actually participated was 91 and 84 business entities completed the benchmark instrument. A total of 392 interviews were conducted in participating covered entities, with an average of four interviews conducted in each organization. A total of 363 interviews were conducted in participating business associates, with an average of four interviews conducted in each organization.

Table 1. Benchmark sampling response	CE 2016	BA 2016
Organizations contacted	516	474
Organizations agreeing to participate	117	130
Organizations participating	91	84
Participation rate	18%	18%

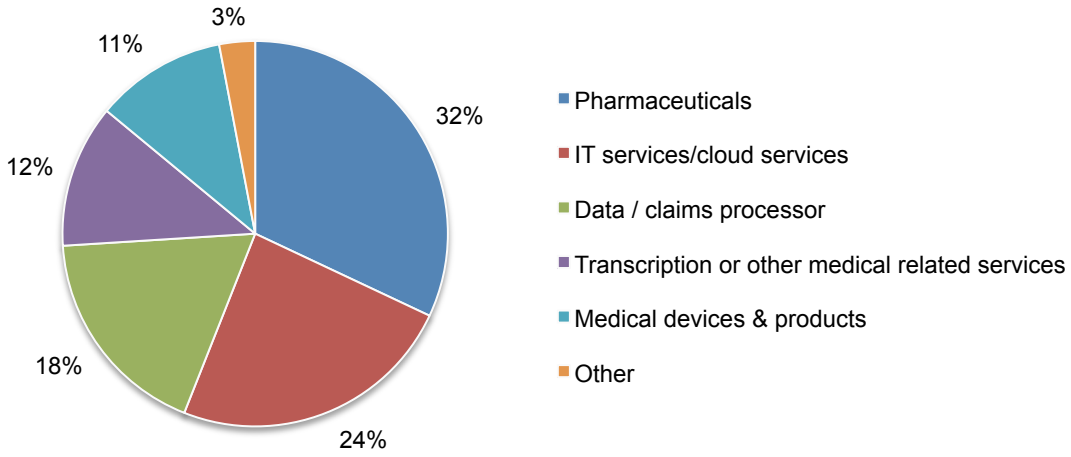
Pie Chart 1 reports the type of category that best describes the respondent's organization. Half of respondents (50 percent) reported they are a private healthcare provider followed by 37 percent that responded public healthcare provider.

Pie Chart 1. Type of covered entity



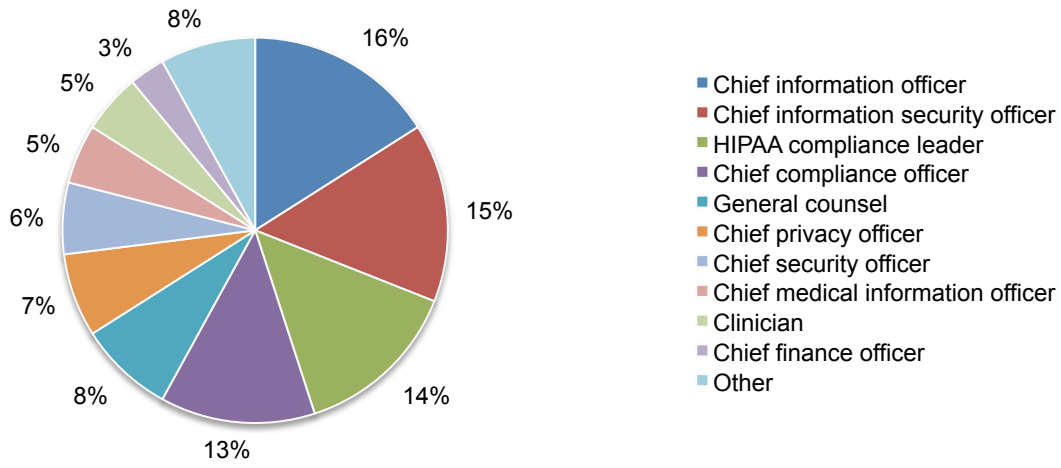
Pie Chart 2 reports the type of category that best describes the respondent's organization. Thirty-two percent of the business associates reported they are in pharmaceuticals. Another 24 percent identified as IT services/cloud services.

Pie Chart 2. Type of business associate



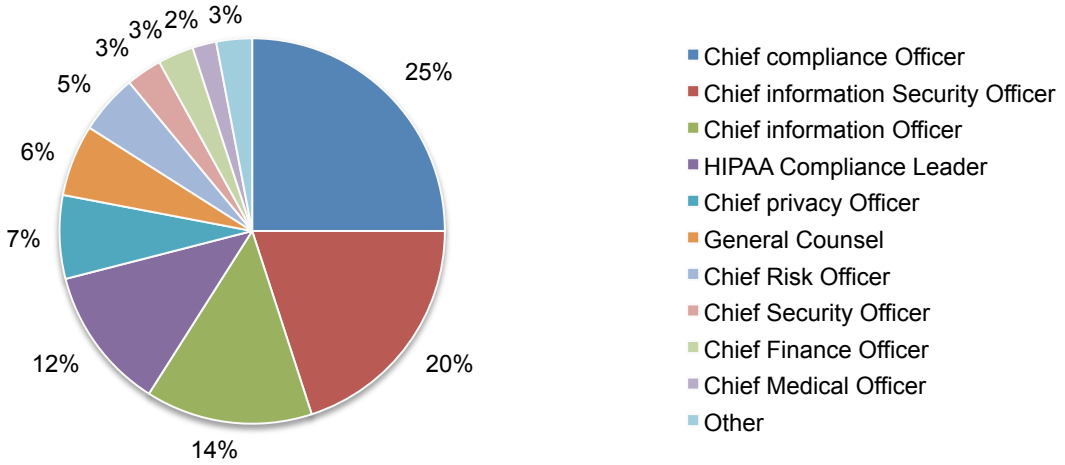
As shown in Pie Chart 3, the primary role of covered entity respondents is the chief information officer (16 percent) followed by the chief information security officer (15 percent) and HIPAA compliance leader (14 percent).

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



Pie Chart 4 reports the primary role of business associate respondents. Twenty-five percent responded chief compliance officer, and an additional 20 percent responded chief information security officer. Fourteen 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 33 and 34 identify the department or function for the covered entity and business associate. Healthcare organizations and business associates reported compliance (95 percent and 92 percent, respectively) as their primary department or function. Another 75 percent of healthcare organizations and 88 percent of BA respondents identified information technology as their primary function.

Figure 33. What best describes your department or function?

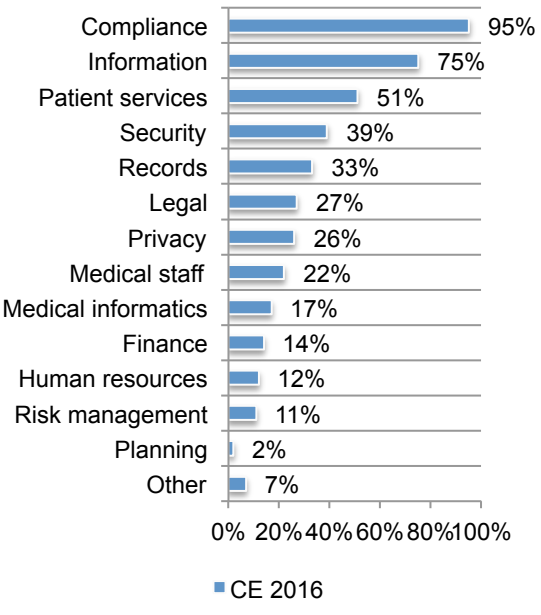
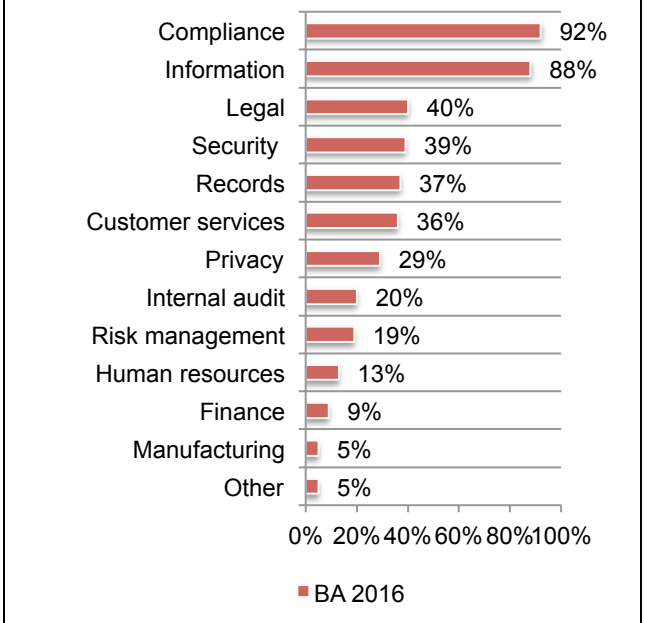


Figure 34. What best describes your department function?



Appendix: Detailed Results

The following tables provide the frequency of all benchmark survey questions completed by 91 covered entities and 84 business associates. All field research was completed over a four-week period from March 2016 to April 2016.

Benchmark study response	CE 2016	BA 2016	CE 2015	BA 2015
Organizations contacted	516	474	525	466
Organizations agreeing to participate	117	130	113	137
Organizations participating	91	84	90	88
Participation rate	18%	18%	17%	19%

Screening Question

S1. Is your organization a covered entity or business associate subject to HIPAA?	CE 2016	BA 2016	CE 2015	BA 2015
Covered entity	100%	0%	100%	0%
Business associate	0%	100%	0%	100%
No (Stop)	0%	0%	0%	0%
Total	100%	100%	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 2016	BA 2016	CE 2015	BA 2015
Public healthcare provider	37%		34%	
Private healthcare provider	50%		54%	
Government agency	4%		5%	
Health insurer	7%		5%	
Healthcare clearinghouse	0%		0%	
Other	2%		2%	
Total	100%		100%	

Q1b. Please indicate the region of the United States where you are located.	CE 2016	BA 2016	CE 2015	BA 2015
Northeast	22%		21%	
Mid-Atlantic	18%		19%	
Midwest	16%		16%	
Southeast	12%		12%	
Southwest	12%		13%	
Pacific-West	20%		19%	
Total	100%		100%	

Q1c. What best describes your role or the role of your supervisor?	CE 2016	BA 2016	CE 2015	BA 2015
Chief security officer	6%		5%	
Chief information security officer	15%		14%	
Chief information officer	16%		13%	
Chief privacy officer	7%		7%	
Chief compliance officer	13%		9%	
Chief medical officer	1%		2%	
Chief clinical officer	0%		1%	
Chief risk officer	1%		0%	
Chief medical information officer	5%		3%	
Chief finance officer	3%		4%	
Chief development officer	0%		0%	
General counsel	8%		7%	
HIPAA compliance leader	14%		12%	
Clinician	5%		4%	
Billing & administrative leader			8%	
Medical records management leader			8%	
Human resources leader			3%	
Other	6%			
Total	100%		100%	
Total number of individual interviews	392		395	
Average number of interviews per organization	4.31		4.39	
Q1d. What best describes your department or function?	CE 2016	BA 2016	CE 2015	BA 2015
Compliance	95%		98%	
Privacy	26%		29%	
Information technology (IT)	75%		74%	
Security	39%		44%	
Legal	27%		25%	
Finance	14%		16%	
Marketing	0%		0%	
Medical informatics	17%		19%	
Medical staff	22%		23%	
Patient services	51%		48%	
Records management	33%		29%	
Risk management	11%		12%	
Development - foundation	0%		0%	
Planning	2%		3%	
Human resources	12%		14%	
Other	7%		5%	
Total	431%		439%	

Q1e. What best describes your organization's privacy and security functions? Please select one.	CE 2016	BA 2016	CE 2015	BA 2015
Privacy and security functions are completely separate	27%		32%	
Privacy and security functions overlap in some places (hybrid)	44%		49%	
Privacy and security functions are combined	29%		19%	
Total	100%		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 2016	BA 2016	CE 2015	BA 2015
Data / claims processor		18%		19%
IT services/cloud services		24%		21%
Medical devices & products		11%		10%
Pharmaceuticals		32%		35%
Government agency		0%		0%
Transcription or other medical related services		12%		15%
Other		3%		0%
Total		100%		100%

Q2b. Please indicate the region of the United States where you are located.	CE 2016	BA 2016	CE 2015	BA 2015
Northeast		18%		19%
Mid-Atlantic		19%		20%
Midwest		17%		16%
Southeast		14%		13%
Southwest		13%		13%
Pacific-West		19%		19%
Total		100%		100%

Q2c. What is your organization's global headcount?	CE 2016	BA 2016	CE 2015	BA 2015
Less than 100		2%		0%
100 to 500		5%		4%
501 to 1,000		23%		24%
1,001 to 5,000		29%		32%
5,001 to 10,000		25%		23%
10,001 to 25,000		11%		12%
More than 25,000		5%		5%
Total		100%		100%
Q2d. What best describes your role or the role of your supervisor?	CE 2016	BA 2016	CE 2015	BA 2015
Chief Security Officer		3%		2%
Chief information Security Officer		20%		22%
Chief information Officer		14%		15%
Chief privacy Officer		7%		8%
Chief compliance Officer		25%		22%
Chief Medical Officer		2%		5%
Chief Risk Officer		5%		5%
Chief Operating Officer		1%		2%
Chief Finance Officer		3%		2%
General Counsel		6%		5%
HIPAA Compliance Leader		12%		12%
Other		2%		
Total		100%		100%
Total number of individual interviews		363		388
Average number of interviews per organization		4.32		4.41

Q2e. What best describes your department or function? One choice permitted in 2016 only	CE 2016	BA 2016	CE 2015	BA 2015
Compliance		92%		98%
Privacy		29%		35%
Information technology (IT)		88%		90%
Security		39%		40%
Legal		40%		35%
Finance		9%		8%
Sales / marketing		0%		0%
Logistics		0%		0%
Manufacturing		5%		6%
Customer services		36%		39%
Records management		37%		33%
Risk management		19%		20%
Human resources		13%		16%
Internal audit		20%		16%
Other		5%		5%
Total		432%		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 2016	BA 2016	CE 2015	BA 2015
Strongly agree	21%	23%	19%	18%
Agree	33%	28%	30%	28%
Unsure	24%	29%	28%	32%
Disagree	16%	12%	15%	13%
Strongly disagree	6%	8%	8%	9%
Total	100%	100%	100%	100%

Q4. My organization has sufficient resources to prevent or quickly detect unauthorized patient data access, loss or theft.	CE 2016	BA 2016	CE 2015	BA 2015
Strongly agree	18%	21%	15%	18%
Agree	19%	24%	18%	23%
Unsure	33%	32%	35%	35%
Disagree	25%	19%	26%	19%
Strongly disagree	5%	4%	6%	5%
Total	100%	100%	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 2016	BA 2016	CE 2015	BA 2015
Strongly agree	23%	23%	23%	21%
Agree	34%	28%	30%	29%
Unsure	21%	31%	23%	29%
Disagree	17%	15%	18%	17%
Strongly disagree	5%	3%	6%	4%
Total	100%	100%	100%	100%

Q6. Our organization's security budget is sufficient to curtail or minimize data breach incidents.	CE 2016	BA 2016	CE 2015	BA 2015
Strongly agree	19%	21%	16%	18%
Agree	22%	19%	21%	19%
Unsure	33%	32%	35%	36%
Disagree	18%	21%	19%	21%
Strongly disagree	8%	7%	9%	6%
Total	100%	100%	100%	100%

Q7. My organization has personnel who are knowledgeable about HITECH and states' data breach notification laws.	CE 2016	BA 2016	CE 2015	BA 2015
Strongly agree	26%	20%	24%	18%
Agree	30%	22%	25%	19%
Unsure	33%	26%	39%	28%
Disagree	11%	23%	12%	25%
Strongly disagree	0%	9%	0%	10%
Total	100%	100%	100%	100%

Q8. My organization has sufficient policies and procedures that effectively prevent or quickly detect unauthorized patient data access, loss or theft.	CE 2016	BA 2016	CE 2015	BA 2015
Strongly agree	26%	20%	26%	21%
Agree	37%	33%	32%	29%
Unsure	18%	23%	19%	24%
Disagree	17%	20%	19%	21%
Strongly disagree	2%	4%	4%	5%
Total	100%	100%	100%	100%

Q9. In 2016, what will be the threats to sensitive and confidential information your organization will be the most concerned about? Please select the top three.	CE 2016	BA 2016	CE 2015	BA 2015
Employee-owned mobile devices or BYOD	23%	28%	29%	36%
Mobile device insecurity	30%	35%	32%	40%
Use of public cloud services	29%	46%	33%	48%
Insecure medical devices	9%	12%	6%	15%
Employee negligence	69%	53%	70%	51%
Malicious insiders	24%	28%	26%	19%
Cyber attackers	45%	36%	40%	35%
Identity thieves	21%	6%	19%	5%
Insecure mobile apps (eHealth)	19%	20%	13%	19%
System failures	13%	23%	15%	19%
Process failures	15%	11%	15%	13%
Other	3%	2%	2%	0%
Total	300%	300%	300%	300%

Q10. Please select the two types of cyber attacks your organization is most concerned about?	CE 2016	BA 2016
Malware	41%	34%
Phishing	32%	29%
Password attacks	8%	11%
Ransomware	44%	45%
Denial of Service (DoS)	48%	48%
Rogue software	11%	13%
Advanced Persistent Threats	16%	20%
Other	0%	0%
Total	200%	200%

Q11a. Do you assess your organization's vulnerabilities to a data breach?	CE 2016	BA 2016
Yes	60%	54%
No	40%	46%
Total	100%	100%

Q11b. If yes, how often do you conduct an assessment?	CE 2016	BA 2016
Monthly	3%	11%
Quarterly	5%	14%
Annually	41%	33%
No regular schedule	43%	35%
Unsure	8%	7%
Total	100%	100%

Part 3: Data Breach

Data breach is defined as, generally, an impermissible use or disclosure under the Privacy Rule that compromises the security or privacy of the protected health information. An impermissible use or disclosure of protected health information is presumed to be a breach unless the covered entity or business associate, as applicable, demonstrates that there is a low probability that the protected health information has been compromised based on a risk assessment. State data breach laws vary and may be different than federal laws (Source: U.S. Department of Health & Human Services).

12. Has your organization suffered a data breach involving the loss or theft of patient data in the past 24 months as defined above?	CE 2016	BA 2016	CE 2015	BA 2015
No	11%	39%	9%	41%
Yes, 1 breach	10%	33%	12%	30%
Yes, 2 to 5 breaches	34%	15%	39%	14%
Yes, more than 5 breaches	45%	13%	40%	15%
Total	100%	100%	100%	100%

Q13. How confident are you that your organization has the ability to detect **all** patient data loss or theft?	CE 2016	BA 2016	CE 2015	BA 2015
Very confident	18%	15%	16%	13%
Confident	35%	30%	33%	29%
Little confidence	30%	33%	31%	34%
No confidence	17%	22%	20%	24%
Total	100%	100%	100%	100%

Q14a. Do you believe healthcare organizations are more vulnerable than other industries to data breaches?	CE 2016	BA 2016
Yes	69%	63%
No	23%	30%
Unsure	8%	7%
Total	100%	100%

Q14b. If yes, why? Please select the top two reasons	CE 2016	BA 2016
Healthcare organizations are not investing in technologies to mitigate a data breach	41%	50%
Healthcare organizations are not hiring enough skilled IT security practitioners	44%	42%
Healthcare employees are negligent in the handling of patient information	35%	54%
It is difficult to identify malicious insiders who work in healthcare organizations	12%	10%
Patient information is more valuable to identity thieves and cyber attackers than other types of information	14%	10%
Healthcare organizations are not vigilant in ensuring their partners and other third parties protect patient information	51%	32%
Other	3%	2%
Total	200%	200%

Q15a. Did any of the recent healthcare data breaches affect your security practices?	CE 2016	BA 2016
Yes	67%	62%
No	33%	38%
Total	100%	100%

Q15b. If yes, how? Please select the top two reasons.	CE 2016	BA 2016
Increased our investment in technologies to mitigate a data breach	58%	55%
Hired more skilled IT security practitioners	26%	29%
Increased employee training	52%	60%
Became more vigilant in ensuring our partners and other third parties have necessary precautions in place to safeguard patient information	61%	53%
Other	3%	3%
Total	200%	200%

Q16. Two separate data breach incidents over the past two years.	CE 2016	BA 2016	CE 2015	BA 2015
Number of incidents reported	368	295	361	304
Number of observed incidents used in the analysis	163	157	170	161

Q16a. Number of compromised records	CE 2016	BA 2016	CE 2015	BA 2015
< 10	6%	0%	3%	0%
10 to 100	49%	51%	50%	54%
101 to 1,000	22%	17%	24%	15%
1,001 to 5,000	16%	13%	15%	15%
5,001 to 10,000	4%	13%	6%	11%
10,001 to 100,000	2%	4%	1%	3%
> 100,000	1%	2%	1%	2%
Total	100%	100%	100%	100%
Extrapolated average number of lost or stolen records over two years	3,128	5,887	2,710	5,237

Q16b. Nature of the breach	CE 2016	BA 2016	CE 2015	BA 2015
Unintentional employee action	36%	55%	40%	51%
Intentional non-malicious employee action	8%	6%	7%	4%
Technical systems glitch	29%	24%	31%	27%
Criminal attack	50%	41%	45%	39%
Malicious insider	13%	9%	12%	10%
Third-party snafu	41%	52%	39%	49%
Stolen computing device	39%	33%	43%	35%
Total	216%	220%	217%	215%

Q16c. Type of device compromised or stolen (skip if none)	CE 2016	BA 2016	CE 2015	BA 2015
Desktop or laptop	23%	28%	26%	32%
Smartphone	35%	31%	29%	23%
Tablet	30%	27%	29%	29%
Notebook	1%	0%	0%	0%
Server	2%	2%	2%	3%
USB drive	9%	12%	14%	13%
Total	100%	100%	100%	100%

Q16d. Type of patient data lost, accessed without authorization or stolen	CE 2016	BA 2016	CE 2015	BA 2015
Medical file	64%	24%	55%	23%
Billing and insurance record	45%	56%	46%	55%
Scheduling details	12%	4%	18%	6%
Prescription details	11%	23%	18%	21%
Payment details	22%	45%	20%	41%
Monthly statements	16%	8%	15%	6%
Other	1%	2%	2%	3%
Total	171%	162%	174%	155%

Q16e. How the data breach was discovered	CE 2016	BA 2016	CE 2015	BA 2015
Accidental	20%	35%	23%	33%
Loss prevention	5%	14%	5%	13%
Patient complaint	31%	14%	30%	17%
Law enforcement	5%	9%	6%	12%
Legal complaint	16%	22%	18%	21%
Employee detected	47%	58%	44%	60%
Audit/assessment	74%	50%	69%	49%
Total	198%	202%	195%	205%

Q16f. Offer of protection services	CE 2016	BA 2016	CE 2015	BA 2015
None offered	64%	67%	65%	63%
Credit monitoring	19%	15%	19%	14%
Medical identity monitoring*	4%	0%		
Other identity monitoring			10%	9%
Insurance	1%	0%	0%	0%
Identity restoration	8%	7%	6%	7%
Financial incentives (i.e., gift cards)	2%	8%	0%	7%
Other	2%	3%	0%	0%
Total	100%	100%	100%	100%

Q17. In your opinion (best guess), what best describes the lifetime economic value, on average, of one patient or customer to your organization?	CE 2016	BA 2016	CE 2015	BA 2015
Less than $10,000	10%	70%	11%	69%
$10,001 to $50,000	31%	15%	33%	16%
$50,001 to $100,000	19%	3%	18%	3%
$100,001 to $200,000	17%	1%	19%	1%
$200,001 to $500,000	9%	1%	6%	0%
$500,001 to $1 million	1%	0%	2%	0%
More than $1 million	1%	0%	1%	0%
Cannot determine	12%	10%	10%	11%
Total	100%	100%	100%	100%
Average lifetime value of one patient or customer	$113,580	$20,056	$110,989	$16,584

Q18. In your opinion (best guess), what best describes the economic impact of data breach incidents experienced by your organization over the past two years?	CE 2016	BA 2016	CE 2015	BA 2015
Less than $10,000	4%	6%	4%	3%
$10,001 to $50,000	3%	6%	4%	5%
$50,001 to $100,000	5%	18%	6%	21%
$100,001 to $200,000	9%	23%	9%	27%
$200,001 to $500,000	21%	15%	21%	15%
$500,001 to $1 million	24%	13%	24%	12%
More than $1 million	28%	12%	27%	12%
Cannot determine	6%	7%	5%	5%
Total	100%	100%	100%	100%
Average economic impact of data breach over the past two years	$2,225,543	$1,054,129	$2,134,800	$1,032,126

Q19. In your opinion, what harms do patients actually suffer if their records are lost or stolen?	CE 2016	BA 2016	CE 2015	BA 2015
Increased risk of financial identity theft	61%	46%	59%	44%
Increased risk of medical identity theft	66%	28%	65%	23%
Increased risk that personal health facts will be disclosed	79%	67%	74%	69%
None	7%	18%	6%	19%
Total	213%	159%	204%	155%

Q20a. Are you aware of any cases of medical identity theft that affected your patients or customers during the past 24 months?	CE 2016	BA 2016	CE 2015	BA 2015
Yes	38%	26%	33%	25%
No	47%	58%	50%	60%
Unsure	15%	16%	17%	15%
Total	100%	100%	100%	100%

Q20b. If yes, what were the root causes of the medial identity theft?	CE 2016	BA 2016	CE 2015	BA 2015
Unintentional employee action	48%	20%	50%	22%
Intentional non-malicious employee action	15%	33%	17%	30%
Technical system glitches/authentication failure	1%	1%	0%	0%
Criminal attack	9%	8%	7%	9%
Malicious insider	11%	20%	13%	22%
Third-party snafu	11%	14%	10%	13%
Stolen computing device	3%	2%	3%	4%
Unsure	2%	2%	0%	0%
Total	100%	100%	100%	100%

Q20c. If yes, is there a process in place to correct errors in victim's medical records?	CE 2016	BA 2016
Yes	19%	11%
No	58%	67%
Unsure	23%	22%
Total	100%	100%

Part 4. Post breach response

Q21. Does your organization have an incident response process in place?	CE 2016	BA 2016	CE 2015	BA 2015
Yes	71%	64%	69%	65%
No (Go to Q25)	29%	36%	31%	35%
Total	100%	100%	100%	100%

Q22. Does your organization's incident response plan have the in-house expertise to respond effectively to a data breach?	CE 2016	BA 2016
Yes	51%	46%
No (Go to Q26)	49%	54%
Total	100%	100%

Q23. Do you believe your incident response process has adequate funding and resources?	CE 2016	BA 2016	CE 2015	BA 2015
Yes	44%	41%	44%	41%
No	56%	59%	56%	59%
Total	100%	100%	100%	100%

Q24. Who manages the data breach incident response process? Please check all that apply.	CE 2016	BA 2016	CE 2015	BA 2015
Legal	15%	33%	18%	38%
Corporate Compliance	80%	72%	79%	69%
Internal Audit	12%	30%	13%	28%
Privacy Office	55%	48%	58%	51%
Information Technology	91%	88%	88%	91%
Information Security	83%	85%	84%	95%
Human Resources	40%	26%	47%	24%
Security	23%	41%	26%	43%
Risk Management	27%	19%	30%	20%
Corporate Communications	24%	42%	27%	39%
Records Management	6%	0%	5%	0%
Other	2%	3%	0%	3%
Total	458%	487%	475%	498%

Q25. Which department/function is ultimately accountable for the data breach incident response process? Please check only one.	CE 2016	BA 2016
Legal	5%	4%
Corporate Compliance	25%	19%
Privacy Office	6%	3%
Information Technology	30%	41%
Information Security	21%	25%
Human Resources	0%	0%
Security	2%	1%
Risk Management	9%	7%
Other	2%	0%
Total	100%	100%

Q26a. Does your organization engage third parties to help it prepare and respond to a data breach or security incident?	CE 2016	BA 2016
Yes	40%	33%
No	55%	61%
Unsure	5%	6%
Total	100%	100%

Q26b. If yes, what type of providers do you hire? Please check all that apply.	CE 2016	BA 2016
Identity theft and/or credit monitoring provider	30%	20%
Call center	21%	15%
Data breach resolution provider (i.e. notification, protection products)	27%	23%
Outside legal counsel	65%	67%
Forensic/IT security provider	48%	43%
Public relations firm	16%	12%
Regulatory influencer/lobbyist	1%	0%
Total	208%	180%

Q26c. If yes, how do you select these vendors? Please select the one best reason	CE 2016	BA 2016
Expertise of vendor	64%	65%
Cost	26%	32%
Location of the vendor	15%	18%
Referral from cyber insurance provider or consultant	41%	38%
Recommendation from peer or other	24%	21%
Reputation of vendor	36%	33%
Total	206%	207%

Q27. What percentage of your organization's **security** budget is allocated to data breach response? Please include personnel, services and technology costs/investments in your estimate? Your best guess is welcome.	CE 2016	BA 2016	CE 2015	BA 2015
Less than 10%	17%	23%	28%	26%
10% to 20%	60%	40%	48%	52%
21% to 30%	17%	31%	19%	18%
31% to 40%	6%	5%	5%	4%
41% to 50%	0%	1%	0%	0%
More than 50%	0%	0%	0%	0%
Total	100%	100%	100%	100%
Extrapolated value	17%	18%	16%	16%

Q28. How has this percentage changed over the past 24 months?	CE 2016	BA 2016	CE 2015	BA 2015
Increased	30%	32%	33%	35%
Decreased	10%	11%	11%	9%
Stayed the same	52%	50%	50%	48%
Cannot determine	8%	7%	6%	8%
Total	100%	100%	100%	100%

Q29. What percentage of your organization's **privacy** budget is allocated to data breach response? Please include personnel, services and technology costs/investments in your estimate? Your best guess is welcome.	CE 2016	BA 2016	CE 2015	BA 2015
Less than 10%	11%	14%	12%	16%
10% to 20%	30%	38%	33%	36%
21% to 30%	28%	25%	25%	23%
31% to 40%	25%	23%	25%	25%
41% to 50%	6%	0%	5%	0%
More than 50%	0%	0%	0%	0%
Total	100%	100%	100%	100%
Extrapolated value	24%	21%	23%	21%

Q30. How has this percentage changed over the past 24 months?	CE 2016	BA 2016	CE 2015	BA 2015
Increased	39%	43%	44%	45%
Decreased	8%	12%	5%	9%
Stayed the same	46%	39%	45%	38%
Cannot determine	7%	6%	6%	8%
Total	100%	100%	100%	100%

Q31a. Following a data breach do you believe credit monitoring or medical identity theft protection should be provided?	CE 2016	BA 2016
Yes	56%	52%
No	44%	48%
Total	100%	100%

Q31b. If yes, how long should credit monitoring or medical identity theft protection be provided?	CE 2016	BA 2016
2 to 3 years	69%	76%
4 to 7 years	21%	19%
8 to 10 years	8%	5%
More than 10 years	2%	0%
Total	100%	100%

Q32a. Does your organization provide employees with identity theft protection?	CE 2016	BA 2016
Yes	17%	15%
No	83%	85%
Total	100%	100%

Q32b. If no, are you considering offering identity theft protection?	CE 2016	BA 2016
Yes	24%	22%
No	76%	78%
Total	100%	100%

Part 5. Data breach insurance

Q33. Does your organization have a data breach insurance policy?	CE 2016	BA 2016
Yes	33%	29%
No [Stop]	67%	71%
Total	100%	100%

Q34. What limits did you purchase?	CE 2016	BA 2016
Less than $1 million	23%	25%
$1 million to $5 million	34%	27%
$6 million to $20 million	27%	32%
$21 million to $100 million	15%	16%
More than $100 million	1%	0%
Total	100%	100%

Q35a. Have you ever submitted a claim following a data breach or security incident?	CE 2016	BA 2016
Yes	35%	31%
No	47%	49%
We did not have data breach or security incident that qualified for a claim	18%	20%
Total	100%	100%

Q35b. If yes, using the following 10-point scale, please rate your organization's satisfaction with how the claim was handled? 1 = not satisfied to 10 = highly satisfied	CE 2016	BA 2016
1 or 2	6%	9%
3 or 4	8%	11%
5 or 6	7%	8%
7 or 8	33%	29%
9 or 10	46%	43%
Total	100%	100%
Extrapolated value	7.60	7.22

Q35c. Using the following 10-point scale, please rate your organization's satisfaction with the amount paid. 1 = not satisfied to 10 = highly satisfied	CE 2016	BA 2016
1 or 2	11%	9%
3 or 4	21%	25%
5 or 6	26%	25%
7 or 8	23%	20%
9 or 10	19%	21%
Total	100%	100%
Extrapolated value	5.86	5.88

Q36. What types of incidents does your organization's data breach cover? Please select all that apply.	CE 2016	BA 2016
External attacks by cyber criminals	56%	57%
Malicious or criminal insiders	35%	36%
System or business process failures	21%	19%
Human error, mistakes and negligence	16%	15%
Incidents affecting business partners, vendors or other third parties that have access to your company's information assets	48%	52%
Other (please specify)	4%	6%
Unsure	9%	9%
Total	189%	194%

Q37. What coverage does this insurance offer your company? Please select all that apply.	CE 2016	BA 2016
Forensics and investigative costs	65%	68%
Notification costs to data breach victims	50%	48%
Communication costs to regulators	9%	12%
Employee productivity losses	24%	23%
Replacement of lost or damaged equipment	56%	49%
Revenue losses	14%	15%
Legal defense costs	71%	73%
Regulatory penalties and fines	24%	28%
Third-party liability	21%	23%
Brand damages	11%	8%
Other (please specify)	5%	8%
Unsure	9%	9%
Total	359%	364%

Q38. In addition to cost coverage, what other services does the cyber insurer provide your company in the event of a security exploit or data breach? Please check all that apply.	CE 2016	BA 2016
Access to cyber security forensic experts	60%	56%
Access to legal and regulatory experts	71%	75%
Access to specialized technologies and tools	45%	52%
Advanced warnings about ongoing threats and vulnerabilities	37%	36%
Assistance in the remediation of the incident	55%	49%
Assistance in the notification of breach victims	64%	63%
Identity protection services for breach victims	74%	79%
Credit monitoring services for breach victims	78%	80%
Assistance in reputation management activities	17%	14%
Other (please specify)	2%	3%
Total	503%	507%

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.