Ponemon INSTITUTE

Fifth 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: February 2018

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

Ponemon Institute, February 2018

Part 1. Introduction

Recent highly publicized data breaches involving customer records make it clear that many companies are not ready for a big data breach and will suffer significant financial and reputational consequences. In 2017, a Ponemon Institute study found that the average consolidated cost of a data breach is $3.62 million.[1] There are a number of factors that complicate data breach preparedness and should be incorporated into data breach response plans, including:

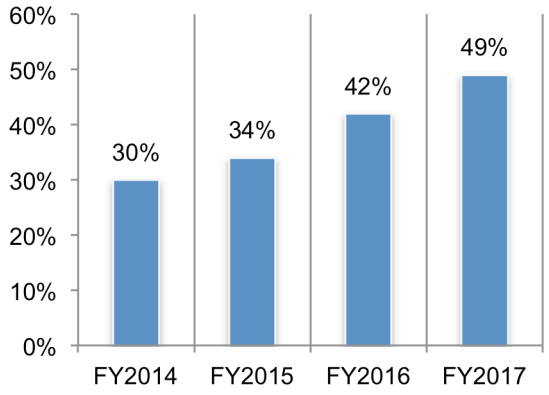
- New notification rules in the European Union's (EU) General Data Protection Regulation (GDPR) scheduled to go into effect in May 25, 2018[2]
- The increasing risk of a data breach due to unsecured Internet of Things (IoT) devices in the workplace
- The increasing risk of a data breach due to ransomware and spear phishing attacks

The *Fifth Annual Study: Is Your Company Ready for a Big Data Breach* sponsored by Experian® Data Breach Resolution and conducted by Ponemon Institute examines the progress companies are making in preparing for the increasing likelihood they will have personal and sensitive information lost or stolen in the coming year. Each year more companies represented in this research study have a data breach. In this year's study, 56 percent of respondents report their organization had a breach, an increase from 52 percent last year. Seventy percent of respondents say their organization had multiple breaches and 39 percent of respondents say their companies' data breaches were global.

Eighty-eight percent of companies represented in this research study have some type of data breach plan in place. Of these respondents, less than half of respondents (49 percent) say their companies' ability to respond to data breaches is either very effective or effective, as shown in Figure 1.

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

Very effective and Effective responses combined



The following findings reveal why 51 percent of respondents do not rate their breach response plan as very effective:

- Inability to prevent the loss of customers' and business partners' trust and confidence (60 percent of respondents)
- Not prepared to respond to a data breach involving business confidential information and intellectual property (60 percent of respondents)
- Inability to prevent negative public opinion, blog posts and media reports (64 percent of respondents)

[1] 2017 Ponemon Institute Cost of Data Breach Study, conducted by Ponemon Institute and sponsored by IBM Security, July 2017.

[2] For more information about the GDPR see *Data Protection Risks & Regulations in the Global Economy,* sponsored by Experian® Data Breach Resolution and conducted by Ponemon Institute, June 2017

- Inability to minimize the financial and reputational consequences of a material data breach (75 percent of respondents)

In this year's study, Ponemon Institute surveyed 624 executives and staff employees who work primarily in privacy, compliance and IT security in the United States. Of these, just 119 or 19 percent of the total respondents self-reported that their organizations' data breach response plan is highly effective. According to these respondents, their organizations are more likely to adopt the following practices:

1. Ensure senior level executives and boards of directors are knowledgeable about and engaged in the data breach response plan and preparedness. This includes having a high-level review of the organization's privacy and security preparedness and the threats they face.

2. Data breach response plans should include guidance on how to prevent negative publicity, maintain the trust and confidence of business partners and customers and minimize the financial and reputational consequences of the incident.

3. Data breaches caused by employee negligence are a concern of 80 percent of respondents. Organizations should conduct regular training and awareness programs on the consequences of mishandling sensitive confidential information. These programs should also educate employees about how to recognize and minimize spear phishing incidents.

4. Purchase cyber and data breach insurance. These policies can help manage the financial consequences of the incident. According to a recent Ponemon Institute study, data breaches resulting in business disruption have a greater impact on information assets than on PPE.[3]

5. Following a data breach, take steps to preserve customer trust and loyalty. In a recent Ponemon Institute study, 65 percent of consumers say being a victim of a data breach caused them to lose trust in the breached organization, and almost a third took steps to terminate their relationship.[4]

[3] *The 2017 Global Risk Transfer Comparison Report*, conducted by Ponemon Institute and sponsored by Aon Risk Services, April 2017
[4] *The Impact of Data Breaches on Reputation & Share Value: A Study of Marketers, IT Practitioners and Consumers*, conducted by Ponemon Institute and sponsored by Centrify, May 2017

Part 2. Key findings

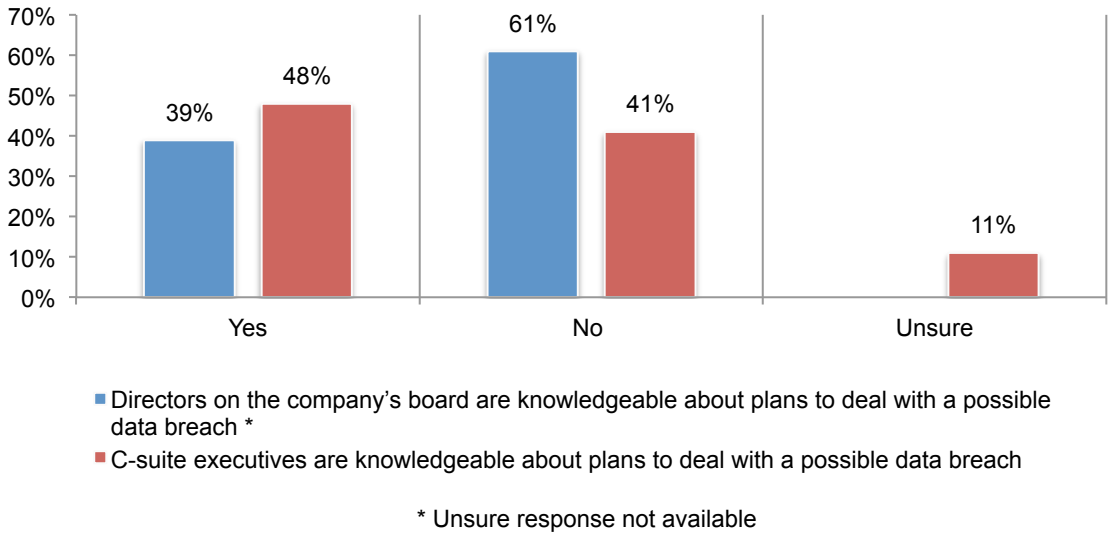
In this section, we provide an analysis of the key findings. The complete audited findings are presented in the Appendix of this report. When available, we compare the findings from previous studies to this year's findings. We have organized the report according to the following topics:

- The importance of good governance in data breach preparedness
- Effectiveness of data breach response plans
- Threats that affect data breach preparedness
- Best practices in data breach preparedness

The importance of good governance in data breach preparedness

Most boards of directors, chairmen and CEOs are not actively engaged, and avoid responsibility, in data breach preparedness. Less than half of respondents (48 percent) say C-suite executives and only 39 percent of respondents say boards of directors are informed and knowledgeable about how their companies plan to respond to a data breach.

Figure 2. Are C-suite executives and boards of directors knowledgeable about plans to deal with a possible data breach?

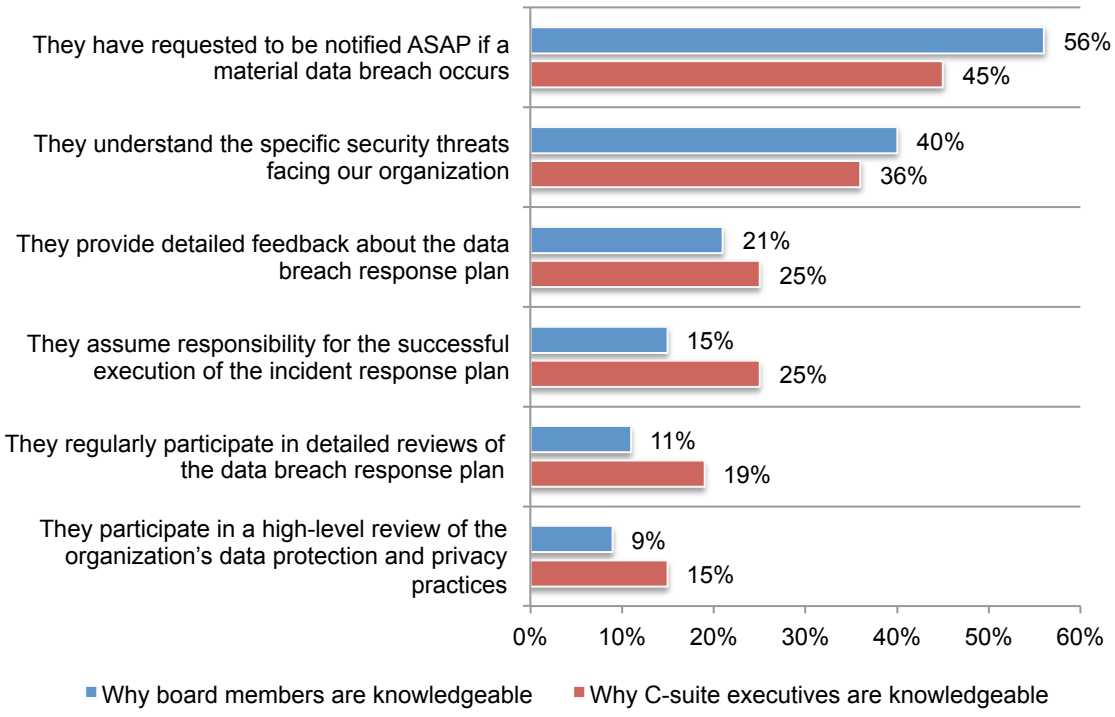


* Unsure response not available

Very few C-suite executives and board members actually participate in even a high-level review of their organizations' data protection and privacy practices. Figure 3 reveals the lack of engagement of corporate leaders in many areas important to reducing the consequences of a data breach.

Fifty-six percent of respondents say their board members want to know ASAP if a material data breach occurs. However, only 45 percent of respondents say the C-suite would want to be informed about a data breach. Only 40 percent of respondents say the board understands the specific security threats facing their organization and only 15 percent of respondents believe the board is willing to assume responsibility for the successful execution of the incident response plan.

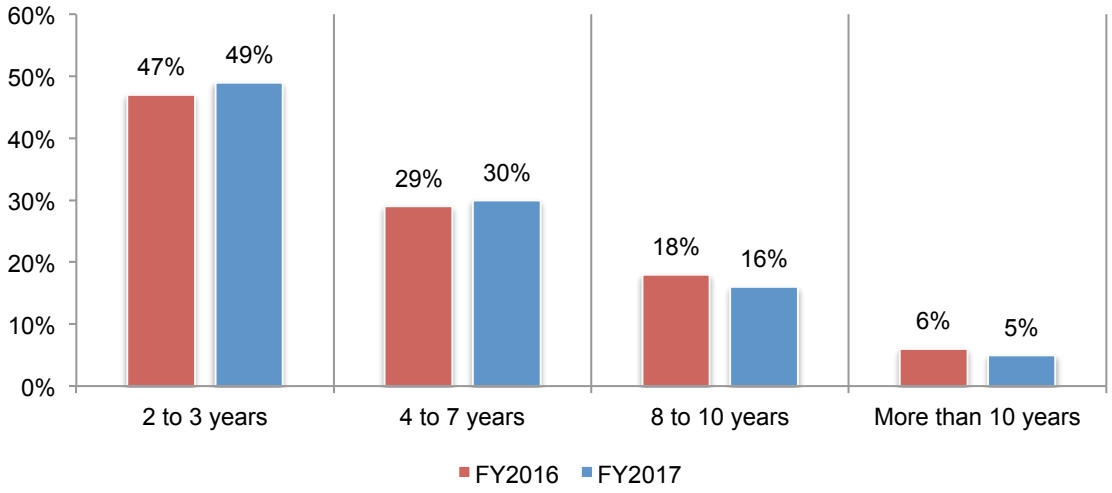
Figure 3. Why do you believe board members are knowledgeable?
From the yes responses only
More than one response permitted



Credit monitoring and identity theft protection need to be provided for more than one year. Respondents in high-performing organizations (77 percent) are more likely to say their organizations provide identity theft protection for more than one year. In the overall findings, 71 percent of respondents say such services should be offered at least four years.

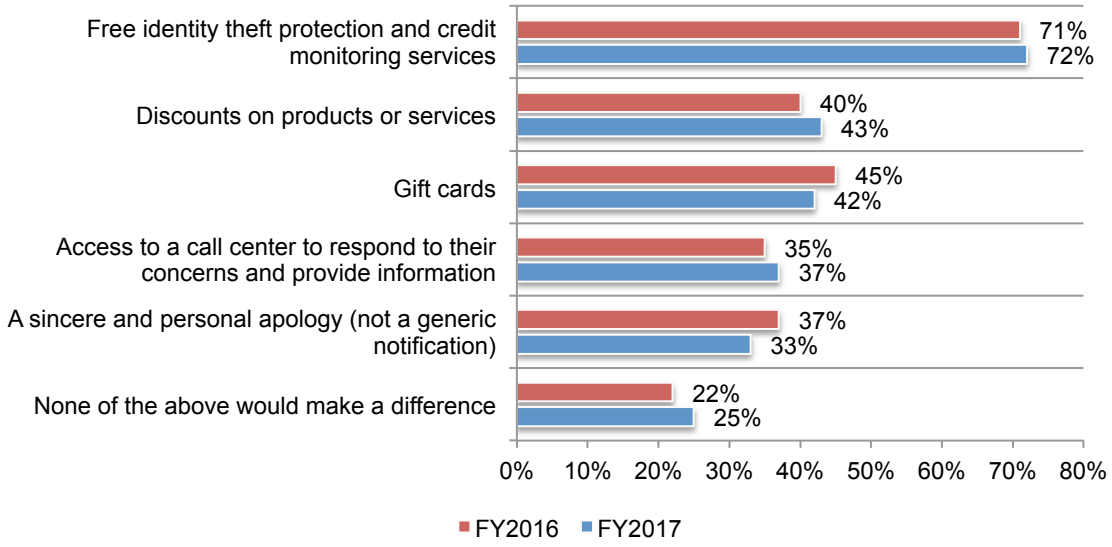
As shown in Figure 4, 51 percent of all respondents (30 percent + 16 percent + 5 percent) say protection should be provided for a minimum of four years. Last year, 53 percent said identity theft protection should be provided at least four years (29 percent + 18 percent + 6 percent).

Figure 4. How long should identity theft protection be provided?



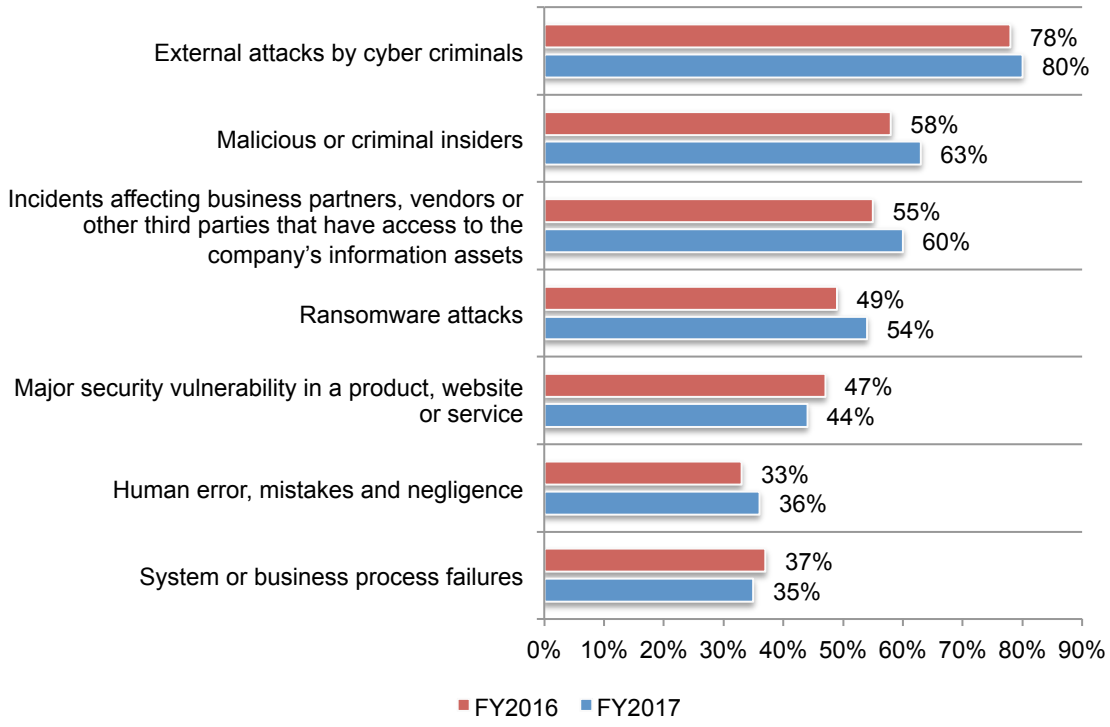
The best approach to keep customers and maintain reputation is to offer free identity theft protection and credit monitoring services. Seventy-two percent of respondents say providing free identity theft protection and credit monitoring services is the best step for preventing the loss of customers and for protecting reputation, followed by 43 percent of respondents who say that discounts on products or services help, as well as 42 percent who say gift cards should be offered to victims, as shown in Figure 5.

Figure 5. What is the best approach to keep customers and maintain reputation?
More than one response permitted



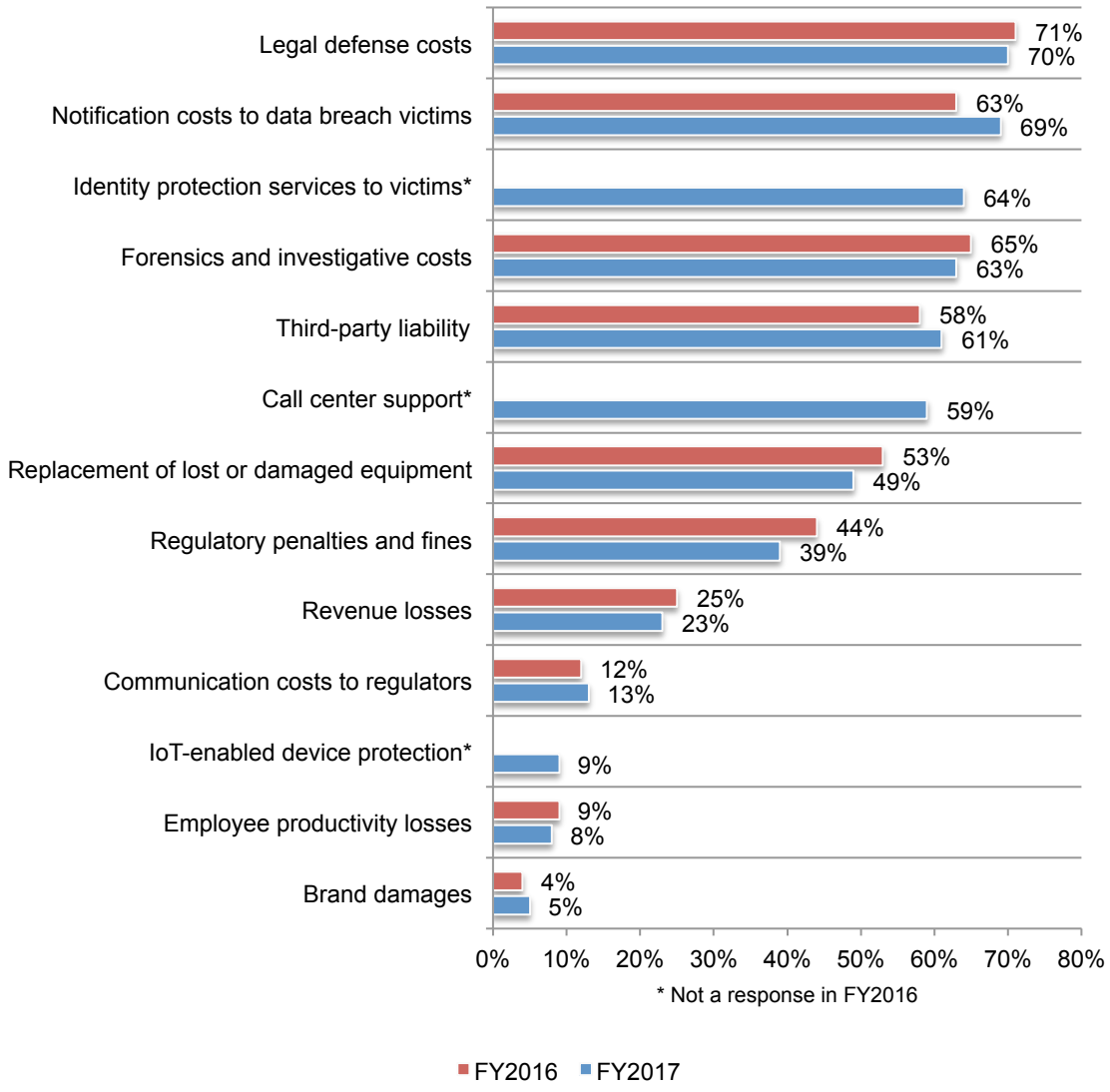
Cyber insurance policies mainly cover external cyber attacks. As shown in Figure 6, the 45 percent of respondents who have cyber insurance policies say they mainly cover external attacks by cyber criminals (80 percent of respondents), malicious or criminal insiders (63 percent of respondents) and incidents affecting business partners, vendors or other third parties with access to company's information assets (60 percent of respondents). Coverage for ransomware attacks increased from 49 percent of respondents in 2016 to 54 percent of respondents in this year's study.

Figure 6. What types of incidents does your organization's cyber insurance cover?
More than one choice permitted



Legal defense and notification costs are most often covered. Of the 45 percent of respondents who say their organizations have cyber insurance, most respondents (70 percent) say their cyber insurance policies reimburse legal defense costs and 69 percent of respondents say notification costs are covered, as shown in Figure 7. For the first time, respondents report their policies include identity protection services to victims (64 percent of respondents). Only nine percent of respondents say IoT-enabled device protection is offered.

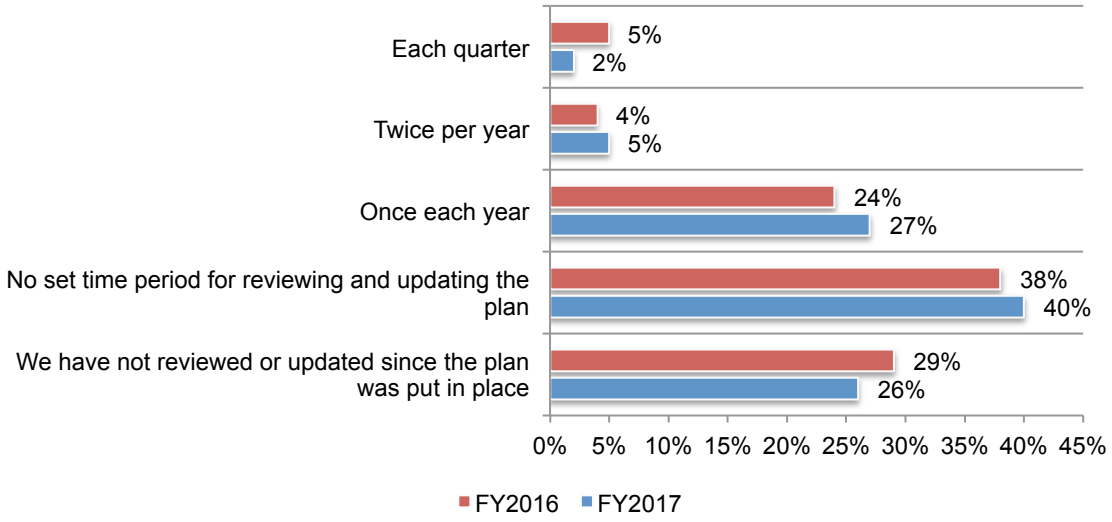
Figure 7. What coverage does this insurance offer your company?
More than one response permitted



Data breach response plan effectiveness

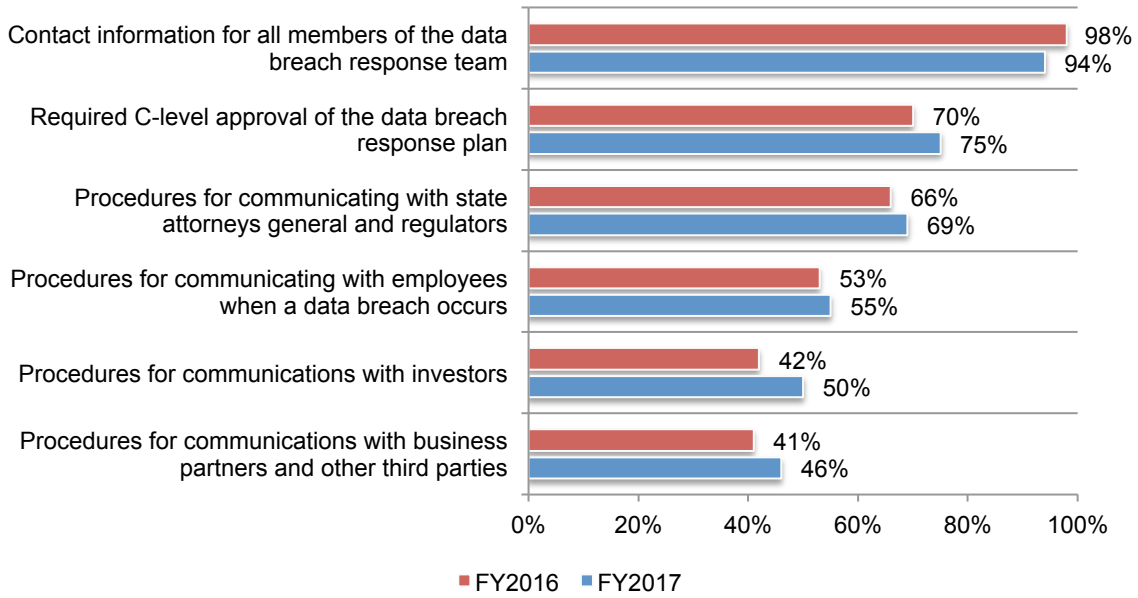
Most companies have a data breach response plan but it is not regularly reviewed. Eighty-eight percent of respondents say their organizations have a data breach notification plan in place. However, as shown in Figure 8, 66 percent of respondents have no set time for reviewing and updating the plan or have not reviewed the plan since it was put in place.

Figure 8. How often does your company update the data breach response plan?



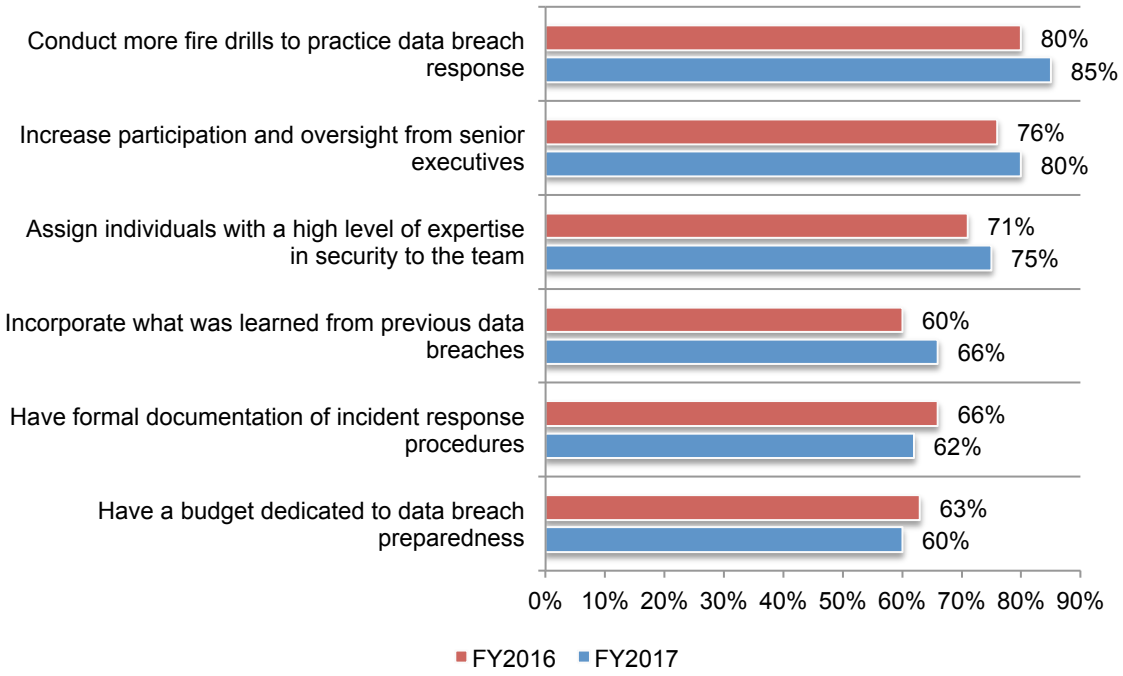
A comprehensive plan requires many activities to minimize the consequences of a data breach. As revealed in Figure 9, most of the requirements of a data breach response plan in the companies represented in this study focus on internal and external communications. Similar to last year, all plans include contact information for all members of the data breach response team.

Figure 9. What are the requirements in your company's data breach response plan?
More than one response permitted



To be effective, data breach response plans need senior level involvement. As discussed previously, those at the top are not actively engaged in the data breach response plan. According to Figure 10, most organizations believe conducting fire drills to practice data breach response and increased participation and oversight from senior executives would make data breach response plans more effective.

Figure 10. How could your data breach response plan become more effective?
More than one response permitted



Most respondents say their organization's data breach response practice includes a review of the plan by those most responsible for data breach response. This is followed by a review of what was learned from previous data breaches or other security incidents (75 percent of respondents) and training and awareness about security threats facing the organization (68 percent of respondents), as shown in Figure 11.

Figure 11. What is included in the data breach response practice?
More than one response permitted

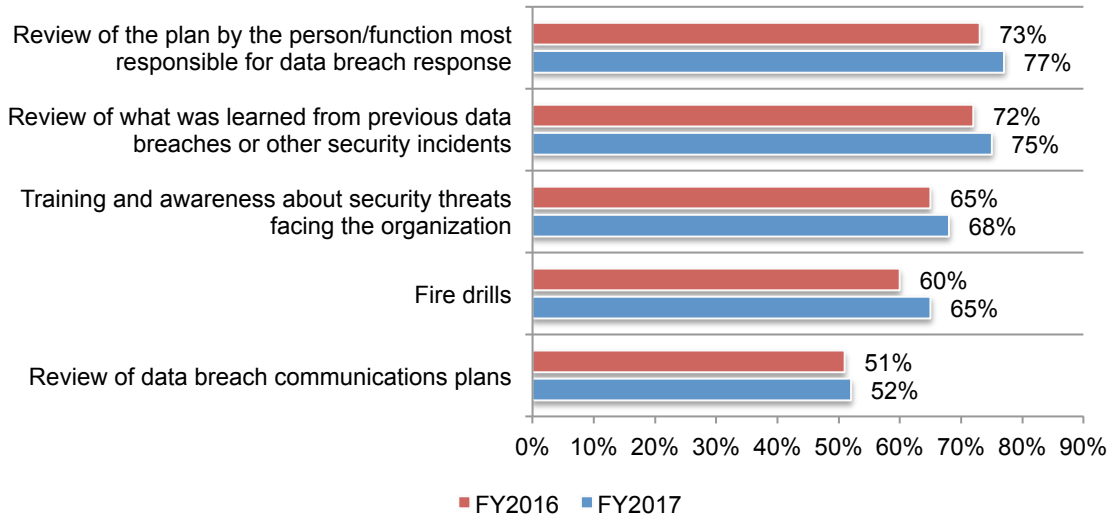
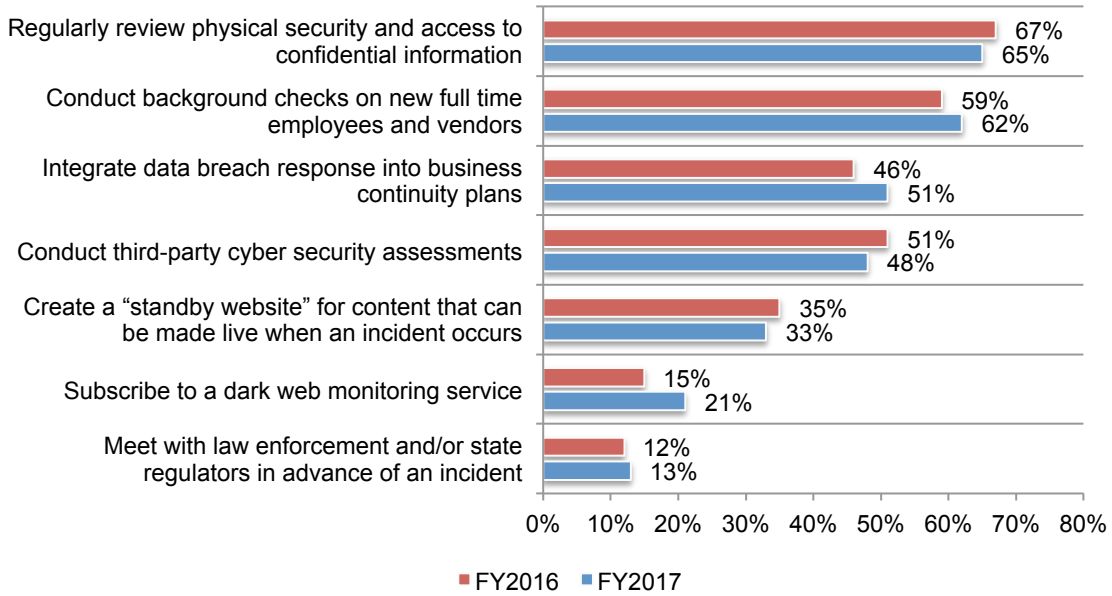


Figure 12 reveals that 65 percent of respondents say their organizations regularly review physical security and access to confidential information and conduct background checks on new full-time employees and vendors (62 percent of respondents). Very few companies are meeting with law enforcement and/or state regulators in advance of an incident (13 percent of respondents).

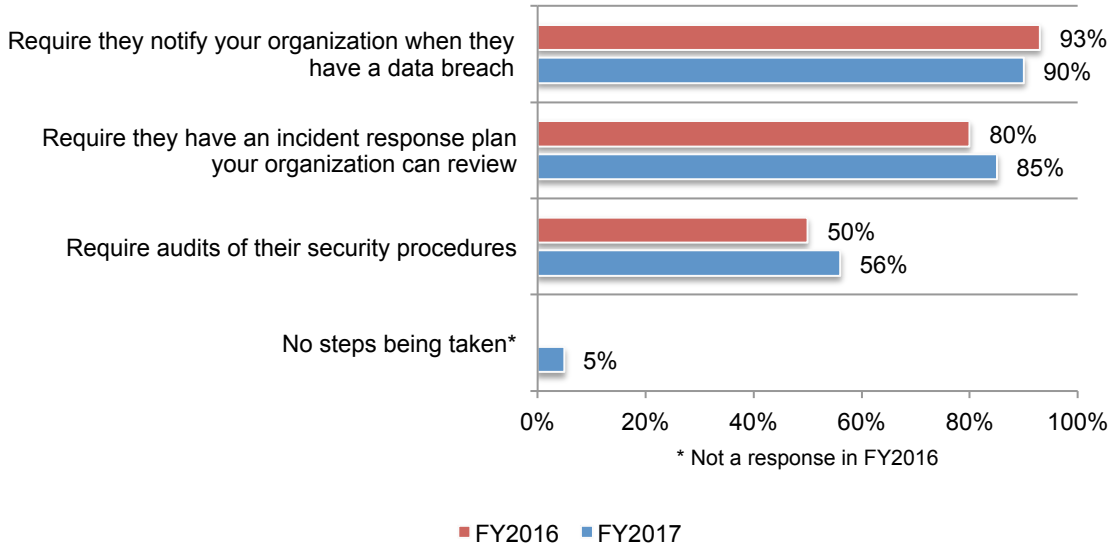
Figure 12. Does your organization take any special steps to prepare for a data breach?
More than one response permitted



Threats that affect data breach preparedness

Most companies depend upon their business partners and third parties to notify them if they experienced a data breach. Ninety-five percent of respondents say their companies take steps to minimize the consequences of a data breach involving a business partner or other third party. These steps are presented in Figure 13**.** To reduce the negative consequences of a third-party data breach, more companies should require audits of their security procedures. Currently, 56 percent of respondents say they have such a requirement.

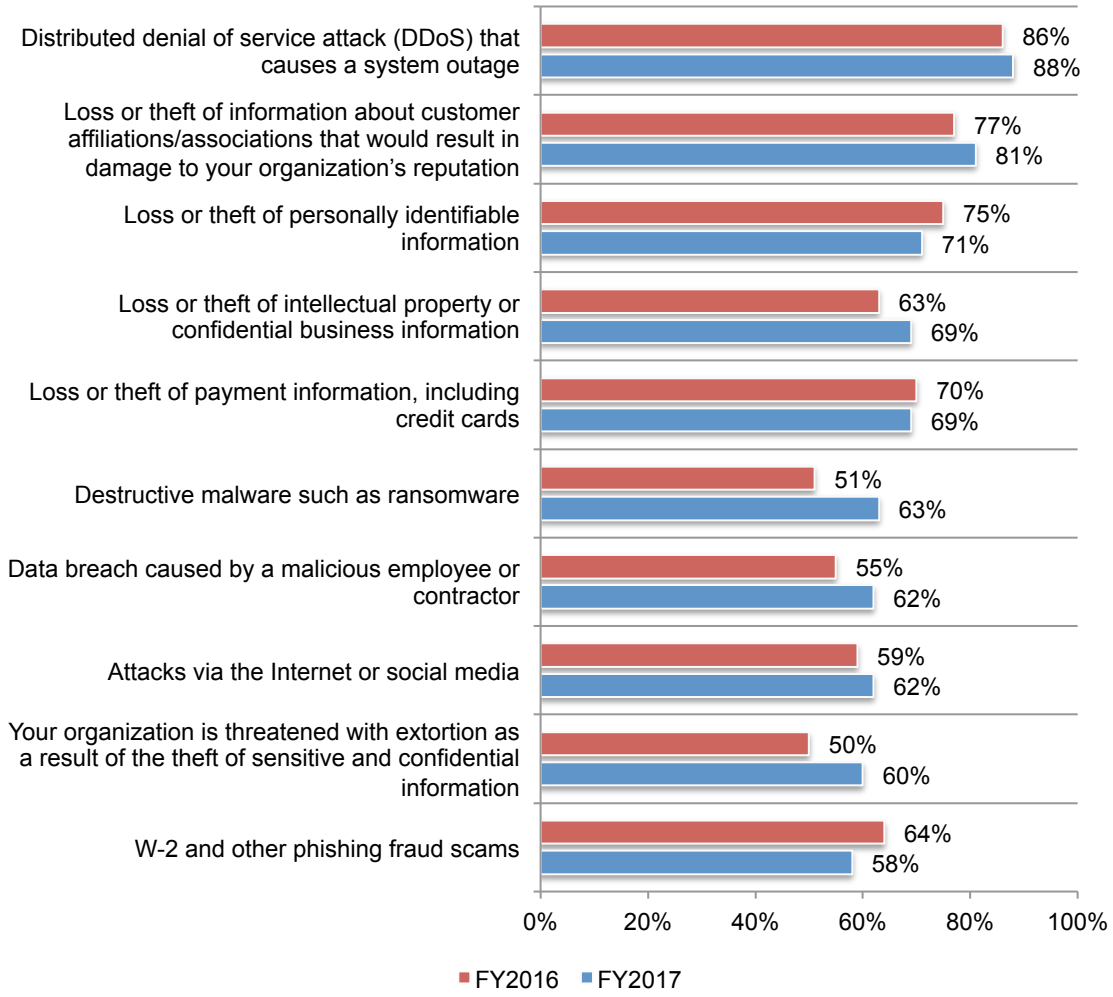
Figure 13. How companies minimize the consequences of a third-party data breach
More than one response permitted



Most companies' response plans provide guidance on how to address a DDoS attack or the loss or theft of intellectual property or confidential business information. As revealed in Figure 13, similar to last year, guidance on how to deal with a DDoS attack that causes a system outage was most often included in a data breach response plan.

Other areas of guidance include managing such incidents as: loss or theft of information about customer affiliations/associations that would affect the organization's reputation (81 percent of respondents) and loss or theft of personally identifiable information (71 percent of respondents).

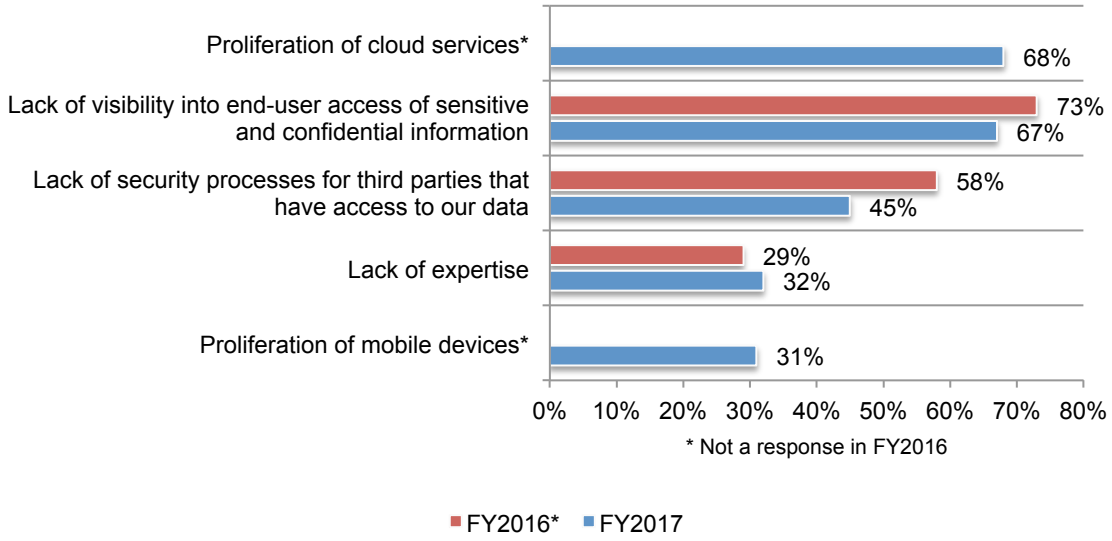
Figure 14. What guidance does the plan provide on dealing with security incidents?
More than one response permitted



Threats that affect data breach preparedness

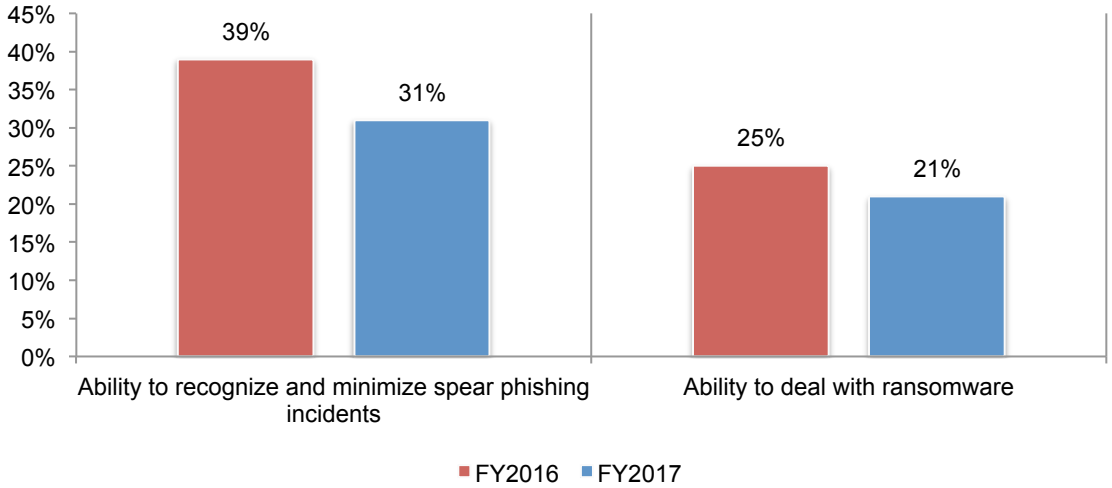
Proliferation of cloud services and lack of visibility are the biggest barriers to improving IT security's ability to respond to a data breach. According to Figure 15, respondents recognize the difficulty in dealing with the proliferation of cloud services and the lack of visibility into end-user access of sensitive and confidential information as serious barriers to responding to a data breach.

Figure 15. What are the biggest barriers to improving the ability of IT security to respond to a data breach?
Two choices permitted



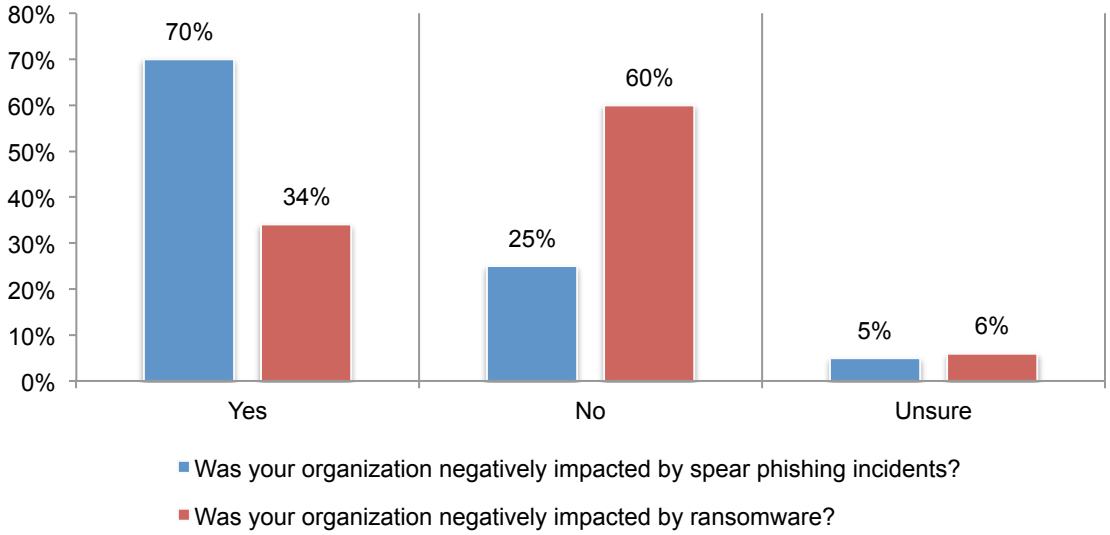
Confidence in the ability to deal with ransomware and spear phishing incidents declines. Last year, 25 percent of respondents said they were confident in their ability to deal with ransomware and this has declined to 21 percent of respondents. Similarly, the ability to recognize and minimize spear phishing incidents declined from 39 percent of respondents who were confident last year to 31 percent of respondents in this year's study.

Figure 16. Confidence in the ability to deal with a ransomware or spear phishing incident
Very confident and Confident responses combined



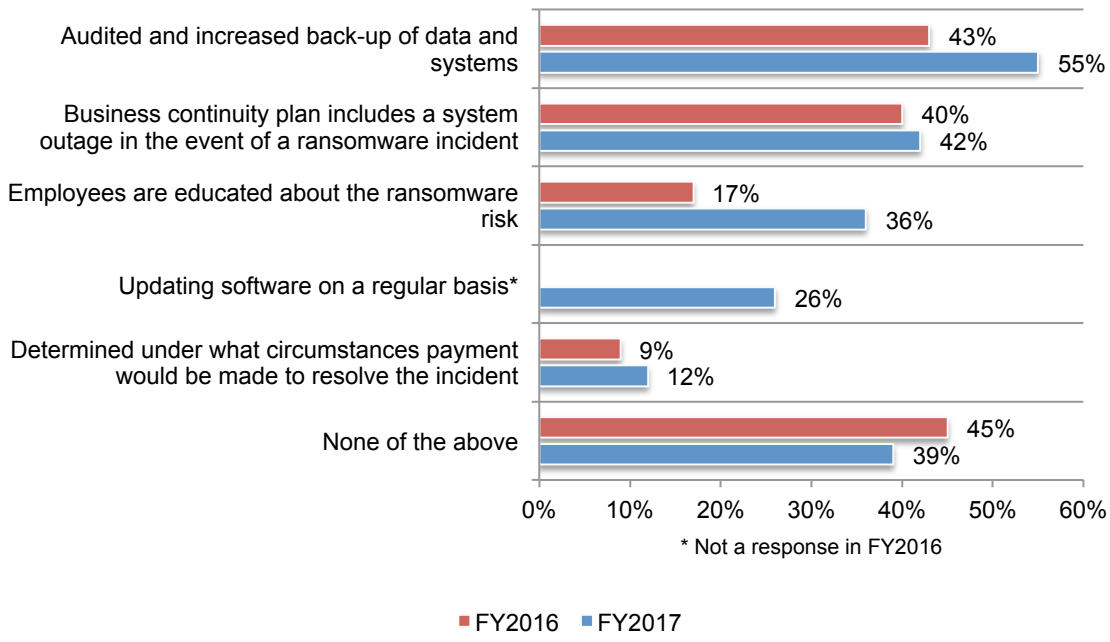
More companies were negatively impacted by spear phishing incidents than ransomware. Seventy percent of respondents say their organizations have been negatively impacted by spear phishing attacks and 34 percent of respondents say they experienced ransomware attacks, as shown in Figure 17.

Figure 17. Was your organization negatively impacted by spear phishing and ransomware?



More companies are taking steps to prepare for a ransomware incident. According to Figure 18, more respondents report they are increasing the back-up of data and systems, and educating employees about the ransomware risk (55 percent and 36 percent of respondents, respectively). Forty-two percent of respondents say they have a business continuity plan in place that addresses a system outage in the event of a ransomware incident.

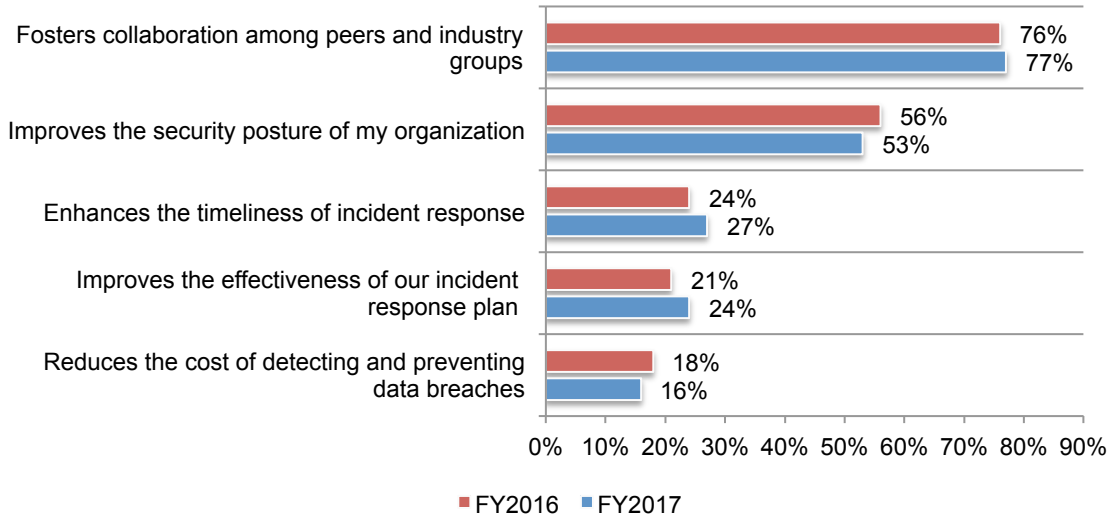
Figure 18. Have you taken the following steps to prepare for a ransomware incident?
More than one choice permitted



Sharing intelligence about data breach experiences and incident response plans can improve the ability to respond to a data breach. Forty-seven 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.

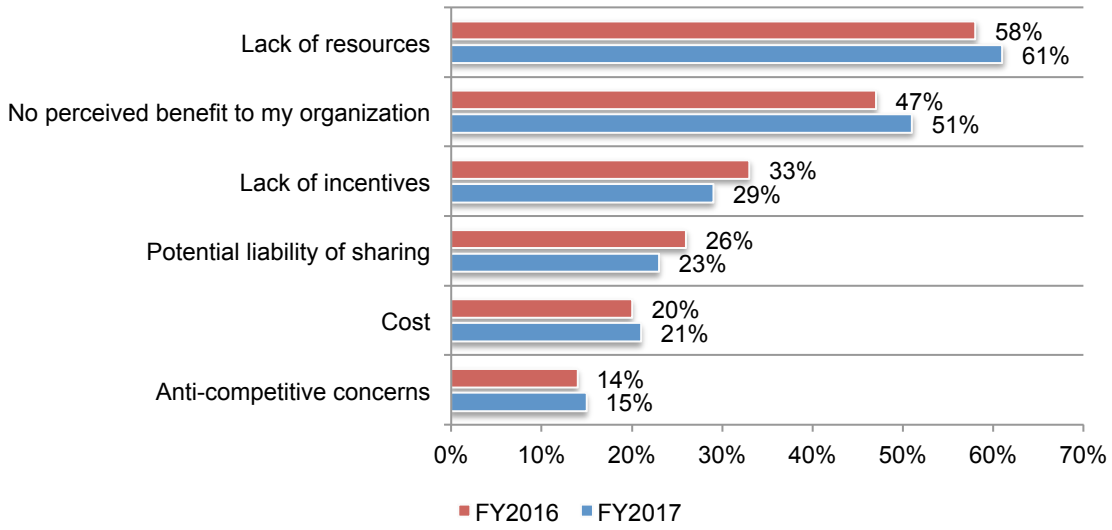
Consistent with last year, as shown in Figure 19, the most important reasons for sharing are the benefits from fostering collaboration among peers and industry groups (77 percent of respondents) and improving the security posture of the organization (53 percent of respondents).

Figure 19. 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 (61 percent of respondents) and no perceived benefit to the organization (51 percent of respondents), according to Figure 20. The potential liability of sharing is not considered a deterrent to sharing by most companies.

Figure 20. Reasons for not sharing information
More than one response permitted



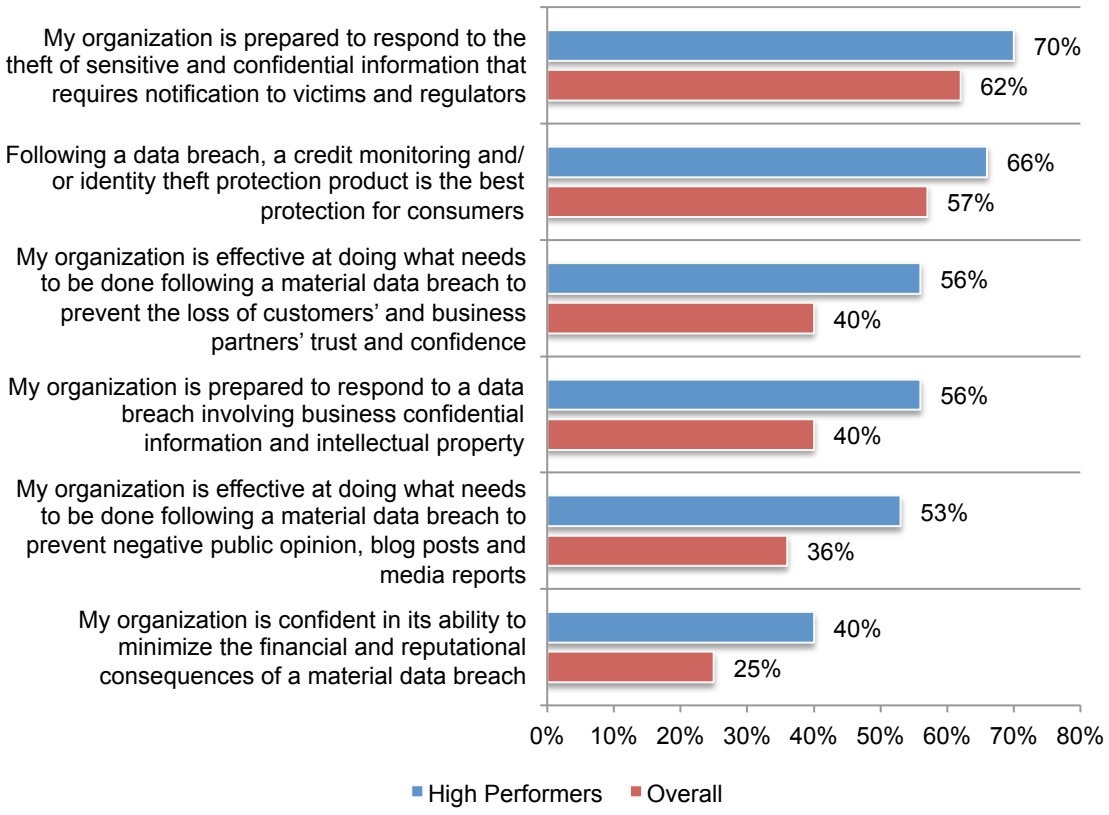
Best practices in data breach preparedness

In this year's study, 19 percent of the total respondents (hereafter referred to as high performers) self-reported that their organizations' data breach response plan is highly effective (9.5 on a scale of 1 = low effectiveness to 10 = very high effectiveness). In this section, we analyze the practices of these high performers.

High performers are more confident in their ability to prevent negative public opinion, minimize the loss of trust and respond to the loss of their intellectual property. According to Figure 21, high performers are far more confident in their ability to minimize the consequences of a data breach.

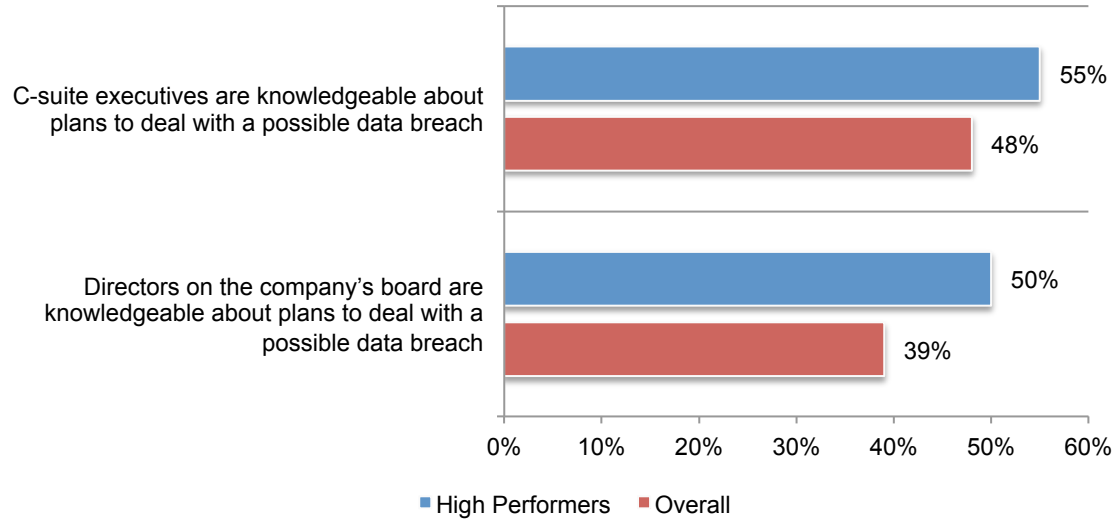
The most significant difference between the two types of respondents are effectiveness in preventing negative public opinion, blog posts and media reports (53 percent vs. 36 percent); responding to a data breach involving business confidential information and intellectual property (56 percent vs. 40 percent); understanding what needs to be done following a material data breach to prevent the loss of customers' and business partners' trust and confidence (56 percent vs. 40 percent) and minimizing the financial and reputational consequences of a material data breach (40 percent vs. 25 percent).

Figure 21. High performers are more confident in their ability to respond to a data breach
Strongly agree and Agree responses



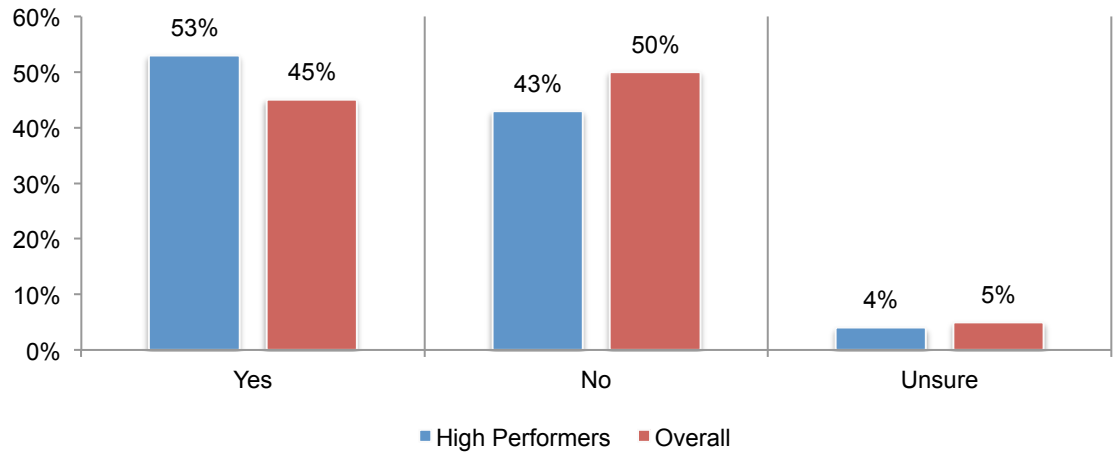
High performing organizations have better governance. The reason for more confidence is that in high performing organizations, the C-suite and boards of directors are more knowledgeable about plans to deal with a possible data breach, as shown in Figure 22.

Figure 22. C-suite executives and boards of directors' knowledge about their organizations' data breach response plans
Yes responses reported



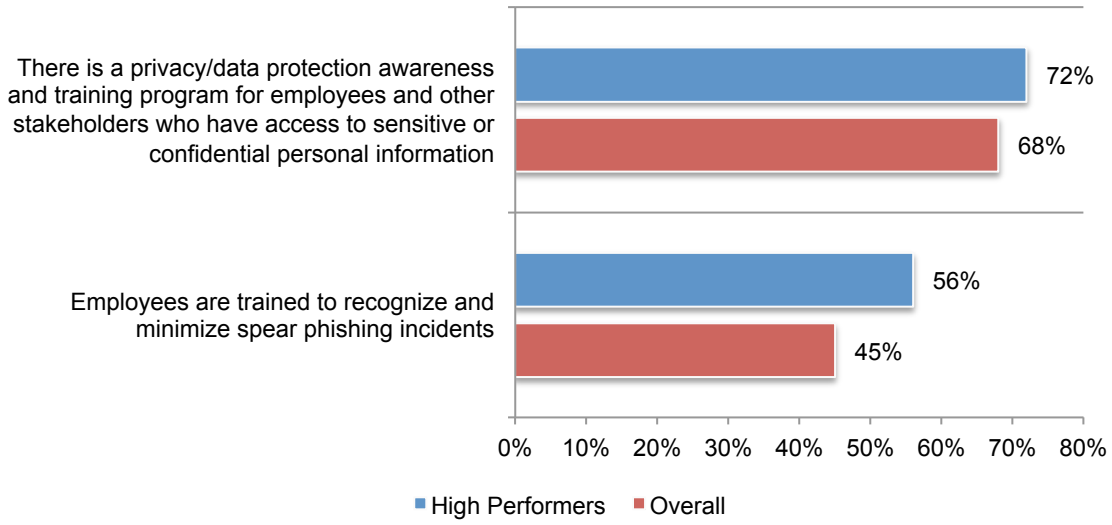
Cyber insurance can help organizations minimize the financial consequences of a data breach. As shown in Figure 23, high performers are more likely to have data breach or cyber insurance policy (53 percent of respondents vs. 45 percent of respondents).

Figure 23. Does your organization have a data breach or cyber insurance policy?



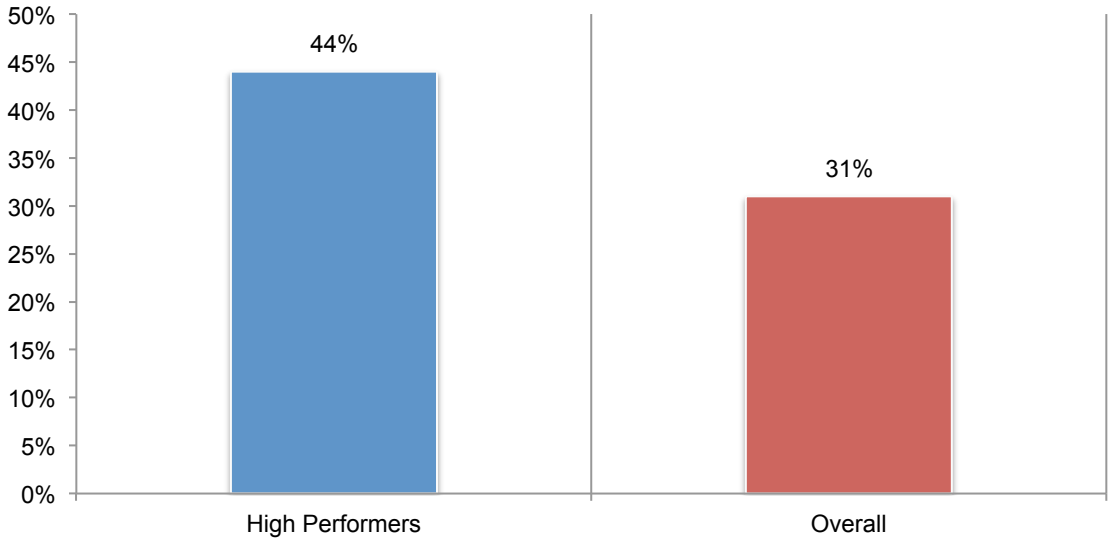
Employee negligence has a significant influence on organizations' overall security posture. Eighty percent of all respondents are concerned about potential data breaches caused by employees' carelessness or lack of awareness about the protection of sensitive data. As shown in Figure 24, most companies have a privacy/data protection awareness and training program for employees and other stakeholders who have access to sensitive or confidential information. However, high performers are more likely to train employees to recognize and minimize spear phishing incidents.

Figure 24. Employee training and awareness programs
Yes responses reported



As a consequence, high performers are more confident in their ability to recognize and minimize spear phishing attacks (44 percent vs. 31 percent), as shown in Figure 25.

Figure 25. How confident is your organization in its ability to recognize and minimize spear phishing incidents?
Very confident and confident responses combined



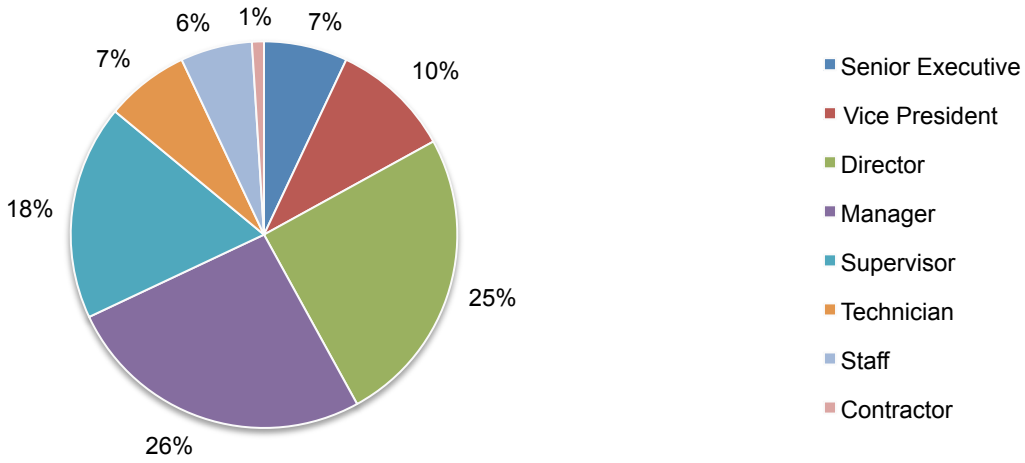
Part 3. Methods

A sampling frame of 15,402 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 679 total returns. Screening and reliability checks required the removal of 55 surveys. Our final sample consisted of 624 surveys or a 4.1 percent response rate.

Table 1. Sample response	Freq	Pct%
Sampling frame	15,402	100.0%
Total returns	679	4.4%
Rejected or screened surveys	55	0.4%
Final sample	624	4.1%

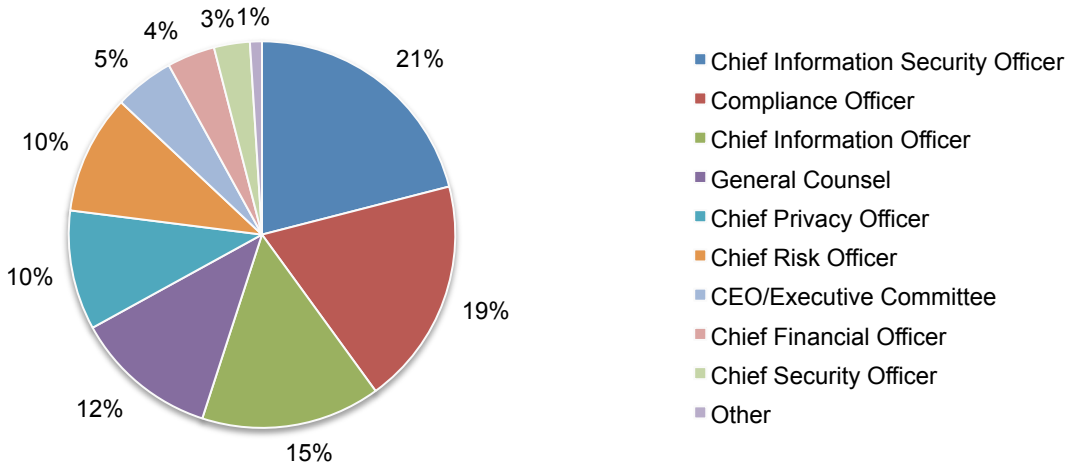
Pie Chart 1 reports the respondent's organizational level within participating organizations. By design, a majority of respondents (86 percent) are at or above the supervisory levels.

Pie Chart 1. Current position within the organization



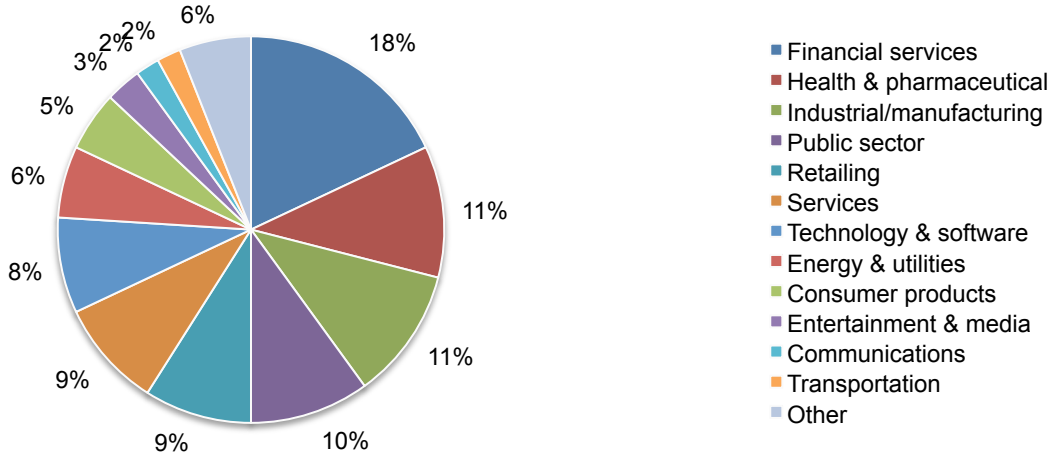
Pie Chart 2 reveals that 21 percent of respondents report to the Chief Information Security Officer, 19 percent report to the Compliance Officer and 15 percent report to the Chief Information Officer.

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



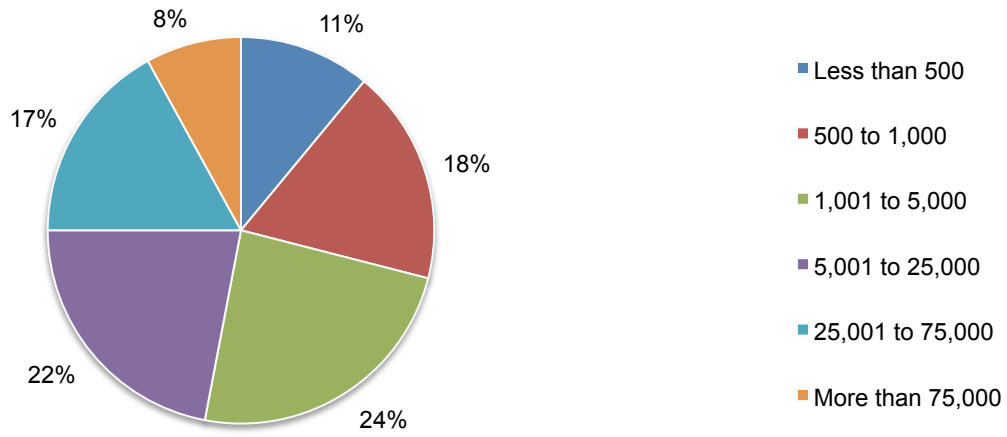
Pie Chart 3 reports the industry classification of respondents' organizations. This chart identifies financial services (18 percent) as the largest segment, followed by health and pharmaceutical (11 percent), industrial/manufacturing (11 percent) and public sector (10 percent).

Pie Chart 3. Primary industry focus



As shown in Pie Chart 5, 71 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 September, 2017.

Survey response	FY2017
Sampling frame	15,402
Total returns	679
Rejected or screened surveys	55
Final sample	624
Response rate	4.1%

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?	FY2017
Yes	56%
No	31%
Unsure	13%
Total	100%

Q1b. If yes, how frequently did these incidents occur during the past 2 years?	FY2017
Only once	30%
2 to 3 times	37%
4 to 5 times	23%
More than 5 times	10%
Total	100%

Q1c. If yes, were any of these breaches international or global in scope?	FY2017
Yes	39%
No	53%
Unsure	8%
Total	100%

Attributions. Please rate each statement using the scale provided below each item. Strongly agree and agree response	FY2017
Q2. My organization is prepared to respond to the theft of sensitive and confidential information that requires notification to victims and regulators.	62%
Q3. My organization is prepared to respond to a data breach involving business confidential information and intellectual property.	40%
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.	40%
Q5. My organization is effective at doing what needs to be done following a material data breach to prevent negative public opinion, blog posts and media reports.	36%
Q6. My organization's incident response plan includes breaches involving IoT devices.	29%
Q7. My organization is confident in its ability to minimize the financial and reputational consequences of a material data breach.	25%
Q8. Following a data breach, a credit monitoring and/or identity theft protection product is the best protection for consumers.	57%

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?	FY2017
Yes	71%
No	29%
Total	100%

Q9b. If yes, how long should identity theft protection be provided?	FY2017
2 to 3 years	49%
4 to 7 years	30%
8 to 10 years	16%
More than 10 years	5%
Total	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?	FY2017
Free identity theft protection and credit monitoring services	72%
A sincere and personal apology (not a generic notification)	33%
Discounts on products or services	43%
Gift cards	42%
Access to a call center to respond to their concerns and provide information	37%
None of the above would make a difference	25%
Total	252%

Q11. Which of the following issues would have the greatest impact on your organization's reputation? Please select one choice.	FY2017
Poor customer service	28%
Labor or union dispute	3%
Environmental incident	8%
Data breach	25%
Regulatory fines	4%
Publicized lawsuits	10%
Product recall	20%
CEO's salary	2%
Total	100%

Part 2. Data breach preparedness

Q12a. Do you believe your company's C-suite executives are knowledgeable about plans to deal with a possible data breach?	FY2017
Yes	48%
No	41%
Unsure	11%
Total	100%

Q12b. If yes, why do you believe your company's C-suite executives are knowledgeable? Please select all that apply.	FY2017
They regularly participate in detailed reviews of our data breach response plan	19%
They understand the specific security threats facing our organization	36%
They provide detailed feedback about the data breach response plan	25%
They assume responsibility for the successful execution of the incident response plan	25%
They have requested to be notified ASAP if a material data breach occurs	45%
They participate in a high level review of the organization's data protection and privacy practices	15%
Total	165%

Q13a. Do you believe directors on your company's board are knowledgeable about plans to deal with a possible data breach?	FY2017
Yes	39%
No	61%
Total	100%

Q13b. If yes, why do you believe board members are knowledgeable? Please select all that apply.	FY2017
They regularly participate in detailed reviews of our data breach response plan	11%
They understand the specific security threats facing our organization	40%
They provide detailed feedback about the data breach response plan	21%
They assume responsibility for the successful execution of the incident response plan	15%
They have requested to be notified ASAP if a material data breach occurs	56%
They participate in a high level review of the organization's data protection and privacy practices	9%
Total	152%

Q14. What types of data loss is your organization most concerned about? Please select the top two.	FY2017
Loss or theft of customer information	63%
Loss or theft of employee personal data	40%
Loss or theft of medical data	11%
Loss or theft of consumer data	20%
Loss or theft of intellectual property	54%
Loss or theft of consumer payment card data	12%
Total	200%

Q15. What are the three biggest barriers to improving the ability of IT security to respond to a data breach? Please select the top three	FY2017
Lack of investment in much needed technologies	17%
Lack of expertise	32%
Lack of C-suite support	11%
Lack of security processes for third parties that have access to our data	45%
Lack of visibility into end-user access of sensitive and confidential information	67%
Lack of understanding of unsecured IoT devices	29%
Proliferation of mobile devices	31%
Proliferation of cloud services	68%
None of the above	0%
Total	300%

Q16. 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?	FY2017
Yes	63%
No	34%
Unsure	3%
Total	100%

Q17. How confident is your organization in its ability to deal with ransomware?	FY2017
Very confident	10%
Confident	11%
Somewhat confident	18%
Not confident	36%
No confidence	25%
Total	100%

Q18. Does your organization train employees to recognize and minimize spear phishing incidents?	FY2017
Yes	45%
No	55%
Total	100%

Q19. How confident is your organization in its ability to recognize and minimize spear phishing incidents?	FY2017
Very confident	15%
Confident	16%
Somewhat confident	25%
Not confident	26%
No confidence	18%
Total	100%

Q20a. Was your organization negatively impacted by spear phishing incidents?	FY2017
Yes	70%
No	25%
Unsure	5%
Total	100%

20b. Was your organization negatively impacted by ransomware?	FY2017
Yes	34%
No	60%
Unsure	6%
Total	100%

Q21. Have you taken the following steps to prepare for a ransomware incident? Please select all that apply.	FY2017
Determined under what circumstances payment would be made to resolve the incident	12%
Audited and increased back up of data and systems	55%
Business continuity plan includes a system outage in the event of a ransomware incident	42%
Employees are educated about the ransomware risk	36%
Updating software on a regular basis	26%
None of the above	39%
Other	4%
Total	214%

Q22a. 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?	FY2017
Yes	68%
No	32%
Unsure	0%
Total	100%

Q22b. If yes, how often is training conducted?	FY2017
As part of employee orientation	45%
Every six months	3%
Annually	27%
Sporadically	24%
Unsure	1%
Total	100%

Q22c. Are the awareness and training programs regularly reviewed and updated to ensure the content addresses the areas of greatest risk to the organization?	FY2017
Yes	54%
No	42%
Unsure	4%
Total	100%

Q23. How significant is the influence of employee negligence on your organization's overall security posture?	FY2017
Very significant	39%
Significant	41%
Not significant	14%
Minimal	6%
Total	100%

Q24a. Does your organization have a data breach or cyber insurance policy?	FY2017
Yes	45%
No	50%
Unsure	5%
Total	100%

Q24b. If no, does your organization plan to purchase a data breach or cyber insurance policy?	FY2017
Yes, within the next six months	21%
Yes, within the next year	24%
Yes, within the next two years	11%
No plans to purchase	40%
Unsure	4%
Total	100%

Q25. What types of incidents does your organization's cyber insurance cover? Please select all that apply.	FY2017
External attacks by cyber criminals	80%
Malicious or criminal insiders	63%
System or business process failures	35%
Human error, mistakes and negligence	36%
Incidents affecting business partners, vendors or other third parties that have access to your company's information assets	60%
Ransomware attacks	54%
Major security vulnerability in a product, website or service	44%
Other	9%
Unsure	7%
Total	388%

Q26. What coverage does this insurance offer your company? Please select all that apply.	FY2017
Identity protection services to victims	64%
Call center support	59%
Forensics and investigative costs	63%
Notification costs to data breach victims	69%
Communication costs to regulators	13%
Employee productivity losses	8%
Replacement of lost or damaged equipment	49%
Revenue losses	23%
Legal defense costs	70%
Regulatory penalties and fines	39%
Third-party liability	61%
Brand damages	5%
IoT enabled device protection	9%
Other	7%
Unsure	5%
Total	544%

Q27. 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.	FY2017
Require they have an incident response plan your organization can review	85%
Require they notify your organization when they have a data breach	90%
Require audits of their security procedures	56%
No steps being taken	5%
Total	236%

Q28a. Does your organization participate in an initiative or program for sharing information with government and industry peers about data breaches and incident response?	FY2017
Yes, currently participating	26%
Yes, planning to participate	21%
No, does not participate	53%
Unsure	0%
Total	100%

Q28b. If your organization shares information about its data breach experience and incident response plans, what are the main reasons? Please select only two top choices.	FY2017
Improves the security posture of my organization	53%
Improves the effectiveness of our incident response plan	24%
Enhances the timeliness of incident response	27%
Reduces the cost of detecting and preventing data breaches	16%
Fosters collaboration among peers and industry groups	77%
Other	3%
Total	200%

Q28c. If no, why does your organization not participate in a threat-sharing program? Please select only two top choices.	FY2017
Cost	21%
Potential liability of sharing	23%
Anti-competitive concerns	15%
Lack of resources	61%
Lack of incentives	29%
No perceived benefit to my organization	51%
Other	0%
Total	200%

Part 3. Data breach response plan

Q29a. Does your organization have a data breach response plan in place?	FY2017
Yes	88%
No	12%
Don't know	
Total	100%

Q29b. If no, why?	FY2017
No resources or budget	38%
Not important to have data breach response plan in place	13%
Lack of C-level support	20%
Outsourced to consultants	29%
Other	0%
Total	100%

Q30. How often does your company update the data breach response plan?	FY2017
Each quarter	2%
Twice per year	5%
Once each year	27%
No set time period for reviewing and updating the plan	40%
We have not reviewed or updated since the plan was put in place	26%
Total	100%

Q31. In addition to documenting and practicing your data breach plan, does your organization take any of the following additional steps to prepare?	FY2017
Conduct third-party cyber security assessments	48%
Integrate data breach response into business continuity plans	51%
Create a “standby website” for content that can be made live when an incident occurs	33%
Regularly review physical security and access to confidential information	65%
Meet with law enforcement and/or state regulators in advance of an incident	13%
Subscribe to a dark web monitoring service	21%
Conduct background checks on new full time employees and vendors	62%
Total	293%

Q32. Does your data breach response plan include the following requirements? Please select all that apply.	FY2017
Required C-level approval of the data breach response plan	75%
Contact information for all members of the data breach response team	94%
Contact information for all members of the data breach backup response team	40%
Procedures for communicating with employees when a data breach occurs	55%
Procedures for responding to a data breach involving overseas locations	41%
Procedures for communicating with state attorneys general and regulators	69%
Procedures for communications with investors	50%
Procedures for communications with business partners and other third parties	46%
Review of a third party or business partner’s incident response plan	32%
Procedures for determining and offering identity theft protection services	39%
Procedures for reporting results of the forensics investigation to senior management	28%
Procedures for incorporating findings from the forensics investigations into the security strategy	28%
None of the above	4%
Total	601%

Q33. Does your data breach response plan offer guidance on managing the following security incidents? Please check all that apply.	FY2017
Loss or theft of payment information, including credit cards	69%
Loss or theft of personally identifiable information	71%
Destructive malware such as ransomware	63%
IoT-based attacks	14%
Hacktivism/activism	40%
Attacks via the Internet or social media	62%
W-2 and other phishing fraud scams	58%
Distributed denial of service attack (DDoS) that causes a system outage	88%
Loss or theft of information about customer affiliations/associations that would result in damage to your organization's reputation	81%
Loss or theft of intellectual property or confidential business information	69%
Data breach caused by a malicious employee or contractor	62%
Your organization is threatened with extortion as a result of the theft of sensitive and confidential information	60%
Loss or theft of paper documents and tapes containing sensitive and confidential information	36%
None of the above	5%
Total	778%

Q34. Using the following 10-point scale, please rate your organization's preparedness for dealing with IoT-based attacks. 1 = not prepared to 10 = fully prepared.	FY2017
1 to 2	38%
3 to 4	30%
5 to 6	15%
7 to 8	10%
9 to 10	7%
Total	100%
Extrapolated value	3.86

Q35. Using the following 10-point scale, please rate the effectiveness of your organization's data breach response plan. 1 = very low effectiveness to 10 = very high effectiveness.	FY2017
1 to 2	10%
3 to 4	15%
5 to 6	26%
7 to 8	30%
9 to 10	19%
Total	100%
Extrapolated value	6.16

Q36. How could your data breach response plan become more effective? Please select the top three choices.	FY2017
Conduct more fire drills to practice data breach response	85%
Have formal documentation of incident response procedures	62%
Incorporate what was learned from previous data breaches	66%
Ensure seamless coordination among all departments involved in incident response	40%
Increase participation and oversight from senior executives	80%
Assign individuals with a high level of expertise in security to the team	75%
Assign individuals with a high level of expertise in compliance with privacy, data protection laws and regulations to the team	48%
Have a budget dedicated to data breach preparedness	60%
Increase involvement of third-party experts	44%
None of the above	2%
Total	562%

Q37a. Does your organization practice responding to a data breach?	FY2017
Yes	71%
No	29%
Total	100%

Q37b. If yes, how often is the response practiced? Please check all that apply.	FY2017
At least twice a year	44%
Once each year	19%
Every two years	4%
More than two years	9%
Never	0%
No set schedule	24%
Total	100%

Q37c. If yes, what is included in the practice response? Please check all that apply.	FY2017
Fire drills	65%
Case discussions	46%
Training and awareness about security threats facing the organization	68%
Review of the plan by the person/function most responsible for data breach response	77%
Review of data breach communications plans	52%
Review of what was learned from previous data breaches or other security incidents	75%
None of the above	11%
Other	4%
Total	398%

Q37d. If no, why? Please check all that apply.	FY2017
Not enough budget	37%
We are confident in our ability to respond to a data breach	45%
Too difficult to schedule a practice response	73%
Not a priority	61%
Total	216%

Q38a. Does your incident response plan include processes to manage an international data breach?	FY2017
Yes	54%
No	41%
Unsure	5%
Total	100%

Q38b. If yes, is your organization's plan specific to each location where it operates?	FY2017
Yes	50%
No	46%
Unsure	4%
Total	100%

Q39. How confident is your organization in its ability to deal with an international data breach?	FY2017
Very confident	11%
Confident	17%
Somewhat confident	26%
Not confident	34%
No confidence	12%
Total	100%

Part 4. Organizational characteristics & respondent demographics

D1. What organizational level best describes your current position?	FY2017
Senior Executive	7%
Vice President	10%
Director	25%
Manager	26%
Supervisor	18%
Technician	7%
Staff	6%
Contractor	1%
Other	0%
Total	100%

D2. Check the **Primary Person** you report to within your organization.	FY2017
CEO/Executive Committee	5%
Chief Financial Officer	4%
General Counsel	12%
Chief Privacy Officer	10%
Chief Information Officer	15%
Compliance Officer	19%
Human Resources VP	0%
Chief Security Officer	3%
Chief Risk Officer	10%
Chief Information Security Officer	21%
Other	1%
Total	100%

D3. What industry best describes your organization's industry focus?	FY2017
Agriculture & food service	1%
Communications	2%
Consumer products	5%
Defense & aerospace	0%
Education & research	1%
Energy & utilities	6%
Entertainment & media	3%
Financial services	18%
Health & pharmaceutical	11%
Hospitality	1%
Industrial/manufacturing	11%
Public sector	10%
Retailing	9%
Services	9%
Technology & software	8%
Transportation	2%
Other	3%
Total	100%

D4. What is the worldwide headcount of your organization?	FY2017
Less than 500	11%
500 to 1,000	18%
1,001 to 5,000	24%
5,001 to 25,000	22%
25,001 to 75,000	17%
More than 75,000	8%
Total	100%

Please contact research@ponemon.org or call us at 800.887.3118 if you have any questions.

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.