Fourth Annual Study: Is Your Company Ready for a Big Data Breach?

Sponsored by Experian® Data Breach Resolution

Independently conducted by Ponemon Institute LLC

Publication Date: September 2016

Fourth Annual Study: Is Your Company Ready for A Big Data Breach?

Ponemon Institute, September 2016

Part 1: Introduction

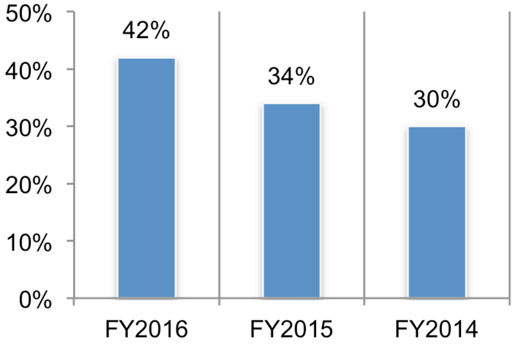
Ponemon Institute is pleased to present the *Fourth Annual Study: Is Your Company Ready for a Big Data Breach* sponsored by Experian® Data Breach Resolution. Since 2013, we have been tracking and identifying important trends in how organizations are planning for and responding to data breaches. Each year the number of companies experiencing a data breach increases. In this year's study, 52 percent of companies represented in this study had a breach, an increase from 49 percent last year, and 66 percent of respondents say their organization had multiple breaches.

Despite the growing likelihood a company will have a security incident, the findings reveal company leaders are not actively engaged and avoid responsibility for the effectiveness of their data breach preparedness plan. This lack of senior level involvement affects data breach preparedness.

Of the 86 percent of respondents who say their company has a data breach plan, 42 percent say it is very effective or effective, as shown in Figure 1. While this is a significant increase since 2014, it is not enough. Given the financial and reputational consequences of a data breach it is in the interest of companies to improve their plans.

Figure 1. How effective is your company's data breach response plan?

Very effective and Effective responses combined



In this year's study, we surveyed 619 executives and staff employees who work primarily in privacy, compliance and IT security in the United States. Some of the key findings we uncovered from this year's survey include.

Companies are not confident dealing with the most serious consequences of a data breach. Confidence in the ability to respond to the theft of sensitive and confidential information that requires notification to victims and regulators increased from 51 percent in 2014 to 59 percent this year. However, most companies in this study are not confident in the following areas:

- Only 41 percent of respondents say their company is able to respond to a data breach involving business confidential information and intellectual property.
- Only 27 percent of respondents say they are confident in their ability to minimize the financial and reputational consequences of a material data breach.

To be effective, data breach response plans need senior level involvement. Most boards of directors, chairmen and CEOs are not actively engaged, and avoid responsibility, in data breach preparedness. Since 2014, participants in this annual research have increasingly asked for more participation and oversight from senior executives, but it does not seem to be happening.

- Fifty-seven percent of respondents say their company's board of directors, chairman and CEO are not informed and involved in plans to deal with a possible data breach.

- Only 40 percent of respondents say they want to know ASAP if a material data breach occurs.

- About one-third (34 percent of respondents) say the board does understand the specific security threats facing their organization.

- Only 26 percent of respondents believe the board is willing to assume responsibility for the successful execution of the incident response plan.

Updating a data breach response plan is a crucial but often missed step. Most companies have a data breach response plan but it is not regularly reviewed. While 86 percent of respondents say their organizations have a data breach notification plan in place, only 24 percent of respondents say they have a procedure for updating their plan on a yearly basis. A deterrent to an effective data breach response plan is keeping it current with changes in the risks and threats facing a company.

Ransomware is becoming a growing nightmare for IT security, but companies are not taking steps to prepare for these attacks.

- Forty-five percent of respondents say they are not taking any of the steps listed to prepare for a possible ransomware attack.

- Only 17 percent of respondents say their companies educate employees about the risk, making companies vulnerable to ransomware.

Companies are not confident in their ability to deal with an international data breach. More than half of respondents (51 percent) have an incident response plan that includes processes to manage an international data breach. Only 31 percent of respondents are very confident (13 percent) or confident (18 percent) they would be able to respond effectively to an international data breach.

Stakeholder communication is key to an effective response plan. Most companies have procedures for communicating with investors, business partners and other third parties are in most plans in order to maintain trust with these stakeholders. Procedures for communicating with state attorneys general and regulators increased significantly from 53 percent of respondents in 2015 to 66 percent of respondents in 2016. However, only 12 percent of respondents say their organizations meet with these influencers in advance of an incident.

More companies are requiring audits of third parties security procedures. Companies should minimize the consequences of a third party data breach by asking for audits of their security procedures.

- Since 2015, more companies are requiring audits of third party's security procedures (an increase from 39 percent to 50 percent).

- Almost all (93 percent of respondents), say they require third parties and business partners to notify them when they have a data breach.

- Eighty percent of respondents say they require an incident response plan their organization can review.

Lack of visibility is the biggest barrier to improving IT security's ability to respond to a data breach. More companies are recognizing the importance of both visibility into end-user access of sensitive and confidential information and lack of security processes for third parties that have access to data.

As part of data breach preparedness, employee privacy and data protection awareness programs are critical to reducing the risk of employee negligence. While more companies are offering these programs, they are often only offered during employee orientation**.** In 2013, 44 percent of respondents said their organizations had such awareness programs for employees and other stakeholders who have access to sensitive or confidential personal information. In 2016, this increased to 61 percent of respondents.

Sharing intelligence about data breach experiences and incident response plans can improve the ability to respond to a data breach. Forty-one percent of respondents say their organization participates in an initiative or program for sharing information with government and industry peers about data breaches and incident response**.** The most important reasons for sharing are the benefits from fostering collaboration among peers and industry groups (76 percent of respondents) and improving the security posture of the organization (56 percent of respondents).

Data breach or cyber insurance policies are gaining traction. In 2013, only 10 percent said their organizations purchased such policies and this year 38 percent of respondents say their organizations are making such a purchase. Following are features of policies, according to those respondents who say their organizations purchase cyber insurance.

- Most respondents (71 percent) say their cyber insurance policies reimburse legal defense and 65 percent of respondents say forensics and investigative costs are covered.

- Sixty-three percent of respondents say they cover notification costs to data breach victims.

Part 3. Key findings

In this section, we provide an analysis of the key findings. The complete audited findings are presented in the Appendix of this report. When available, we compare the findings from previous studies to this year's findings. We have organized the report according to the following topics:

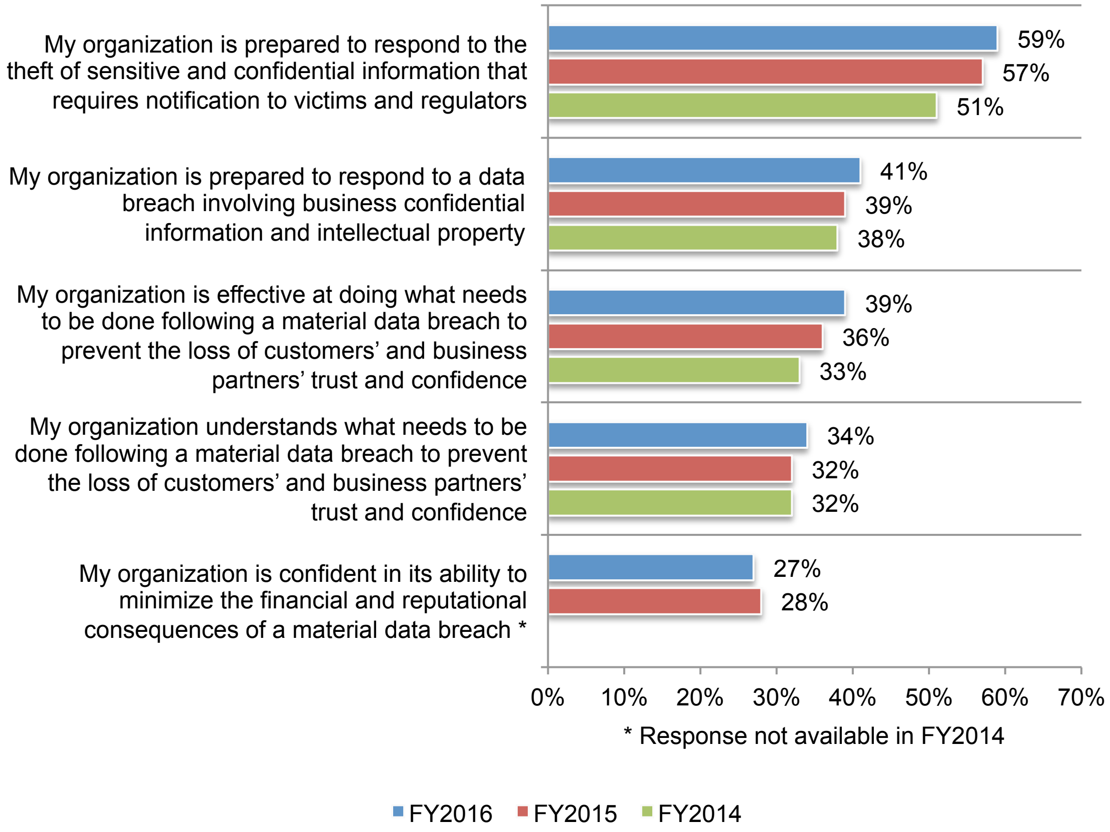
- The confidence gap in data breach preparedness
- The struggle to create a better data breach preparedness plan
- The role of IT security in data breach preparedness
- Cyber insurance as part of a data breach preparedness plan
- The role of identity theft products in data breach preparedness

The confidence gap in data breach preparedness

Companies are not confident dealing with the most serious consequences of a data breach. Confidence in the ability to respond to the theft of sensitive and confidential information that requires notification to victims and regulators increased from 51 percent in 2014 to 59 percent this year, as shown in Figure 2.

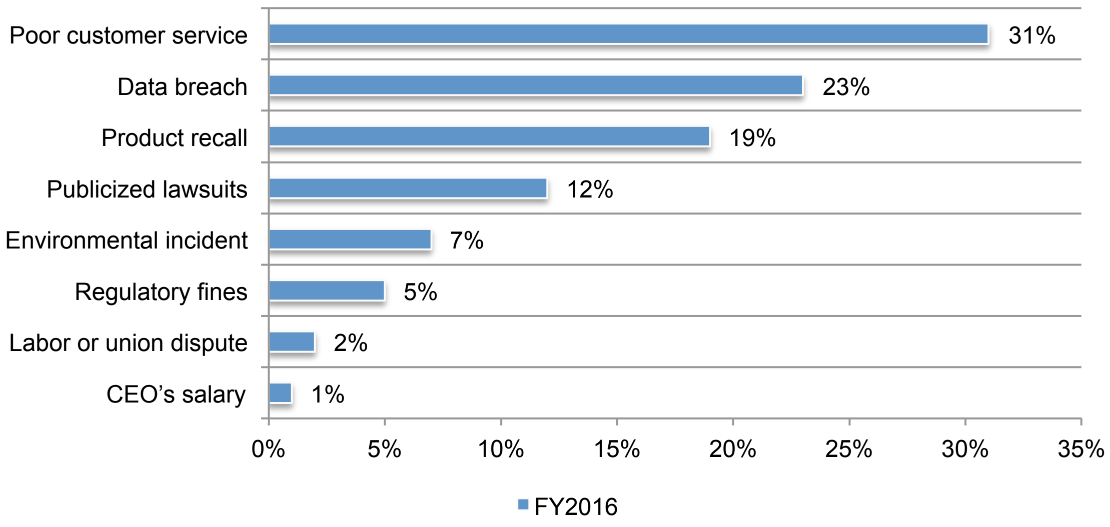
However, most companies are not confident in their ability to prevent the loss of customers' and business partners' trust and confidence, respond to a data breach involving business confidential information and intellectual property, prevent negative public opinion, blog posts and media reports and minimize the financial and reputational consequences of a material data breach.

Figure 2. The confidence gap in responding to a data breach
Strongly agree and agree response combined



Data breaches are more concerning than product recalls and lawsuits. A majority of respondents acknowledge the potential damage data breaches can cause to corporate reputation is significant. As shown in Figure 3, they ranked a data breach second only to poor customer service and ahead of product recalls, environmental incidents and publicized lawsuits. The combination of the higher likelihood and significant impact has caused data breaches to be a major issue across all sectors.

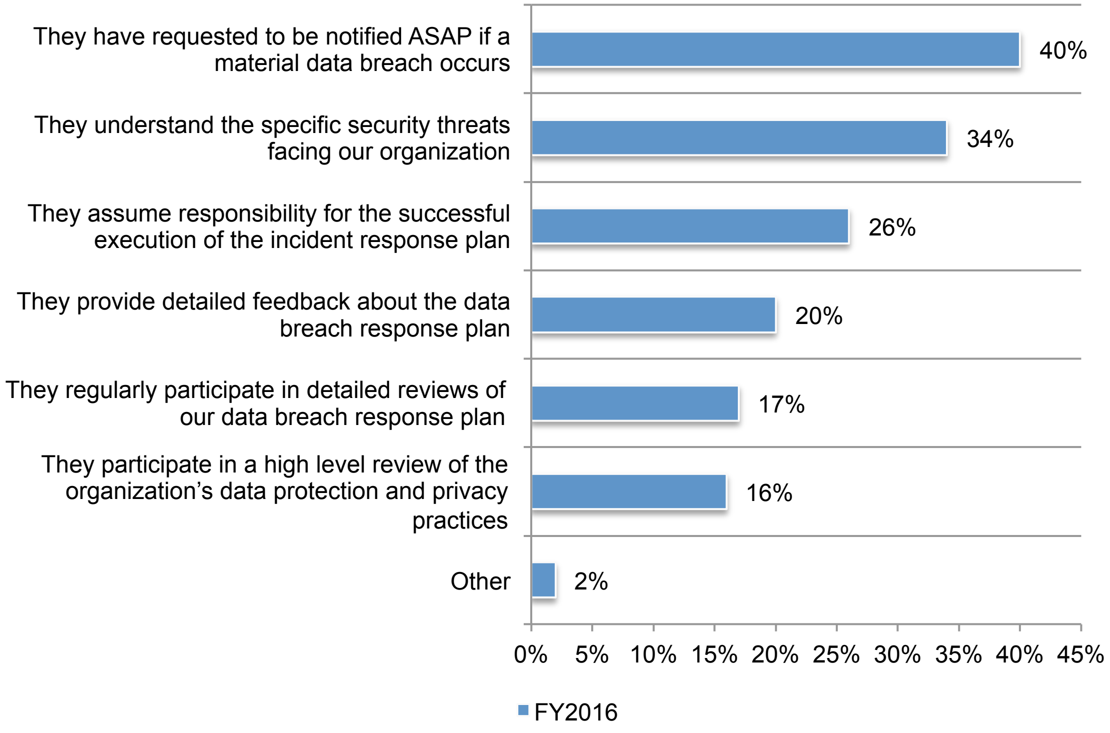
Figure 3. Which of the following issues would have the greatest impact on your organization's reputation?
Two responses permitted



Most boards of directors, chairmen and CEOs are not actively engaged, and avoid responsibility, in data breach preparedness. Fifty-seven percent of respondents say their company's board of directors, chairman and CEO are not informed and involved in plans to deal with a possible data breach.

Figure 4 reveals the lack of engagement of corporate leaders in data breach response. Only 40 percent of respondents say they want to know ASAP if a material data breach occurs. Only about one-third (34 percent of respondents) say the board does understand the specific security threats facing their organization. Only 26 percent of respondents believe the board is willing to assume responsibility for the successful execution of the incident response plan.

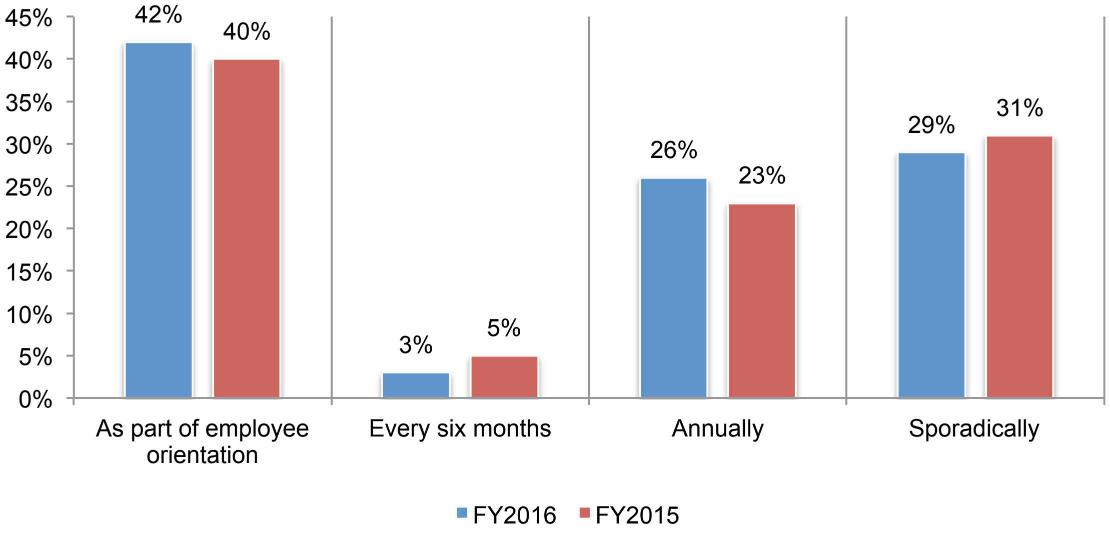
Figure 4. How are the boards of directors, chairmen and CEOs involved in data breach response plans?
More than one response permitted



As part of data breach preparedness, employee privacy and data protection awareness programs are critical to reducing the risk of employee negligence. While more companies are offering these programs, they are often only offered during employee orientation**.** In 2013, 44 percent of respondents said their organizations had such awareness programs for employees and other stakeholders who have access to sensitive or confidential personal information. In 2016, this increased to 61 percent of respondents.

As shown in Figure 5, only 42 percent of respondents say data protection and/or privacy awareness programs are provided as part of the new employee orientation process. Instead, the majority of companies represented in this study (55 percent of respondents) only conduct training annually (26 percent) or sporadically (29 percent). Employees not trained to understand the importance of protecting sensitive and confidential information create a risk of data breaches due to employee negligence. Instead, the

Figure 5. How often is privacy/data protection awareness and training conducted?



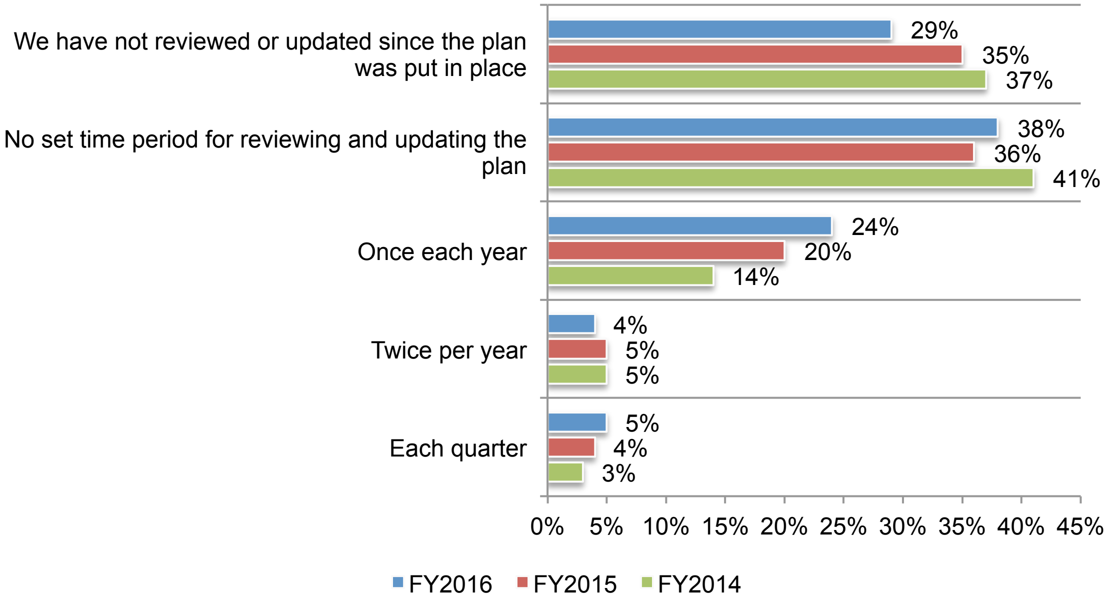
The struggle to create a better data breach preparedness plan

Most companies have a data breach response plan but it is not regularly reviewed. Eighty-six percent of respondents say their organizations have a data breach notification plan in place. A deterrent to an effective data breach response plan is keeping it current with changes in the risks and threats facing a company.

As shown in Figure 6, 67 percent of respondents say they either have not reviewed or updated the data breach preparedness plan since it was put in place (29 percent) or have not set time period for reviewing and updating the plan (38 percent).

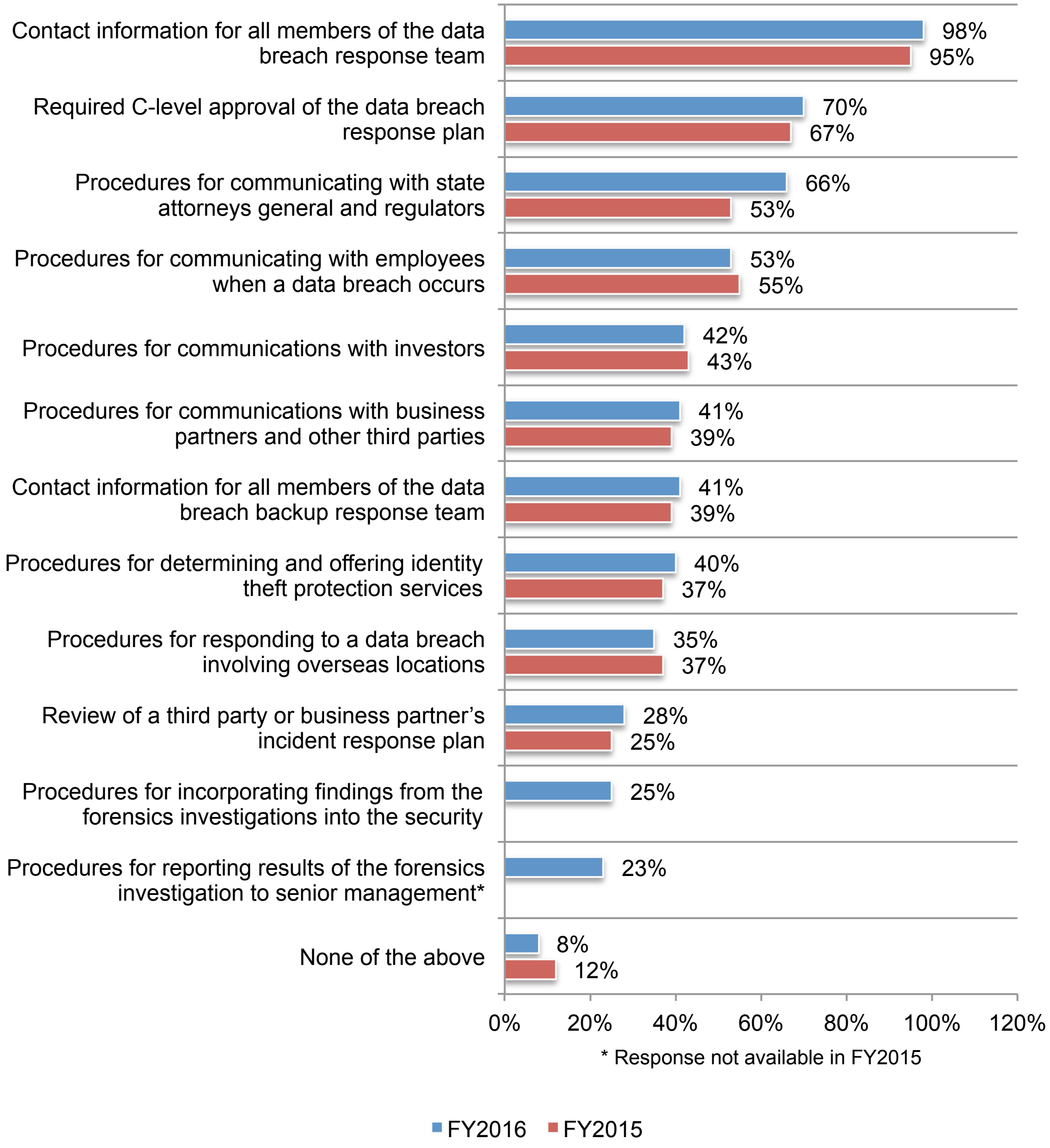
Fifty-one percent of respondents say their company includes in their incident response plans on how to deal with an international data breach. However, only 31 percent of respondents are either very confident or confident in the ability of their companies to deal with an international data breach.

Figure 6. How often does your company update the data breach response plan?



Stakeholder communication is key to an effective response plan. A comprehensive plan requires many activities to minimize the consequences of a data breach. As revealed in Figure 7, most of the requirements of a data breach response plan in the companies represented in this study focuses on internal and external communications. Communications with investors, business partners and other third parties are in most plans in order to maintain trust with these stakeholders. Procedures for communicating with state attorneys general and regulators increased significantly from 53 percent of respondents in 2015 to 66 percent of respondents in 2016.

Figure 7. What are the requirements in your company's data breach response plan?
More than one response permitted

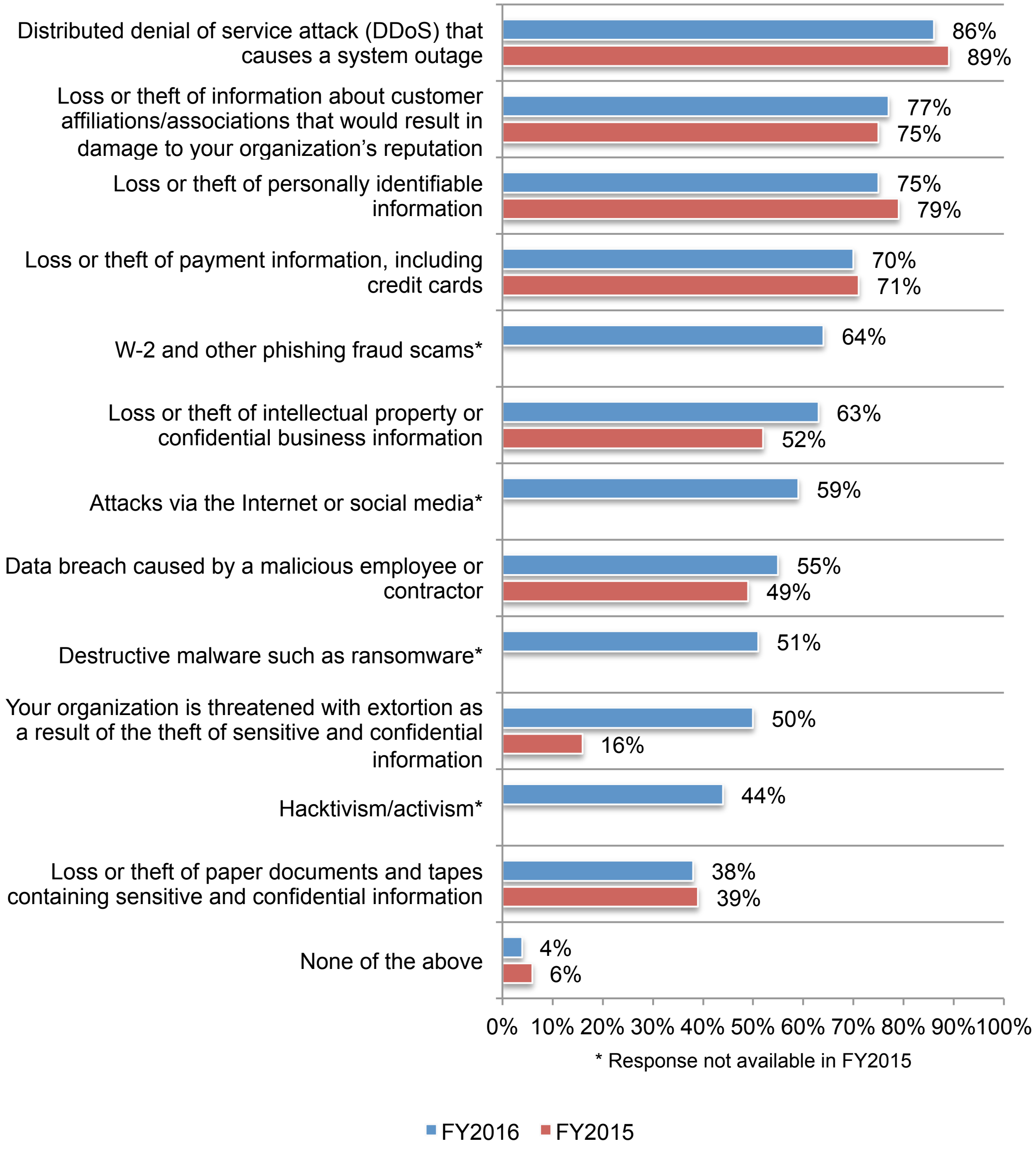


* Response not available in FY2015

The majority of companies are adding new guidance on security incidents to their plans. Figure 8 shows interesting trends in what guidance data breach plans include. W-2 and other phishing fraud scams, attacks via the Internet or social media, destructive malware such as ransomware are included in the majority of organizations. Forty-four percent of respondents say hactivism/activism is now included.

Other guidance includes managing such incidents as: a distributed denial of service attack (DDoS) that causes a system outage (86 percent of respondents), loss or theft of information about customer affiliations/associations that would result in damage to their organization (77 percent of respondents) loss or theft of payment information, including credit cards (70 percent of respondents) and loss or theft of personally identifiable information (75 percent of respondents),

Figure 8. What guidance does the plan provide on dealing with security incidents?
More than one response permitted

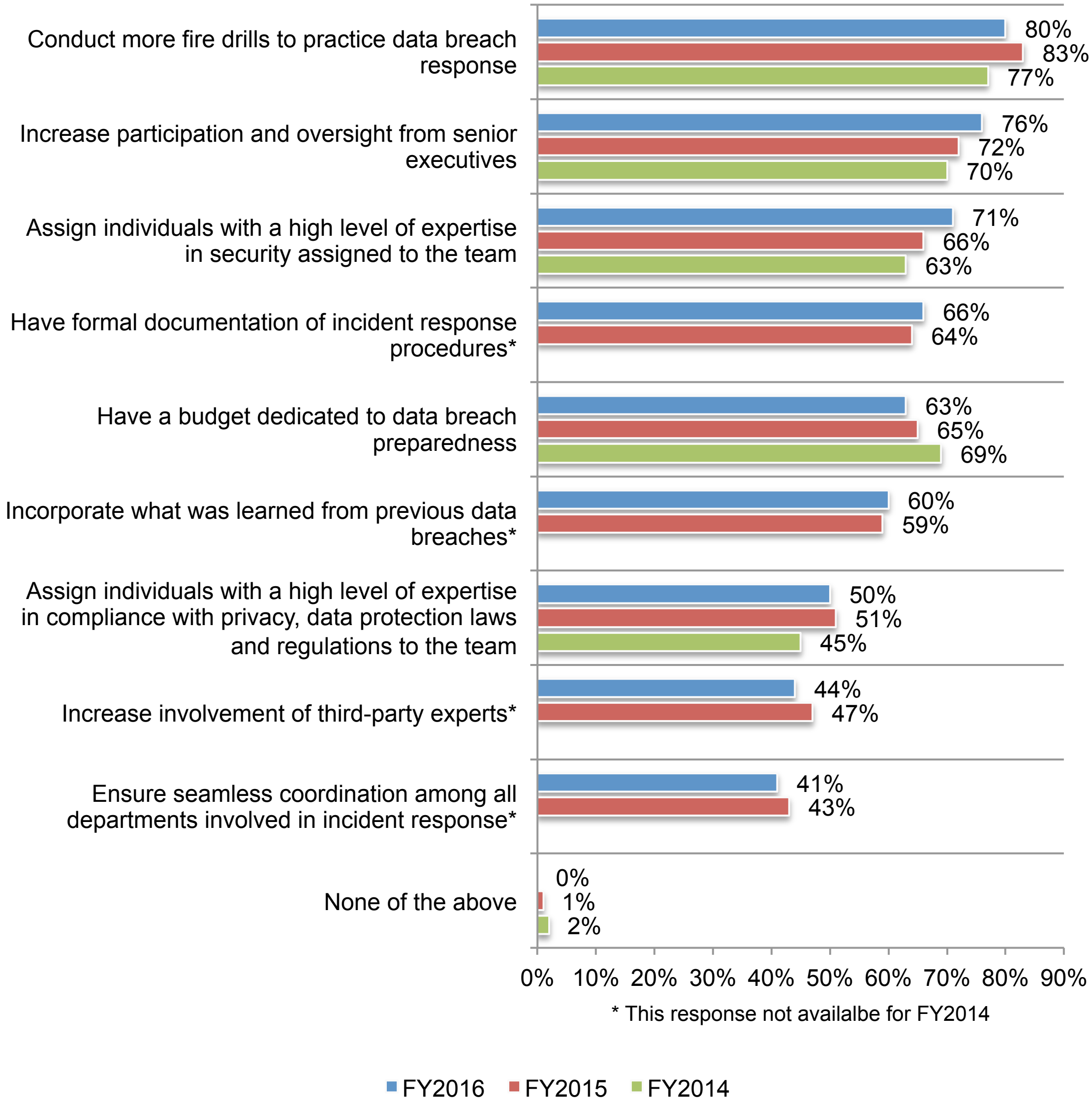


* Response not available in FY2015

To be effective, data breach response plans need senior level involvement. As discussed previously, those at the top area not actively engaged and avoid responsibility for the success of a data breach preparedness plan. Since 2014, respondents are increasingly asking for more participation and oversight from senior executives but it does not seem to be happening (an increase from 70 percent of respondents to 76 percent of respondents).

Other activities are growing in importance. They are: assignment of individuals with a high level of expertise in security assigned to the team (+8 percent), increase participation and oversight from senior executives (+6 percent) and assignment of individuals with a high level of expertise in compliance with privacy, data protection laws and regulations to the team (+5 percent), as shown in Figure 9.

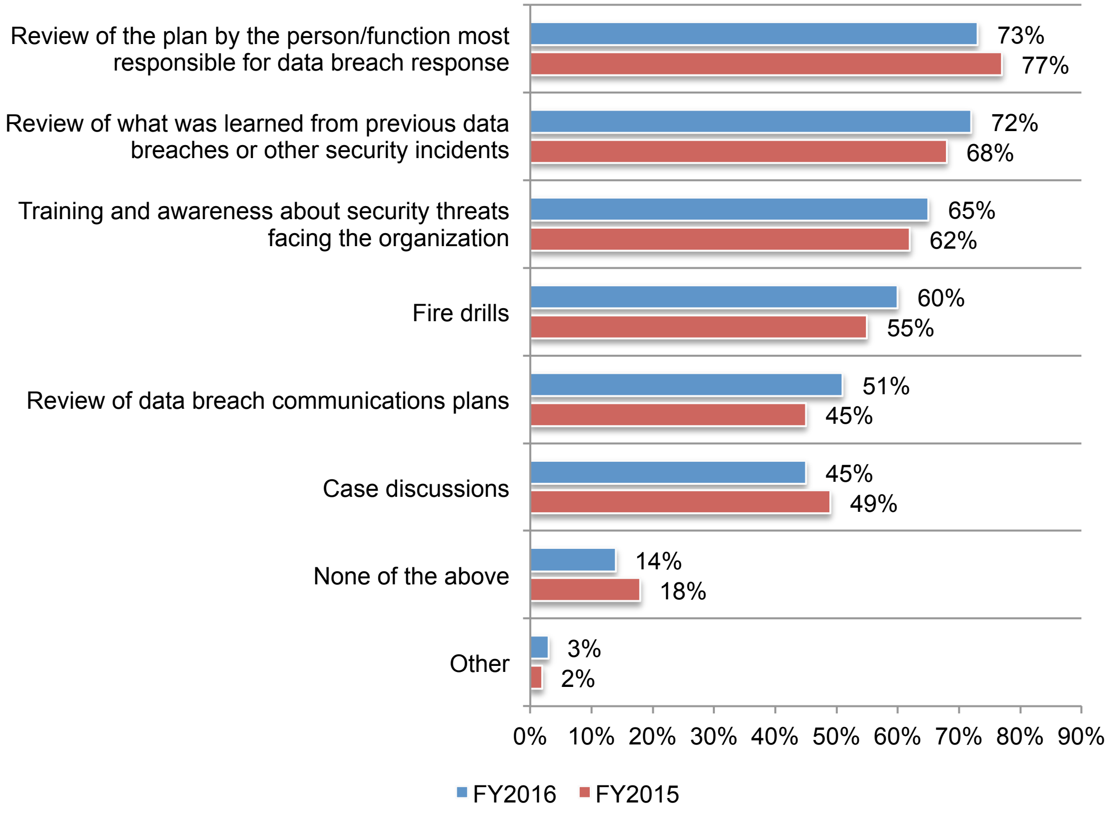
Figure 9. How could your data breach response plan become more effective?
More than one response permitted



More companies are conducting fire drills and reviewing data breach communication plans. Since 2014, more of these companies are reviewing their data breach communications plans (+6) and fire drills (+5) as shown in Figure 10.

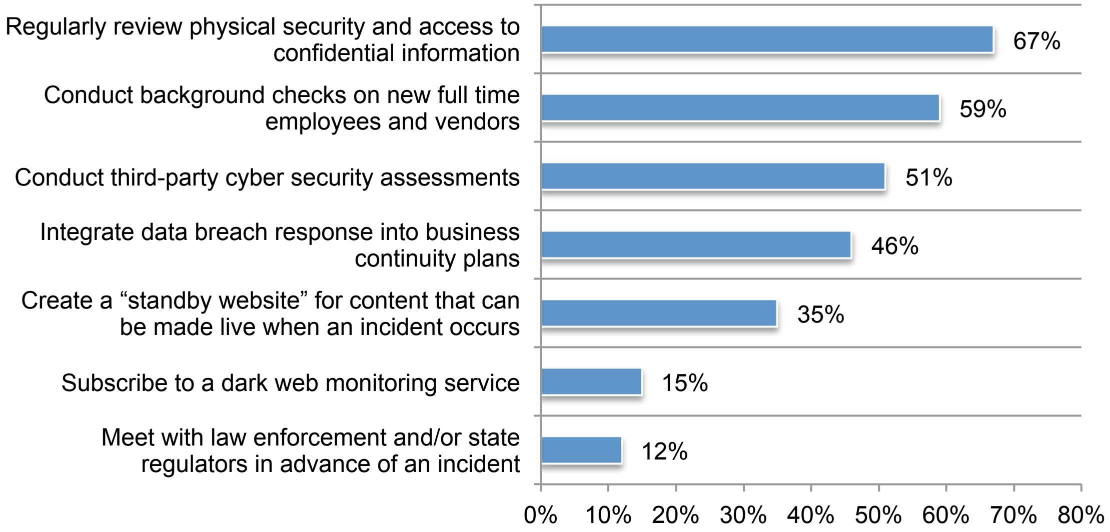
Other popular practices include: a review of the plan by the person or function most responsible for data breach response (73 percent of respondents), review of what was learned from previous data breaches or other security incidents (72 percent of respondents) and training and awareness about security threats facing the organization (65 percent of respondents).

Figure 10. What is included in the data breach response practice?
More than one response permitted



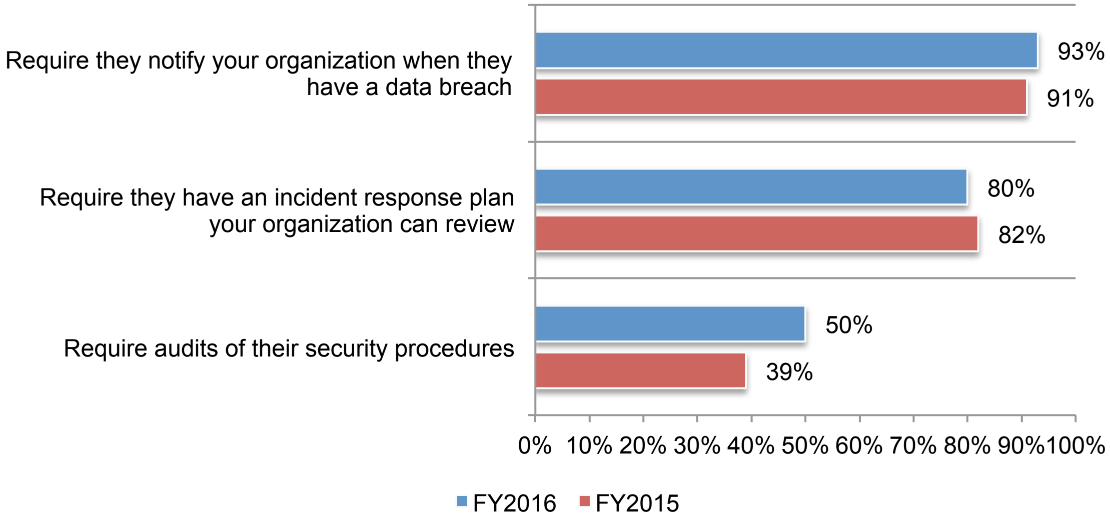
For the first time, we asked if companies are taking any special steps to prepare for a data breach. Sixty-seven percent of respondents say their organizations regularly review physical security and access to confidential information and conduct background checks on new full-time employees and vendors (59 percent of respondents). Very few companies are meeting with law enforcement and/or state regulators in advance of an incident.

Figure 11. Does your organization take any special steps to prepare for a data breach?
More than one response permitted



More companies are requiring audits of third parties security procedures. Companies should minimize the consequences of a third party data breach by asking for audits of their security procedures. Since 2015, more companies are requiring audits of third party's security procedures (an increase from 39 percent to 50 percent), as shown in Figure 12. Almost all, 93 percent of respondents, say they require third parties and business partners to notify them when they have a data breach and 80 percent of respondents require they have an incident response plan their organization can review.

Figure 12. How companies minimize the consequences of a third party data breach
More than one response permitted



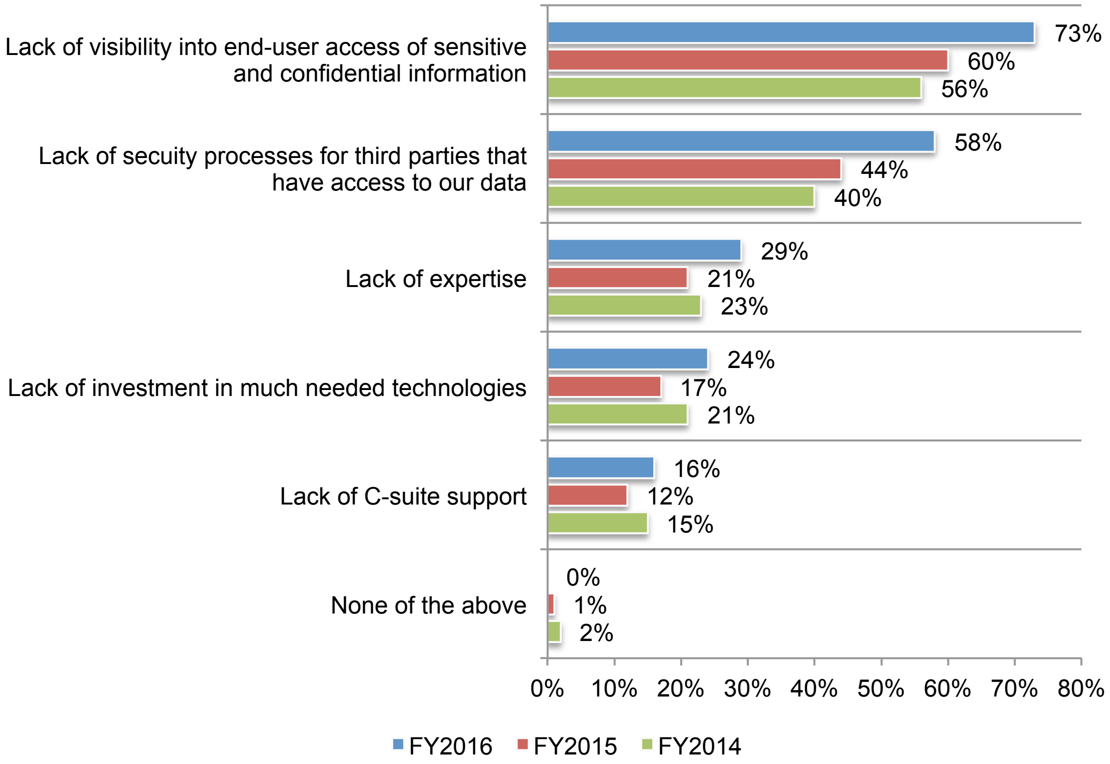
The role of IT security in data breach preparedness

Lack of visibility is the biggest barrier to improving IT security's ability to respond to a data breach. More companies are recognizing the importance of both visibility into end-user access of sensitive and confidential information and lack of security processes for third parties that have access to data.

According to Figure 13, the IT security function is prevented from improving its ability to respond to a data breach because of the lack of visibility into end-user access of sensitive and confidential information (73 percent of respondents), lack of security processes for third parties that have access to our data (58 percent of respondents). Lack of expertise also increased significantly since 2015.

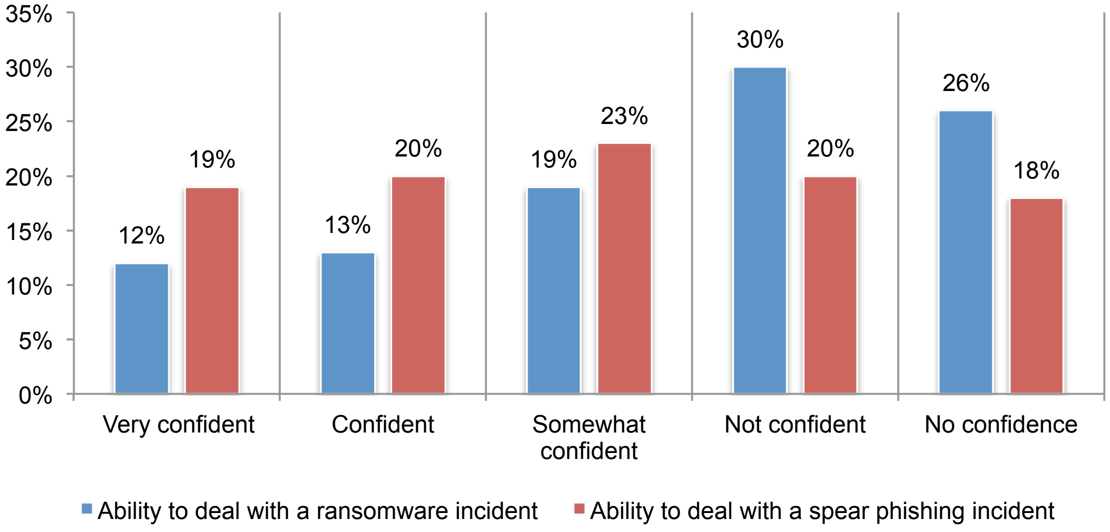
To address these challenges, investments in security technologies have increased to improve detection and response to a data breach. In 2015, 54 percent said investments increased, and this year 58 percent say security technology investments have increased.

Figure 13. What are the biggest barriers to improving the ability of IT security to respond to a data breach?
Two choices permitted



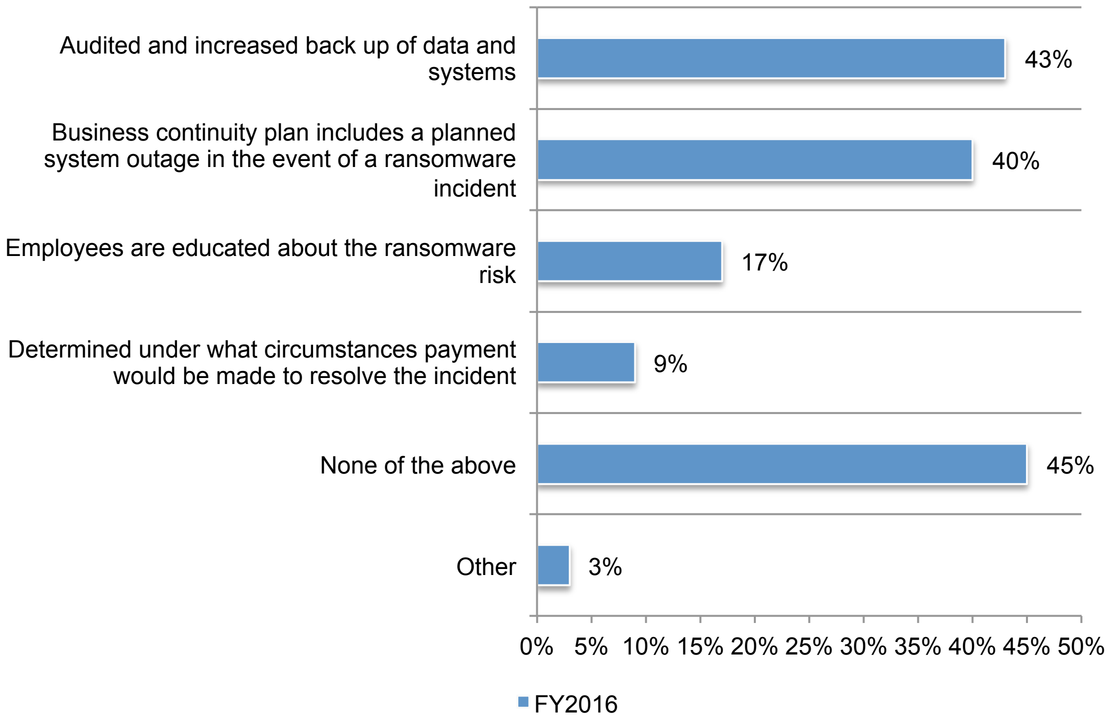
Companies are increasing security investments, but 56 percent of respondents are not confident they can deal with a ransomware attack. Thirty-eight percent of respondents are not confident they can deal with spear phishing incident.

Figure 15. Confidence in the ability to deal with a ransomware or spear phishing incident?



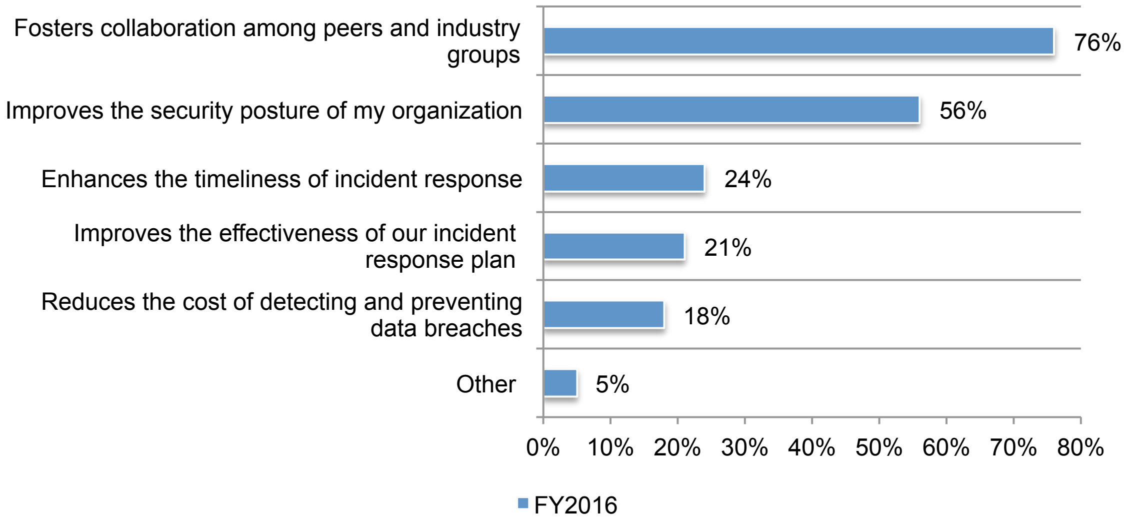
Ransomware is becoming a growing nightmare for IT security. Despite their lack of confidence in dealing with a ransomware attack**,** 45 percent of respondents say they are not taking any of the steps listed to prepare. Further, the lack of education of employees about the risk (only 17 percent of respondents) is making companies vulnerable to ransomware.

Figure 15. Have you taken the following steps to prepare for a ransomware incident?
More than one choice permitted



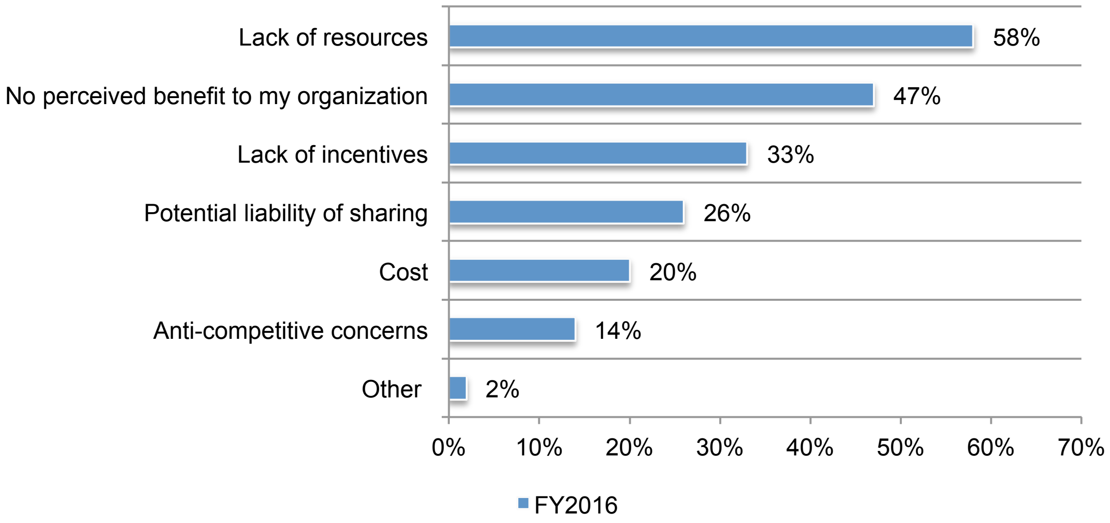
Sharing intelligence about data breach experiences and incident response plans can improve the ability to respond to a data breach. Forty-one percent of respondents say their organization participates in an initiative or program for sharing information with government and industry peers about data breaches and incident response**.** As shown in Figure 16, the most important reasons for sharing are the benefits from fostering collaboration among peers and industry groups (76 percent of respondents) and improving the security posture of the organization (56 percent of respondents).

Figure 16. Why do you share information about your data breach experience and incident response plans?
Two choices permitted



The main reason for not sharing is the lack of resources (58 percent of respondents) and no perceived benefit to their organization, according to Figure 17. The potential liability of sharing is not considered a deterrent to sharing my most companies.

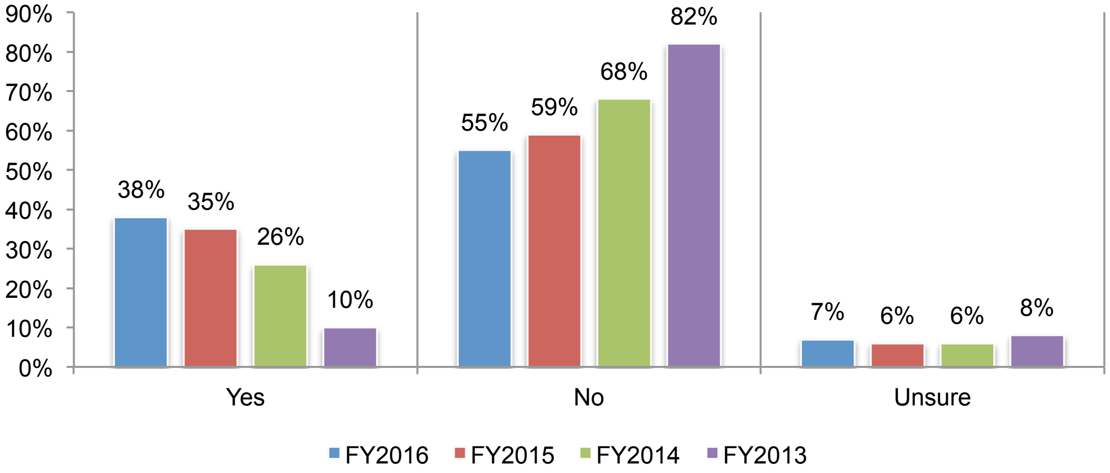
Figure 17. Reasons for not sharing information
More than one response permitted



Cyber insurance as part of a data breach preparedness plan

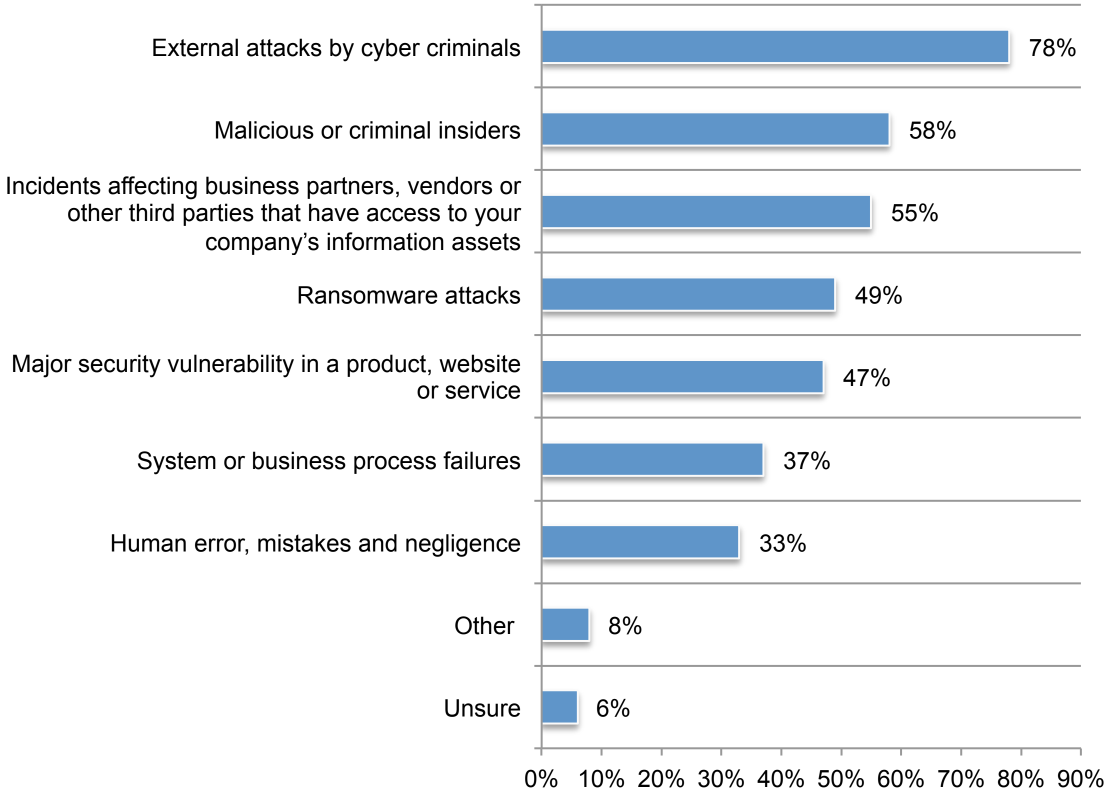
Data breach or cyber insurance policies are gaining traction. As shown in Figure 18, in 2013 only 10 percent said their organizations purchased such policies and this year 38 percent of respondents say their organizations are making such a purchase.

Figure 18. Does your organization have a data breach or cyber insurance policy?



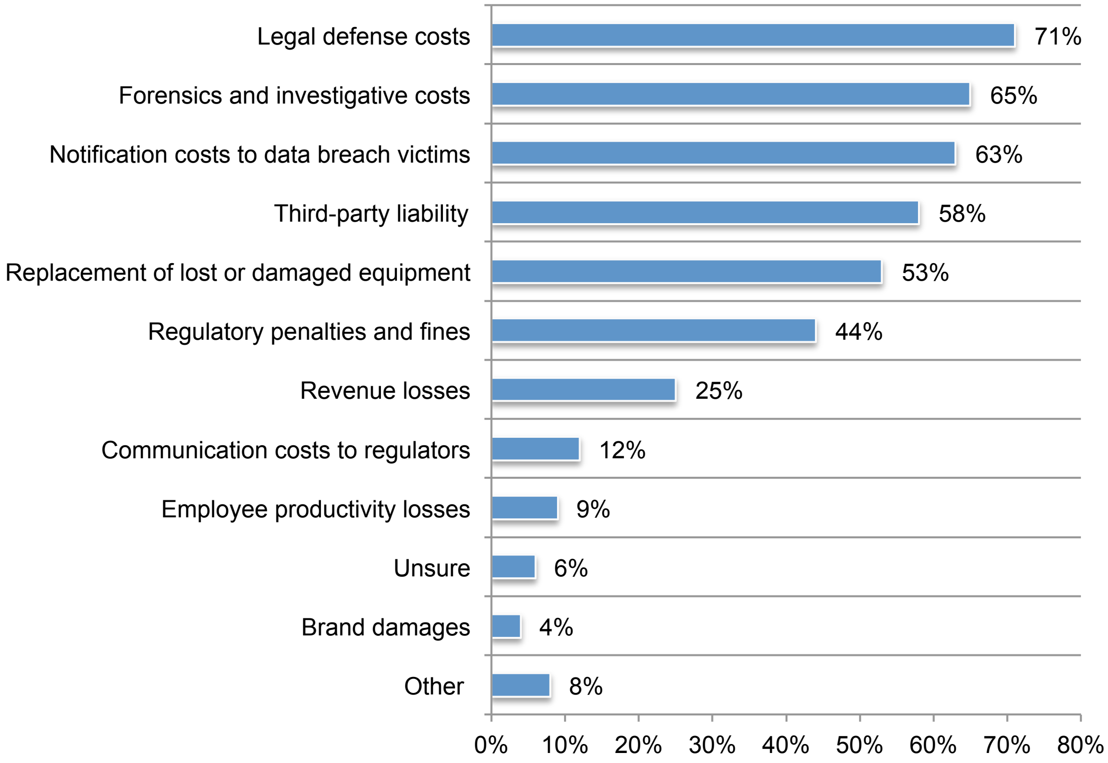
Cyber insurance policies mainly cover external cyber attacks. As shown in Figure 19, cyber insurance policies cover external attacks by cyber criminals (78 percent of respondents), malicious or criminal insiders (58 percent of respondents) and incidents affecting business partners, vendors or other third parties with access to company's information assets (55 percent of respondents). Forty-nine percent of respondents say the policy covers ransomware attacks.

Figure 19. What types of incidents does your organization's cyber insurance cover?
More than one choice permitted



Legal defense and forensics costs are most often covered. Most respondents (71 percent) say their cyber insurance policies reimburse legal defense and 65 percent of respondents say forensics and investigative costs are covered. Sixty-three percent of respondents say they cover notification costs to data breach victims, as shown in Figure 20.

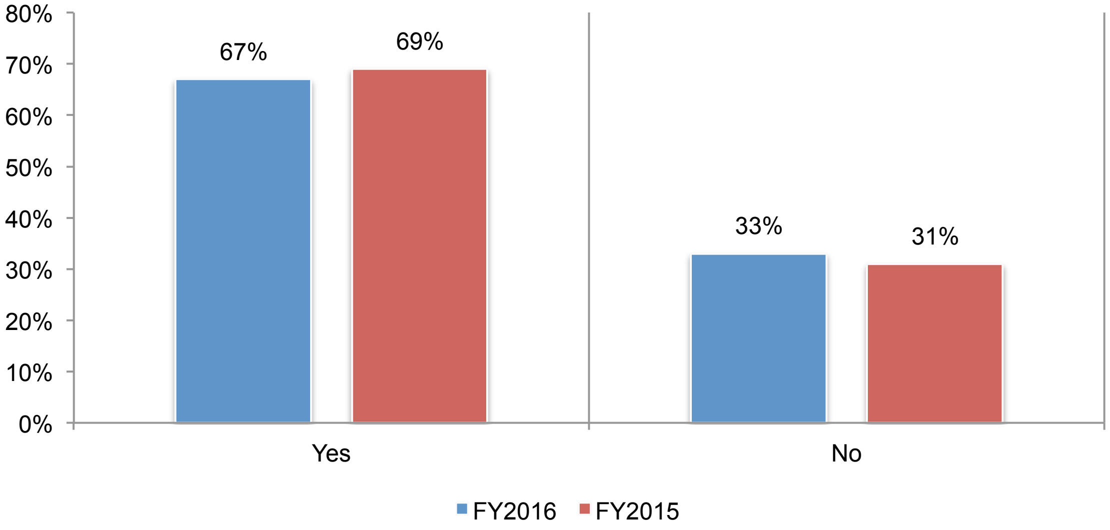
Figure 20. What coverage does this insurance offer your company?
More than one response permitted



The role identity theft products play in data breach preparedness

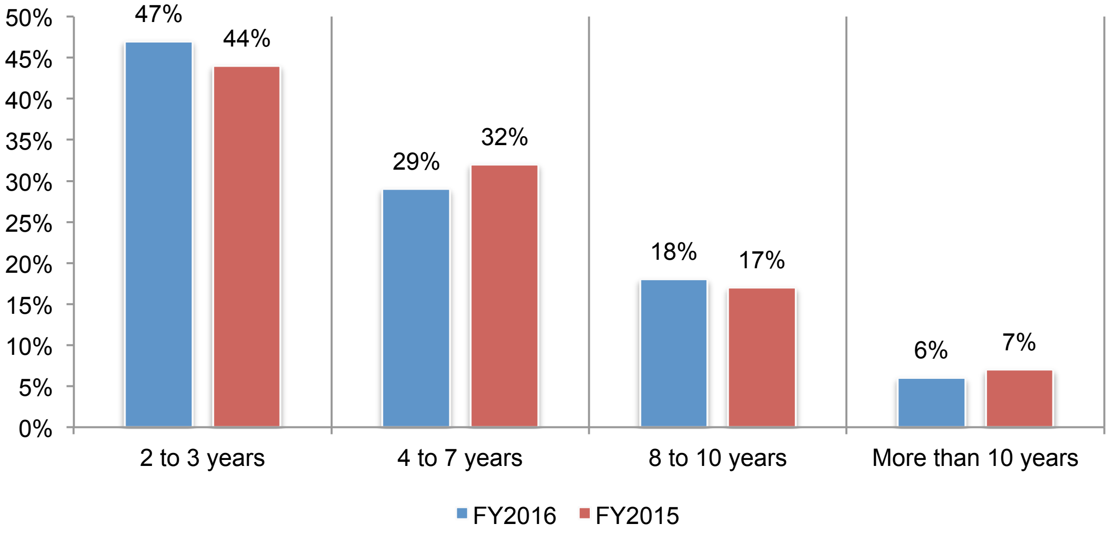
Following a data breach, credit monitoring and/or identity theft protection products are the best protection for consumers. Moreover, a year of protection is not considered sufficient. As shown in Figure 21, 67 percent believe identity theft protection should be provided for more than one year following a data breach.

Figure 21. Do you believe identity theft protection should be provided for more than one year?



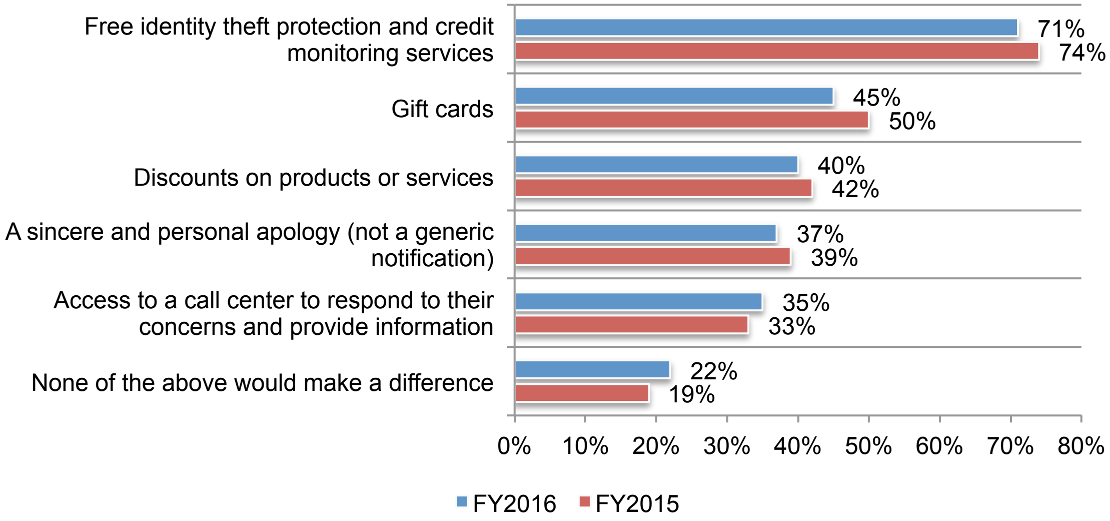
As shown in Figure 22, 53 percent of respondents (29 percent + 18 percent + 6 percent) say protection should be provided for a minimum of four years.

Figure 22. How long should identity theft protection be provided?



The best approach to keep customers and maintain reputation is to offer free services. To prevent loss of customers and reputation, 71 percent of respondents say providing free identity theft protection and credit monitoring services is the best step to take followed by 45 percent of respondents who say gift cards could help as well as 40 percent who say discounts on products or services should be offered to victims, as shown in Figure 23.

Figure 23. What is the best approach to keep customers and maintain reputation?
More than one response permitted



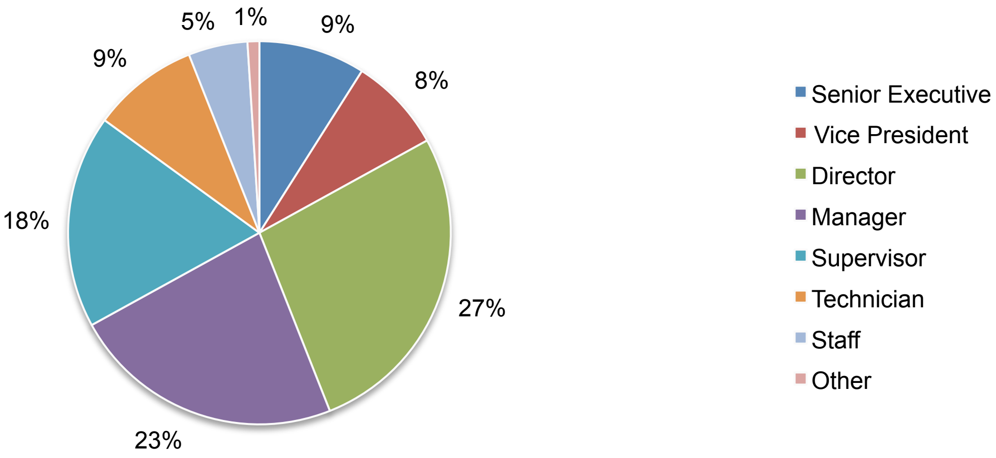
Part 5. Methods

A sampling frame of 14,878 executives and staff employees who work primarily in privacy and compliance in the United States were selected as participants to this survey. Table 1 shows 657 total returns. Screening and reliability checks required the removal of 53 surveys. Our final sample consisted of 619 surveys or a 4.2 percent response.

Table 1. Sample response	Freq	Pct%
Sampling frame	14,878	100.0%
Total returns	665	4.5%
Rejected or screened surveys	46	0.3%
Final sample	619	4.2%

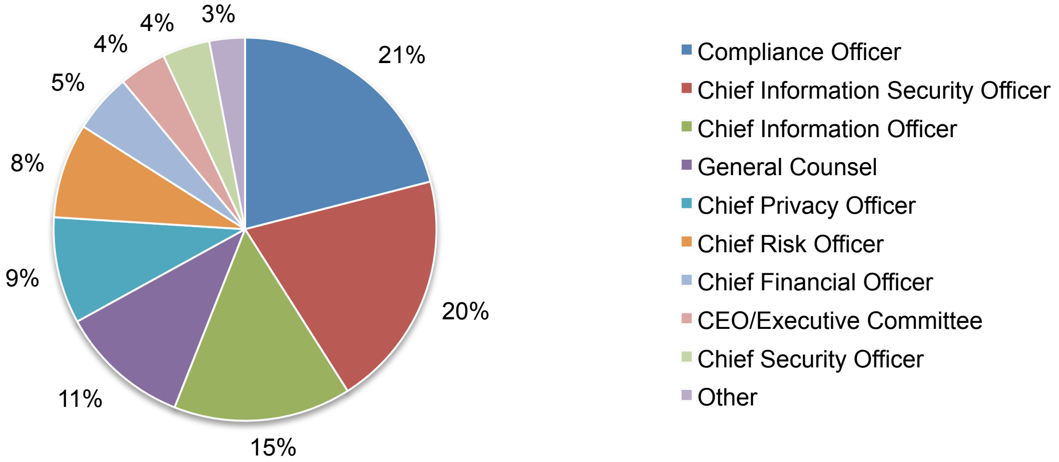
Pie Chart 1 reports the respondent's organizational level within participating organizations. By design, more than half of respondents (85 percent) are at or above the supervisory levels.

Pie Chart 1. Current position within the organization



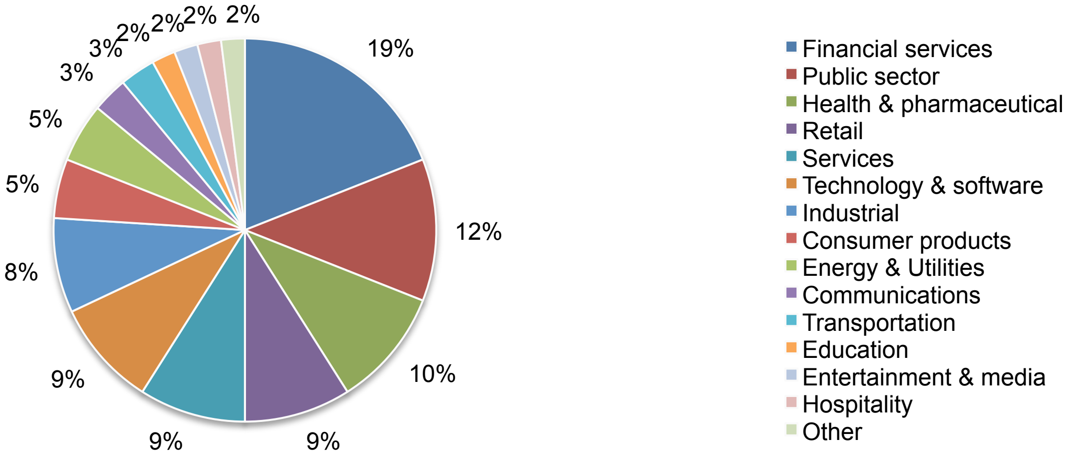
As shown in Pie Chart 2, 21 percent of respondents report to the compliance officer, 20 percent identified the chief information security officer as the primary person they report to and 15 percent responded they report to the chief information officer.

Pie Chart 2. Primary person respondent reports to within the organization



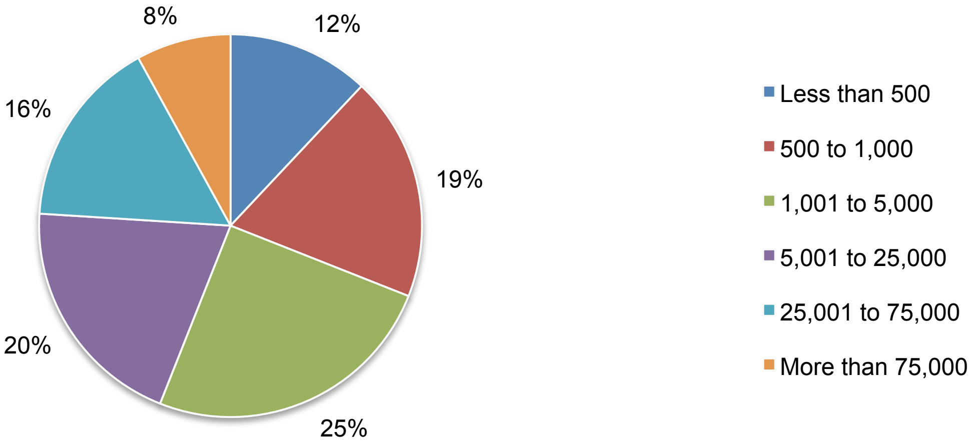
Pie Chart 3 reports the industry classification of respondents' organizations. This chart identifies financial services (19 percent) as the largest segment, followed by public sector (12 percent) and healthcare & pharmaceutical (10 percent).

Pie Chart 3. Primary industry focus



As shown in Pie Chart 5, 69 percent of respondents are from organizations with a global headcount of more than 1,000 employees.

Pie Chart 5. Global employee headcount



Part 4. Caveats to this study

There are inherent limitations to survey research that need to be carefully considered before drawing inferences from findings. The following items are specific limitations that are germane to most web-based surveys.

- Non-response bias: The current findings are based on a sample of survey returns. We sent surveys to a representative sample of individuals, resulting in a large number of usable returned responses. Despite non-response tests, it is always possible that individuals who did not participate are substantially different in terms of underlying beliefs from those who completed the instrument.

- Sampling-frame bias: The accuracy is based on contact information and the degree to which the list is representative of individuals who primarily work in privacy, compliance, IT and IT security. We also acknowledge that the results may be biased by external events such as media coverage. Finally, because we used a web-based collection method, it is possible that non-web responses by mailed survey or telephone call would result in a different pattern of findings.

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

Appendix: Detailed Survey Results

The following tables provide the frequency or percentage frequency of responses to all survey questions contained in this study. All survey responses were captured in August 2016.

Survey response	FY2016	FY2015	FY2014	FY2013
Sampling frame	14878	15040	14,639	11,056
Total returns	665	657	615	503
Rejected or screened surveys	46	53	48	32
Final sample	619	604	567	471
Response rate	4.2%	4.0%	3.9%	4.3%

Part 1. Background & Attributions				
Q1a. Did your organization have a data breach involving the loss or theft of more than 1,000 records containing sensitive or confidential customer or business information in the past 2 years?	FY2016	FY2015	FY2014	FY2013
Yes	52%	49%	43%	33%
No	34%	35%	40%	45%
Unsure	14%	16%	17%	22%
Total	100%	100%	100%	100%

Q1b. If yes, how frequently did these incidents occur during the past 2 years?	FY2016	FY2015	FY2014	FY2013
Only once	34%	37%	40%	48%
2 to 3 times	35%	32%	30%	27%
4 to 5 times	20%	21%	21%	16%
More than 5 times	11%	10%	9%	9%
Total	100%	100%	100%	100%

Attributions. Please rate each statement using the scale provided below each item. Strongly agree and agree response	FY2016	FY2015	FY2014
Q2. My organization is prepared to respond to the theft of sensitive and confidential information that requires notification to victims and regulators.	59%	57%	51%
Q3. My organization is prepared to respond to a data breach involving business confidential information and intellectual property.	41%	39%	38%
Q4 My organization is effective at doing what needs to be done following a material data breach to prevent the loss of customers' and business partners' trust and confidence.	39%	36%	33%
Q5. My organization understands what needs to be done following a material data breach to prevent negative public opinion, blog posts and media reports.	34%	32%	32%
Q6. My organization is effective in having plans in place to respond to a data breach.	45%		
Q7. My organization is confident in its ability to minimize the financial and reputational consequences of a material data breach.	27%	28%	
Q8. Following a data breach, a credit monitoring and/or identity theft protection product is the best protection for consumers.	59%	56%	54%

Q9a. Following a data breach involving customers' or employees' sensitive or confidential information, do you believe identity theft protection should be provided for more than one year?	FY2016	FY2015
Yes	67%	69%
No	33%	31%
Total	100%	100%

Q9b. If yes, how long should identity theft protection be provided?	FY2016	FY2015
2 to 3 years	47%	44%
4 to 7 years	29%	32%
8 to 10 years	18%	17%
More than 10 years	6%	7%
Total	100%	100%

Q10. If your company had a data breach, what do you think would be the best approach to keep your customers and maintain your reputation?	FY2016	FY2015
Free identity theft protection and credit monitoring services	71%	74%
A sincere and personal apology (not a generic notification)	37%	39%
Discounts on products or services	40%	42%
Gift cards	45%	50%
Access to a call center to respond to their concerns and provide information	35%	33%
None of the above would make a difference	22%	19%
Total	250%	257%

Q11. Which of the following issues would have the greatest impact on your organization's reputation? Please select one choice.	FY2016	FY2015*
Poor customer service	31%	55%
Labor or union dispute	2%	7%
Environmental incident	7%	16%
Data breach	23%	39%
Regulatory fines	5%	14%
Publicized lawsuits	12%	25%
Product recall	19%	36%
CEO's salary	1%	8%
Total	100%	200%

* Two responses permitted

Part 2. Data breach preparedness

Q12a. Is your company's board of directors, chairman and CEO informed and involved in plans to deal with a possible data breach?	FY2016	FY2015	FY2014
Yes	43%	39%	29%
No	44%	48%	59%
Unsure	13%	13%	12%
Total	100%	100%	100%

Q12b. If yes, how are they involved? Please select all that apply	FY2016	FY2015	FY2014
They regularly participate in detailed reviews of our data breach response plan	17%		
They understand the specific security threats facing our organization	34%		
They provide detailed feedback about the data breach response plan	20%		
They assume responsibility for the successful execution of the incident response plan	26%		
They have requested to be notified ASAP if a material data breach occurs	40%	41%	36%
They participate in a high level review of the organization's data protection and privacy practices	16%	15%	18%
Other	2%	1%	2%
Total	155%	162%	151%

Q13. What types of data losses is your organization most concerned about? Please select the top two.	FY2016	FY2015
Loss or theft of employee personal data	42%	45%
Loss or theft of medical data	10%	12%
Loss or theft of consumer data	53%	53%
Loss or theft of intellectual property	71%	64%
Loss or theft of consumer payment card data	24%	26%
Total	200%	200%

Q14. What are the two biggest barriers to improving the ability of IT security to respond to a data breach? Please select the top two reasons.	FY2016	FY2015	FY2014
Lack of investment in much needed technologies	24%	17%	21%
Lack of expertise	29%	21%	23%
Lack of C-suite support	16%	12%	15%
Lack of security processes for third parties that have access to our data	58%	44%	40%
Lack of visibility into end-user access of sensitive and confidential information	73%	60%	56%
Proliferation of mobile devices and cloud services		45%	43%
None of the above	0%	1%	2%
Total	200%	200%	200%

Q15. In the past 12 months, has your organization increased its investment in security technologies in order to be able to detect and respond quickly to a data breach?	FY2016	FY2015	FY2014
Yes	58%	54%	48%
No	38%	41%	46%
Unsure	4%	5%	6%
Total	100%	100%	100%

Q16. How confident is your organization in its ability to deal with a ransomware incident?	FY2016
Very confident	12%
Confident	13%
Somewhat confident	19%
Not confident	30%
No confidence	26%
Total	100%

Q17. How confident is your organization in its ability to deal with a spear phishing incident?	FY2016
Very confident	19%
Confident	20%
Somewhat confident	23%
Not confident	20%
No confidence	18%
Total	100%

Q18. Have you taken the following steps to prepare for a ransomware incident? Please select all that apply.	FY2016
Determined under what circumstances payment would be made to resolve the incident	9%
Audited and increased back up of data and systems	43%
Business continuity plan includes a planned system outage in the event of a ransomware incident	40%
Employees are educated about the ransomware risk	17%
None of the above	45%
Other	3%
Total	157%

Q19a. Does your organization have a privacy/data protection awareness and training program for employees and other stakeholders who have access to sensitive or confidential personal information?	FY2016	FY2015	FY2014	FY2013
Yes	61%	57%	54%	44%
No	37%	39%	43%	52%
Unsure	2%	4%	3%	4%
Total	100%	100%	100%	100%

Q19b. If yes, how often is training conducted?	FY2016	FY2015
As part of employee orientation	42%	40%
Every six months	3%	5%
Annually	26%	23%
Sporadically	29%	31%
Unsure	0%	1%
Total	100%	100%

Q19c. Are the awareness and training programs regularly reviewed and updated to ensure the content addresses the areas of greatest risk to the organization?	FY2016	FY2015
Yes	50%	47%
No	45%	45%
Unsure	5%	8%
Total	100%	100%

Q20a. Does your organization have a data breach or cyber insurance policy?	FY2016	FY2015	FY2014	FY2013
Yes	38%	35%	26%	10%
No	55%	59%	68%	82%
Unsure	7%	6%	6%	8%
Total	100%	100%	100%	100%

Q20b. If no, does your organization plan to purchase data breach or cyber insurance policy?	FY2016	FY2015
Yes, within the next six months	19%	17%
Yes, within the next year	24%	20%
Yes, within the next two years	14%	15%
No plans to purchase	40%	44%
Unsure	3%	4%
Total	100%	100%

Q21. What types of incidents does your organization's cyber insurance cover? Please select all that apply.	FY2016
External attacks by cyber criminals	78%
Malicious or criminal insiders	58%
System or business process failures	37%
Human error, mistakes and negligence	33%
Incidents affecting business partners, vendors or other third parties that have access to your company's information assets	55%
Ransomware attacks	49%
Major security vulnerability in a product, website or service	47%
Other	8%
Unsure	6%
Total	371%

Q22. What coverage does this insurance offer your company? Please select all that apply.	FY2016
Forensics and investigative costs	65%
Notification costs to data breach victims	63%
Communication costs to regulators	12%
Employee productivity losses	9%
Replacement of lost or damaged equipment	53%
Revenue losses	25%
Legal defense costs	71%
Regulatory penalties and fines	44%
Third-party liability	58%
Brand damages	4%
Other	8%
Unsure	6%
Total	418%

Q23. What steps do you take to minimize the consequences of a data breach involving a business partner or other third party? Please select all that apply.	FY2016	FY2015
Require they have an incident response plan your organization can review	80%	82%
Require they notify your organization when they have a data breach	93%	91%
Require audits of their security procedures	50%	39%
Total	223%	212%

Q24a. Does your organization participate in an initiative or program for sharing information with government and industry peers about data breaches and incident response?	FY2016
Yes	41%
No	59%
Total	100%

Q24b. If your organization shares information about its data breach experience and incident response plans, what are the main reasons? Please select only two choices.	FY2016
Improves the security posture of my organization	56%
Improves the effectiveness of our incident response plan	21%
Enhances the timeliness of incident response	24%
Reduces the cost of detecting and preventing data breaches	18%
Fosters collaboration among peers and industry groups	76%
Other	5%
Total	200%

Q24c. If no, why does your organization not participate in a threat-sharing program? Please select only two choices.	FY2016
Cost	20%
Potential liability of sharing	26%
Anti-competitive concerns	14%
Lack of resources	58%
Lack of incentives	33%
No perceived benefit to my organization	47%
Other	2%
Total	200%

Part 3. Data breach response plan

Q25a. Does your organization have a data breach response plan in place?	FY2016	FY2015	FY2014	FY2013
Yes	86%	81%	73%	61%
No	14%	19%	22%	30%
Don't know			5%	9%
Total	100%	100%	100%	100%

Q25b. If no, why?	FY2016	FY2015	FY2014
No resources or budget	41%	40%	44%
Not important to have data breach response plan in place	15%	18%	25%
Lack of C-level support	21%	20%	16%
Outsourced to consultants	23%	21%	13%
Other	0%	1%	2%
Total	100%	100%	100%

Q26. How often does your company update the data breach response plan?	FY2016	FY2015	FY2014
Each quarter	5%	4%	3%
Twice per year	4%	5%	5%
Once each year	24%	20%	14%
No set time period for reviewing and updating the plan	38%	36%	41%
We have not reviewed or updated since the plan was put in place	29%	35%	37%
Total	100%	100%	100%

Q27. In addition to documenting and practicing your data breach plan, does your organization take any of the following additional steps to prepare?	FY2016
Conduct third-party cyber security assessments	51%
Integrate data breach response into business continuity plans	46%
Create a “standby website” for content that can be made live when an incident occurs	35%
Regularly review physical security and access to confidential information	67%
Meet with law enforcement and/or state regulators in advance of an incident	12%
Subscribe to a dark web monitoring service	15%
Conduct background checks on new full time employees and vendors	59%
Total	

Q28.Does your data breach response plan include the following requirements? Please select all that apply.	FY2016	FY2015
Required C-level approval of the data breach response plan	70%	67%
Contact information for all members of the data breach response team	98%	95%
Contact information for all members of the data breach backup response team	41%	39%
Procedures for communicating with employees when a data breach occurs	53%	55%
Procedures for responding to a data breach involving overseas locations	35%	37%
Procedures for communicating with state attorneys general and regulators	66%	53%
Procedures for communications with investors	42%	43%
Procedures for communications with business partners and other third parties	41%	39%
Review of a third party or business partner's incident response plan	28%	25%
Procedures for determining and offering identity theft protection services	40%	37%
Procedures for reporting results of the forensics investigation to senior management	23%	
Procedures for incorporating findings from the forensics investigations into the security strategy	25%	
None of the above	8%	12%
Total	570%	502%

Q29. Does your data breach response plan offer guidance on managing the following security incidents? Please check all that apply.	FY2016	FY2015
Loss or theft of payment information, including credit cards	70%	71%
Loss or theft of personally identifiable information	75%	79%
Destructive malware such as ransomware	51%	
Hacktivism/activism	44%	
Attacks via the Internet or social media	59%	
W-2 and other phishing fraud scams	64%	
Distributed denial of service attack (DDoS) that causes a system outage	86%	89%
Loss or theft of information about customer affiliations/associations that would result in damage to your organization's reputation	77%	75%
Loss or theft of intellectual property or confidential business information	63%	52%
Data breach caused by a malicious employee or contractor	55%	49%
Your organization is threatened with extortion as a result of the theft of sensitive and confidential information	50%	16%
Loss or theft of paper documents and tapes containing sensitive and confidential information	38%	39%
None of the above	4%	6%
Total	736%	476%

Q30. Please rate the effectiveness of your organization's data breach response plan.	FY2016	FY2015	FY2014
Very effective	16%	11%	9%
Effective	26%	23%	21%
Somewhat effective	28%	25%	23%
Not effective	17%	26%	30%
Unsure	13%	15%	17%
Total	100%	100%	100%

Q31. How could the data breach response plan become more effective? Please select all the top three.	FY2016	FY2015	FY2014
Conduct more fire drills to practice data breach response	80%	83%	77%
Have formal documentation of incident response procedures	66%	64%	
Incorporate what was learned from previous data breaches	60%	59%	
Ensure seamless coordination among all departments involved in incident response	41%	43%	
Increase participation and oversight from senior executives	76%	72%	70%
Assign individuals with a high level of expertise in security assigned to the team	71%	66%	63%
Assign individuals with a high level of expertise in compliance with privacy, data protection laws and regulations to the team	50%	51%	45%
Have a budget dedicated to data breach preparedness	63%	65%	69%
Increase involvement of third-party experts	44%	47%	
None of the above	0%	1%	2%
Total	551%	551%	326%

Q32a. Does your organization practice responding to a data breach?	FY2016
Yes	68%
No	32%
Total	100%

Q32b. If yes, how often is the response practiced? Please check all that apply.	FY2016	FY2015
At least twice a year	39%	32%
Once each year	18%	15%
Every two years	5%	8%
More than two years	12%	15%
No set schedule	26%	30%
Total	100%	100%

Q32c. If yes, what is included in the practice response? Please check all that apply.	FY2016	FY2015
Fire drills	60%	55%
Case discussions	45%	49%
Training and awareness about security threats facing the organization	65%	62%
Review of the plan by the person/function most responsible for data breach response	73%	77%
Review of data breach communications plans	51%	45%
Review of what was learned from previous data breaches or other security incidents	72%	68%
None of the above	14%	18%
Other	3%	2%
Total	383%	376%

Q32d. If no, why? Please check all that apply.	FY2016	FY2015
Not enough budget	39%	35%
We are confident in our ability to respond to a data breach	46%	41%
Too difficult to schedule a practice response	76%	79%
Not a priority	64%	59%
Total	225%	214%

Q33. Does your incident response plan include processes to manage an international data breach?	FY2016
Yes	51%
No	42%
Unsure	7%
Total	100%

Q34. How confident is your organization in its ability to deal with an international data breach?	FY2016
Very confident	13%
Confident	18%
Somewhat confident	25%
Not confident	31%
No confidence	13%
Total	100%

Part 4. Organizational characteristics & respondent demographics

D1. What organizational level best describes your current position?	FY2016	FY2015	FY2014
Senior Executive	9%	7%	8%
Vice President	8%	9%	8%
Director	27%	29%	28%
Manager	23%	25%	27%
Supervisor	18%	17%	16%
Technician	9%	7%	8%
Staff	5%	4%	4%
Contractor	0%	1%	1%
Other	1%	1%	0%
Total	100%	100%	100%

D2. Check the **Primary Person** you report to within your organization.	FY2016	FY2015	FY2014
CEO/Executive Committee	4%	6%	5%
Chief Financial Officer	5%	5%	4%
General Counsel	11%	13%	14%
Chief Privacy Officer	9%	8%	8%
Chief Information Officer	15%	16%	19%
Compliance Officer	21%	20%	19%
Human Resources VP	1%	0%	2%
Chief Information Security Officer	20%	19%	16%
Chief Security Officer	4%	5%	4%
Chief Risk Officer	8%	6%	3%
Other	2%	2%	6%
Total	100%	100%	100%

D3. What industry best describes your organization’s industry focus?	FY2016	FY2015	FY2014
Agriculture & food services	0%	1%	1%
Communications	3%	2%	2%
Consumer products	5%	4%	0%
Defense	0%	0%	1%
Education	2%	2%	2%
Energy & Utilities	5%	4%	3%
Entertainment & media	2%	2%	4%
Financial services	19%	18%	19%
Health & pharmaceutical	10%	11%	13%
Hospitality	2%	2%	5%
Industrial	8%	8%	9%
Public sector	12%	12%	11%
Retail	9%	10%	10%
Services	9%	10%	8%
Technology & software	9%	8%	7%
Transportation	3%	3%	4%
Other	2%	3%	1%
Total	100%	100%	100%

D4. What is the worldwide headcount of your organization?	FY2016	FY2015	FY2014
Less than 500	12%	10%	11%
500 to 1,000	19%	18%	19%
1,001 to 5,000	25%	23%	24%
5,001 to 25,000	20%	22%	20%
25,001 to 75,000	16%	18%	17%
More than 75,000	8%	9%	9%
Total	100%	100%	100%

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 confidentiality standards to ensure that subjects are not asked extraneous, irrelevant or improper questions.