Ponemon INSTITUTE

Sixth 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 2019

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

Ponemon Institute, February 2019

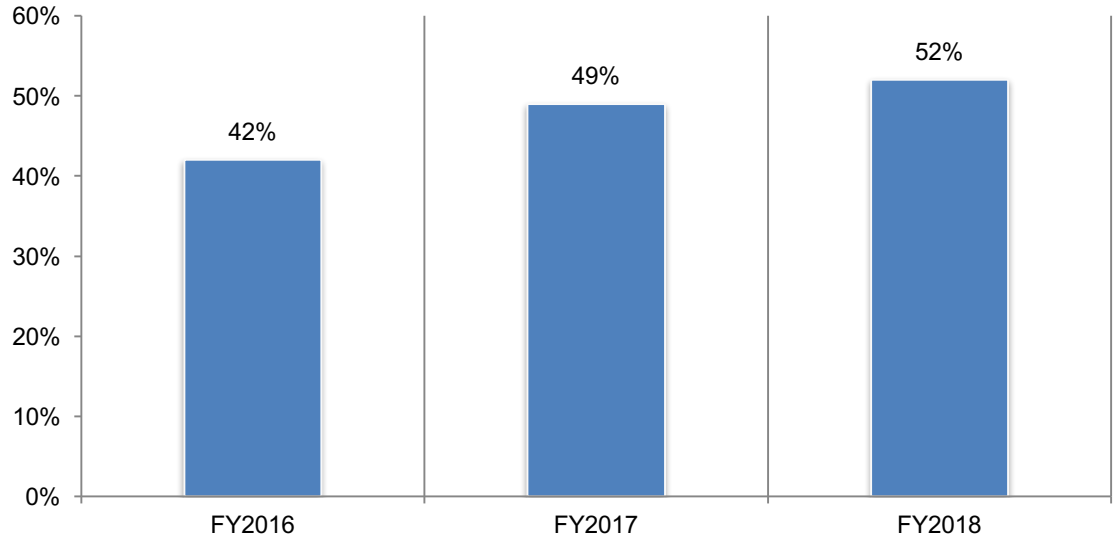
Part 1. Introduction

The types of threats facing organizations are constantly evolving, challenging the ability of organizations to be adequately prepared to respond to a data breach. The *Sixth 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. In this study, we surveyed 643 professionals in IT and IT security, compliance and privacy, who are involved in data breach response plans in their organizations.

Companies are slowly improving the effectiveness of their data breach response plans but only slightly more than half believe their data breach response plans are very effective. Respondents were asked to rank their organization's data breach plan on a scale of 1 = very low effectiveness to 10 = very high effectiveness. Figure 1 presents the very high effectiveness responses (7+ on the 10-point scale). Since 2016, more companies represented in this research have self-reported their data breach response plans are very effective from 42 percent in 2016 to 52 percent of respondents in 2018.

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

1 = very low effectiveness to 10 = very high effectiveness, 7+ responses presented



Employee training programs are critical to combat data breaches. Eighty-four percent of respondents say employee negligence has a significant impact on their organizations' security posture. As a result, training programs that focus on privacy and data protection awareness training should be an important part of data breach preparedness. The findings also show concerns about spear phishing incidents. However, only 47 percent of respondents say their organizations are training employees to recognize and minimize spear phishing incidents.

Following are insights from this year's study.

Data breaches are increasing and the financial consequences are becoming more severe. Each year more companies represented in this research study have a data breach. In this year's study, 59 percent of respondents report their organization had a breach, an increase from 56 percent last year. Seventy-three percent of respondents say their organizations had multiple breaches. In addition to the growth in the frequency of data breaches, they are also becoming more expensive. In 2018, a Ponemon Institute study found that the average consolidated cost of a data breach is $3.86 million.[1] An increase from $3.62 million in 2017.

Organizations believe data breaches can damage their reputation. Respondents were asked what events or issues would have an impact on their reputation. Twenty-nine percent say poor customer service negatively affects reputation followed by 27 percent who say a data breach would affect reputation.

Global data breaches are rising significantly. Forty-three percent of respondents say their companies' data breaches were global, an increase from 39 percent of respondents in last year's study. However, only 29 percent of respondents say their organizations are very confident or confident in their ability to deal with an international data breach.

The EU General Data Protection Regulation is influencing organizations to include guidance on responding to an international data breach in their incident response plans. GDPR went into effect May 25, 2018. In the past year 59 percent of respondents say their organizations' GDPR now includes processes to manage an international data breach, an increase from 51 percent of respondents in 2016.

GDPR data breach notification rules are difficult to comply with. Only 36 percent of respondents say their organization has a high ability to comply with data breach notification rules and only 23 percent of respondents say their organizations are effective in achieving compliance.

The ability to determine quickly if the breach resulted in a "risk for the rights and freedoms of natural persons" is an indication compliance with notification rules is very effective. Of the 23 percent of respondents who rate their organizations as highly effective, 45 percent say they are confident in their effectiveness because they would be able to determine quickly if the breach resulted in a risk to natural persons.

Senior leadership's participation in data breach response plans is mostly reactive. C-suite and boards of director primarily want to know if a material data breach has occurred. They are also in the dark about the specific security threats facing their organizations. Only 37 percent of respondents say the senior leadership and 35 percent of respondents say the board understands the specific security threats facing their organization. Only 22 percent of respondents say the C-suite and 10 percent of respondents say the board regularly participates in detailed reviews of our data breach response plan.

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 the findings, most organizations believe an increase in participation and oversight from senior executives, more fire drills to practice data breach response and assign individuals with a high level of expertise in security to the team will help them have a more effective response plan.

More organizations are integrating data breach response into business continuity plans. Seventy percent of respondents say their organizations regularly review physical security and access to confidential information and conduct background checks on new full-time employees

[1] 2018 Ponemon Institute Cost of Data Breach Study, conducted by Ponemon Institute and sponsored by IBM Security, June 2018.

and vendors (65 percent of respondents). The integration of data breach response into business continuity plans has increased from 46 percent of respondents in 2016 to 52 percent of respondents in 2018.

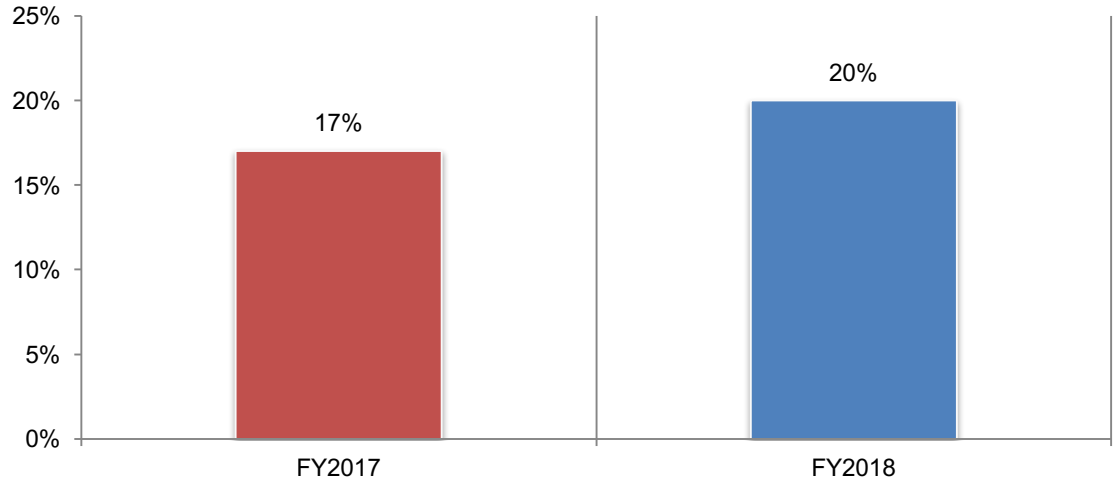
More companies are requiring audits of third party security procedures. To reduce the negative consequences of a third-party data breach, more companies are requiring audits of their security procedures. Currently, 60 percent of respondents say they have such a requirement. Since 2016, the requirement that third parties have an incident response plan for their organizations to review has increased from 80 percent of respondents to 89 percent of respondents.

Almost every company in the study has no confidence in being able to deal with ransomware and spear phishing attacks. Despite efforts to educate employees about the threat of ransomware and spear phishing, only 21 percent of respondents are very confident in their ability to deal with ransomware and only 25 percent of respondents are confident about their ability to minimize spear phishing incidents.

Sharing intelligence about data breach experiences and incident response plans can improve the ability to respond to a data breach. Fifty-one percent of respondents say their organization participates or is planning to participate in an initiative or program for sharing information with government and industry peers about data breaches and incident response**.** The most important reason for sharing is the benefits from fostering collaboration among peers and industry groups (81 percent of respondents). Enhancing the timeliness of incident response has increased since 2016.

The proliferation of IoT devices is exacerbating the risk of a breach and companies seem to be ill-prepared to deal with the consequences. Today, only 35 percent of respondents say their organizations have incident response plans that provide guidance on how to manage data breaches caused by unsecured IoT devices. As a result, when asked to indicate how prepared their organizations are to respond effectively to an IoT attack on a scale of 1 = not prepared to 10 = fully prepared, only 20 percent of respondents say they are fully prepared (7+ responses on the 10-point scale), as shown in Figure 2. This is only a slight increase from last year.

Figure 2. How prepared is your organization to deal with an IoT attack?
1 = not prepared to 10 = fully prepared, 7+ responses presented



Lessons learned from companies that have prevented a data breach.

Data breach response plans that are considered effective can help companies prevent a data breach. For the first time, we did a special analysis of those companies in the research that did not have a data breach in the past two years. A key takeaway is that these companies believe they have incident response plans that are highly effective, giving them the confidence to be able to respond to threats and security exploits.

In this year's study, Ponemon Institute surveyed 643 executives and staff employees who work primarily in privacy, compliance and IT security in the United States. Of these, 186 or 29 percent of the total respondents self-reported that their organizations were able to prevent a data breach involving the loss or theft of more than 1,000 records in the past two years. According to these respondents, their organizations are more likely to adopt the following practices:

Companies that did not have a breach are more likely to rate their data breach plan as highly effective. Sixty-two percent of respondents in companies that did not have a breach say these plans are very effective. In contrast, only 45 percent of respondents in companies that had a data breach rate their plans as highly effective.

Boards of directors and C-suite executives knowledgeable and engaged in incident response plans can reduce the likelihood of a data breach. Fifty-four percent of respondents in organizations that did not have a breach vs. 49 percent in organizations that had a data breach say their C-suite executives are informed about how their privacy and IT security functions plan to deal with a data breach. While it is still a low percentage of respondents, they are more likely to have a knowledgeable board (39 percent vs. 32 percent of respondents).

Investments in technologies that improve detection of and response to a data breach seem to pay off. Seventy-three percent of respondents say their organizations increased their investment in technologies specifically to better detect and respond quickly to a data breach. Sixty-one percent of respondents in companies that had a data breach increased their investments.

Privacy and data protection awareness and training programs have a positive impact on reducing the likelihood of a data breach. Privacy and data protection awareness programs that specifically target employees and other stakeholders who have access to sensitive or confidential personal information are shown to reduce the likelihood of a data breach. Seventy-nine percent of respondents whose organizations did not have a data breach say they provide such training vs. 69 percent of respondent in the data breach group.

Participating in programs to share information about data breaches and incident response supports an organization's ability to avoid a data breach. Learning from industry peers and government agencies about how to better prepare and respond to a data breach can strengthen an organization's security posture and the ability to avoid a data breach. Companies that did not have a data breach are far more likely to participate or plan to participate in such an initiative (59 percent vs. 46 percent of respondents).

Companies that did not have a data breach are more likely to take steps to prepare for a data breach. More companies that managed to prevent a data breach regularly review physical security and access to confidential information, conduct third-party cybersecurity assessments, integrate data breach response into business continuity plans and create a "standby website" for content that can be made live when an incident occurs.

Part 2. Key findings

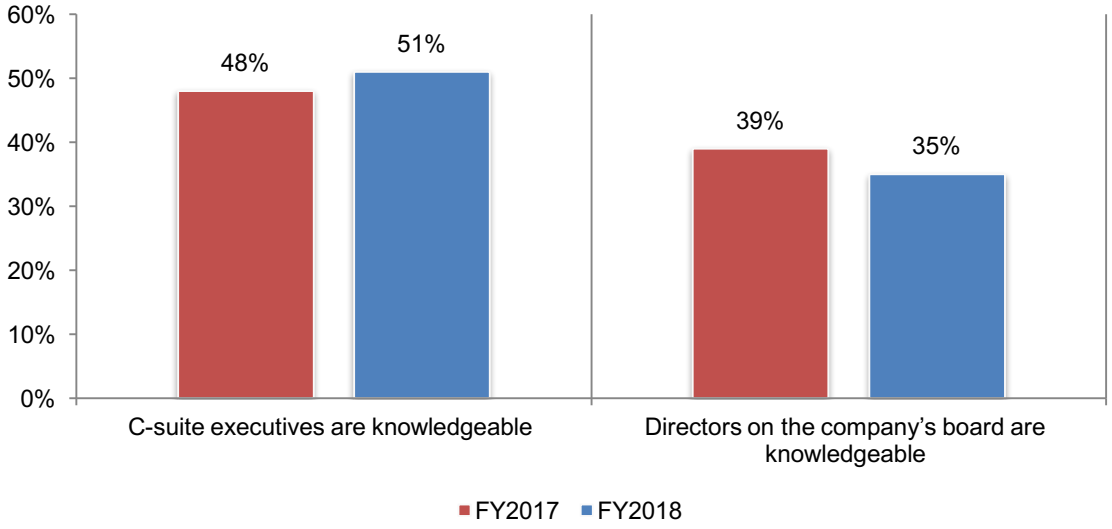
In this section, we provide an analysis of the key findings. The complete audited findings are presented in the Appendix of this report. When available, we compare the findings from previous studies to this year's findings. We have organized the report according to the following topics:

- The importance of good governance in data breach preparedness
- International data breaches are increasing and organizations are not prepared
- Threats that affect data breach preparedness
- Lessons learned from organizations that did not have a data breach

The importance of good governance in data breach preparedness

More C-suite executives are knowledgeable about their organizations' efforts to respond to a data breach, but board of directors' involvement in incident response declines. While more than half of respondents (51 percent) say C-suite executives are informed and knowledgeable about how their companies plan to respond to a data breach, fewer respondents say their board of directors are engaged in their data breach response plans (35 percent).

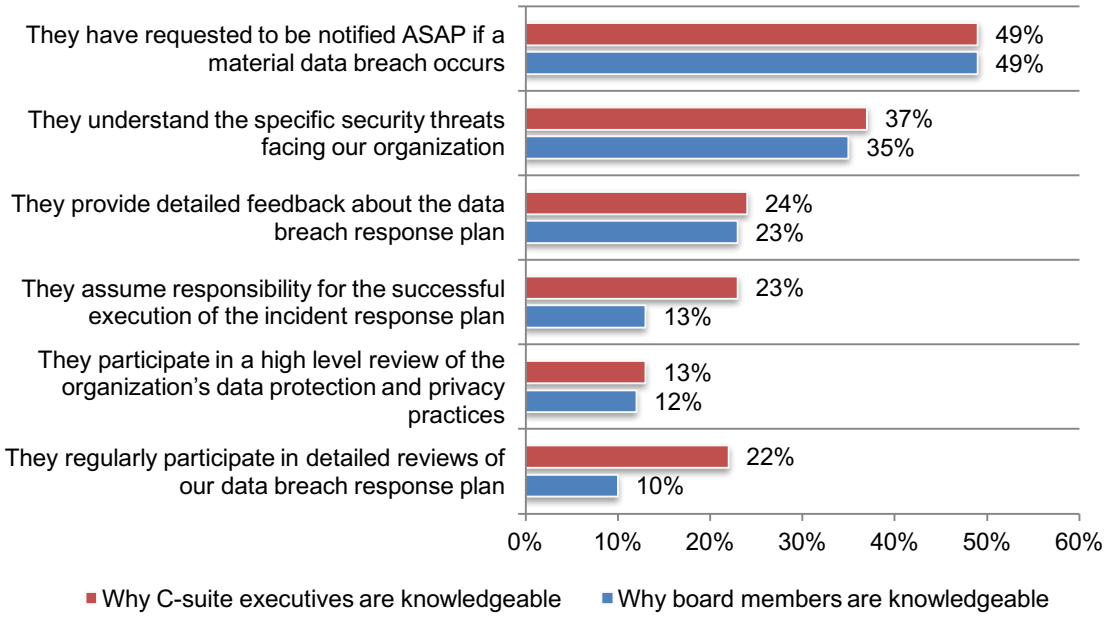
Figure 3. Are C-suite executives and boards of directors knowledgeable about plans to deal with a possible data breach?
Yes responses presented



Senior leadership's participation in data breach response plans is mostly reactive. As discussed, 51 percent of respondents say their C-suite executives are knowledgeable about incident response plans. However, as shown in Figure 4, the primary indication of knowledge is that the C-suite wants to know ASAP if a material data breach has occurred. This is also the case with the 35 percent of respondents with a knowledgeable board who say the board of directors would want to be notified about such an incident.

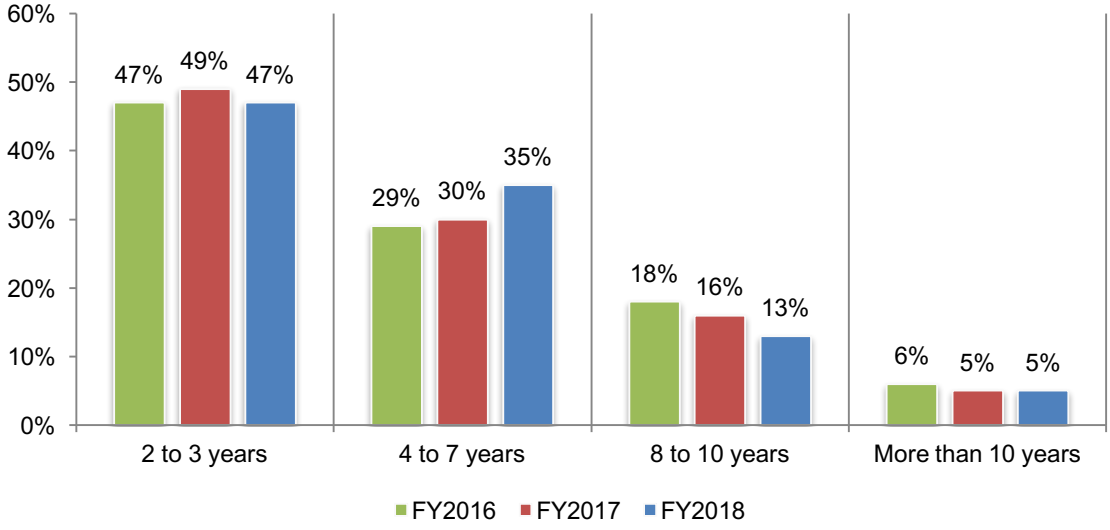
In addition, the C-suite and board are in the dark about the specific security threats facing their organizations. Only 37 percent of respondents say the senior leadership and 35 percent of respondents say the board understands the specific security threats facing their organization. Only 22 percent of respondents say the C-suite and 10 percent of respondents say the board regularly participates in detailed reviews of their data breach response plan.

Figure 4. Why do you believe board members and the C-suite are knowledgeable?
From the 51 percent C-suite executive and 35 percent board member yes responses in Figure 3
More than one response permitted



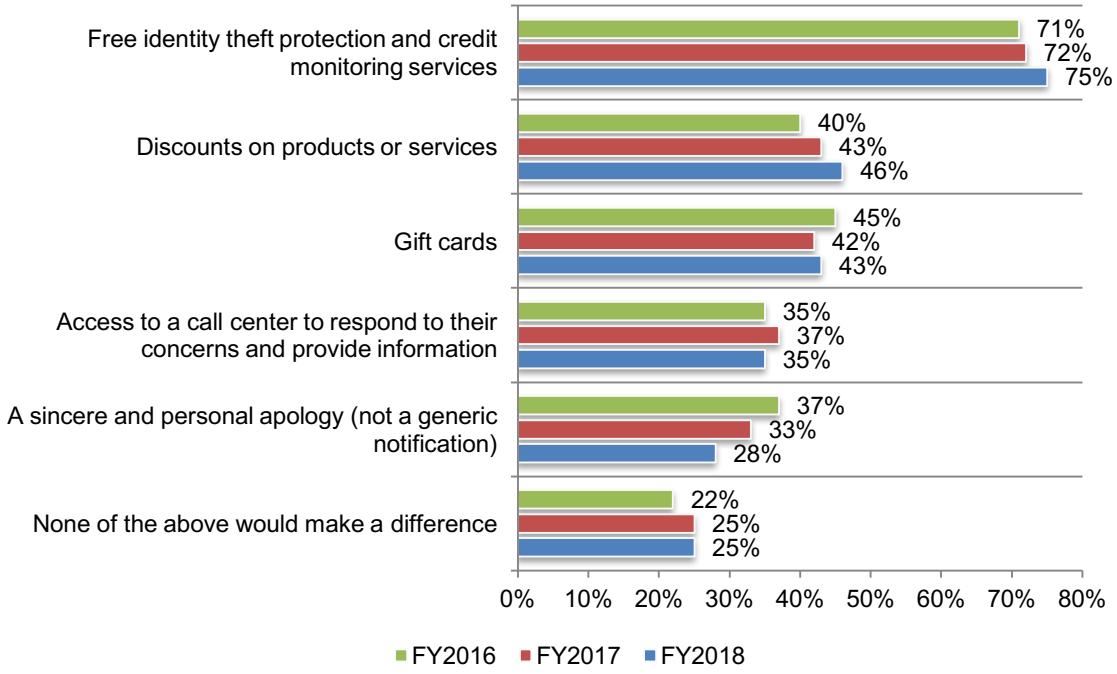
The length of time credit monitoring and identity theft protection should be provided increases. As shown in Figure 5, 53 percent of all respondents (35 percent + 13 percent + 5 percent) say protection should be provided for a minimum of four years. Last year, 51 percent said identity theft protection should be provided at least four years.

Figure 5. How long should identity theft protection be provided?



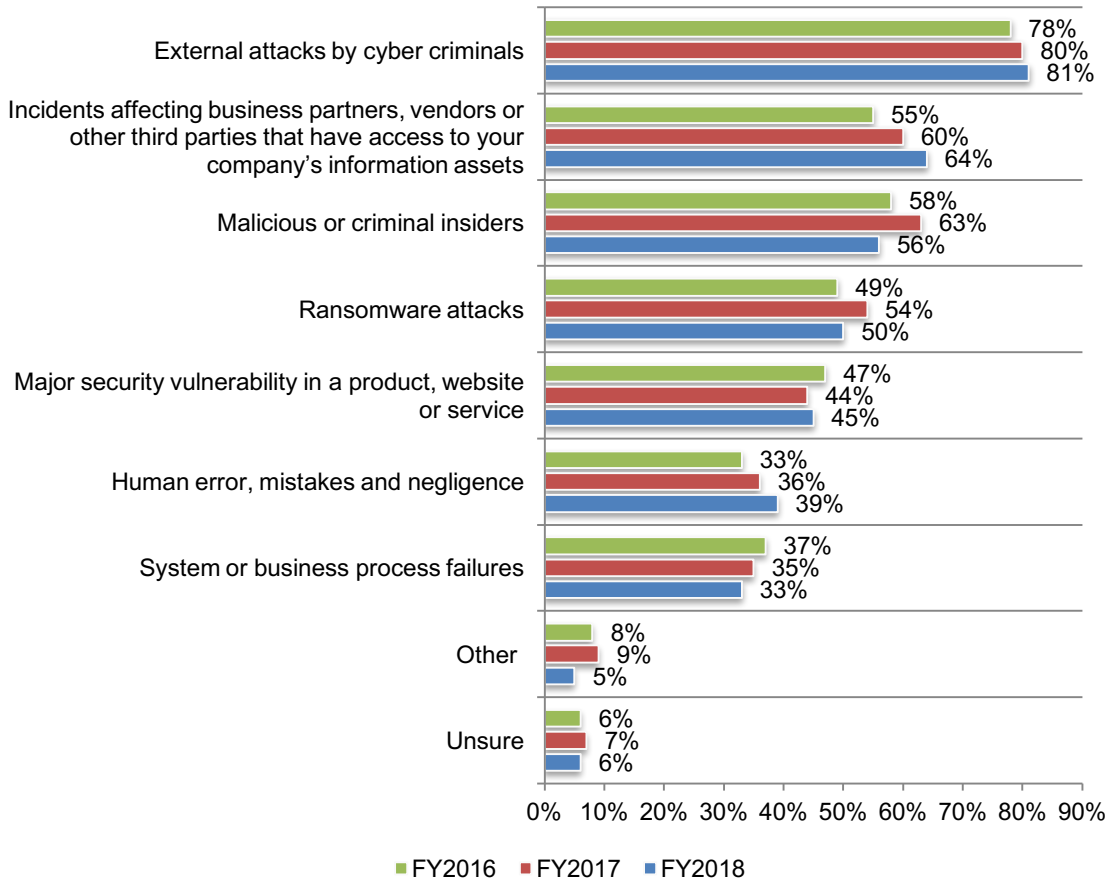
The best approach to keep customers and maintain reputation continues to be the free offer of identity theft protection and credit monitoring services. Seventy-five percent of respondents say providing free identity theft protection and credit monitoring services is the best step for preventing the loss of customers and for protecting reputation, followed by 46 percent of respondents who say that discounts on products or services help, as well as 43 percent who say gift cards should be offered to victims, as shown in Figure 6.

Figure 6. What is the best approach to keep customers and maintain reputation?
More than one response permitted



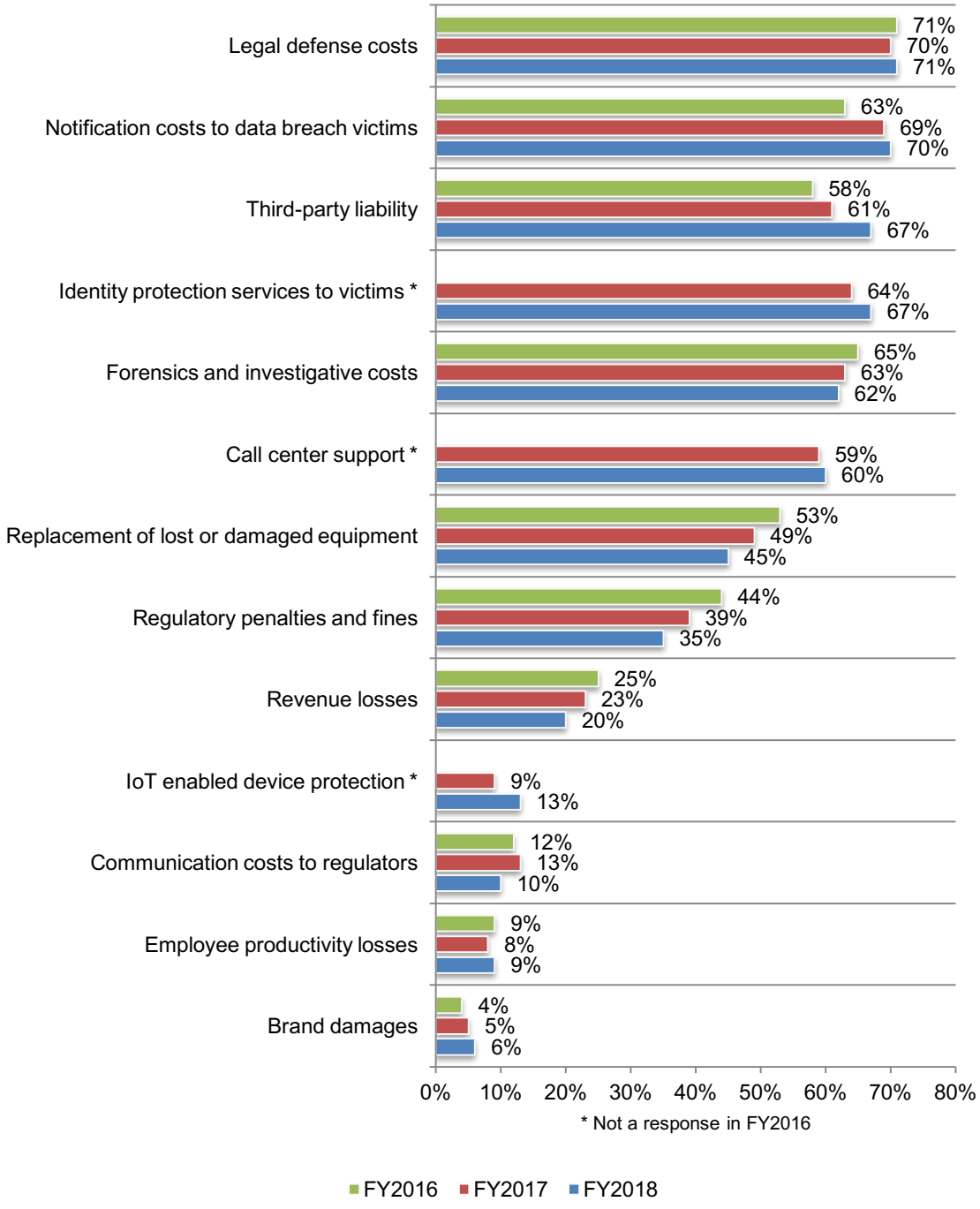
Cyber insurance policies continue to mainly cover external cyberattacks. As shown in Figure 7, the 47 percent of respondents who have cyber insurance policies say they mainly cover external attacks by cyber criminals (81 percent of respondents), malicious or criminal insiders (56 percent of respondents) and incidents affecting business partners, vendors or other third parties with access to company's information assets (64 percent of respondents). Coverage for system or business process failures has decreased from 37 percent of respondents in 2016 to 33 percent of respondents in 2018.

Figure 7. What types of incidents does your organization's cyber insurance cover?
More than one response permitted



Legal defense and notification costs are most often covered. Of the 47 percent of respondents who say their organizations have cyber insurance, most respondents (71 percent) say their cyber insurance policies reimburse legal defense costs and 70 percent of respondents say notification costs are covered, as shown in Figure 8. Respondents report their policies include identity protection services to victims (67 percent of respondents). Only 13 percent of respondents say IoT-enabled device protection is offered.

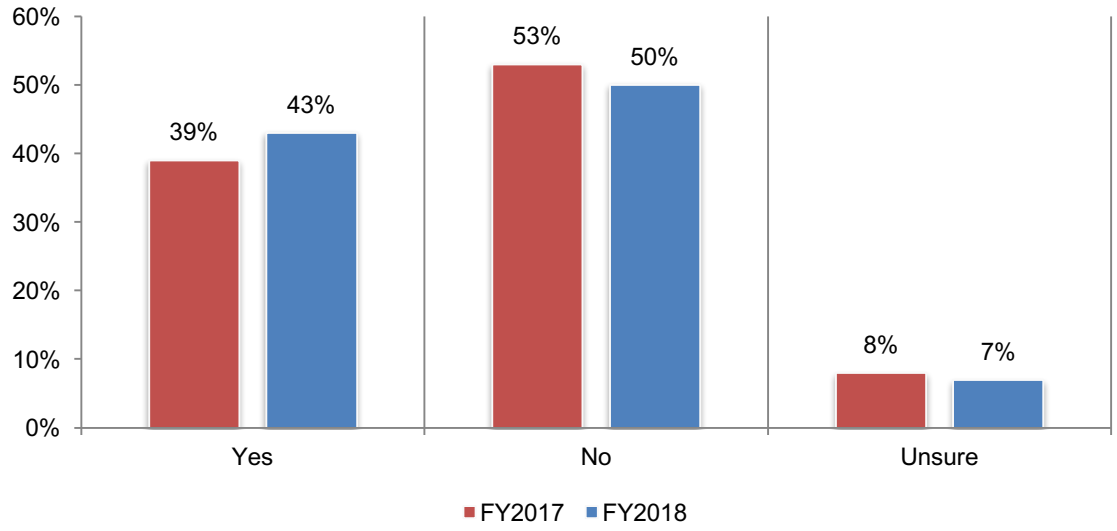
Figure 8. What coverage does this insurance offer your company?
More than one response permitted



International data breaches are increasing and organizations are not prepared

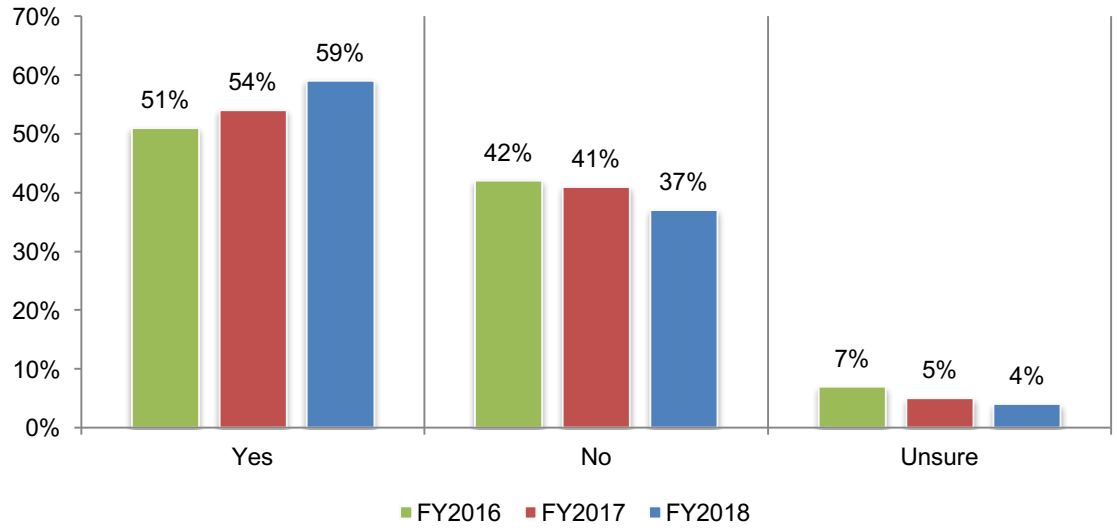
Global data breaches increase. Fifty-nine percent of respondents say their organizations had at least one data breach involving the loss or theft of more than 1,000 records containing sensitive or confidential customer or business information in the past two years. According to Figure 9, 43 percent of respondents in organizations that experienced a data breach report that their organization had an international data breach, an increase from 39 percent in 2017.

Figure 9. International data breaches increase



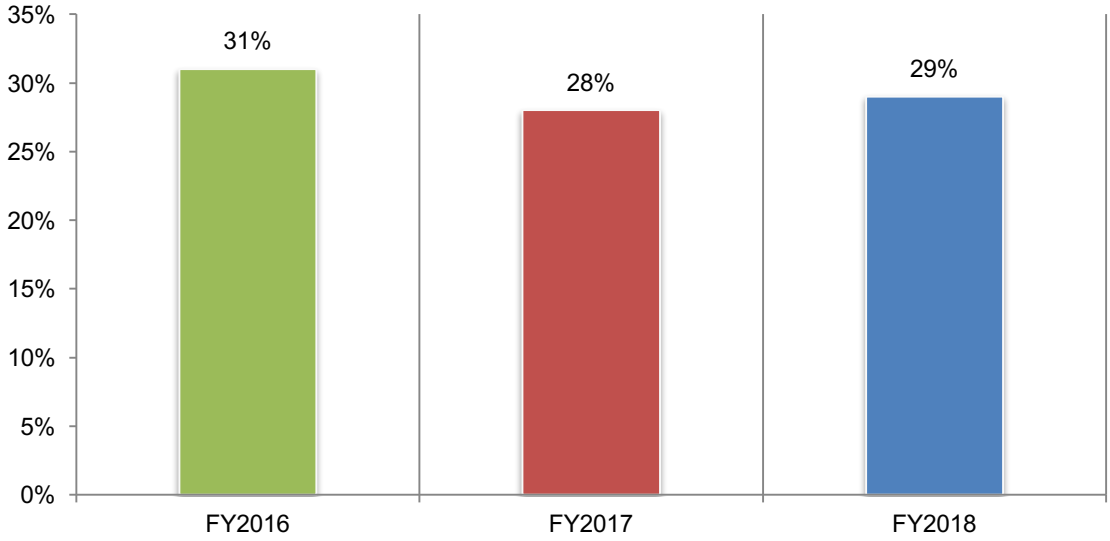
The EU General Data Protection Regulation is influencing organizations to include responding to an international data breach in their incident response plans. GDPR went into effect May 25, 2018. According to Figure 10, in the past year 59 percent of respondents say their organizations' GDPR now includes processes to manage an international data breach, an increase from 51 percent of respondents in 2016.

Figure 10. Does your incident response plan include processes to manage an international data breach?



The increase in global data breaches and GDPR are reducing organizations' confidence in their ability to deal with an international data breach. According to Figure 11, confidence in being able to manage the consequences of an international data breach has not improved.

Figure 11. How confident is your organization in its ability to deal with an international data breach?
Very confident and Confident responses combined

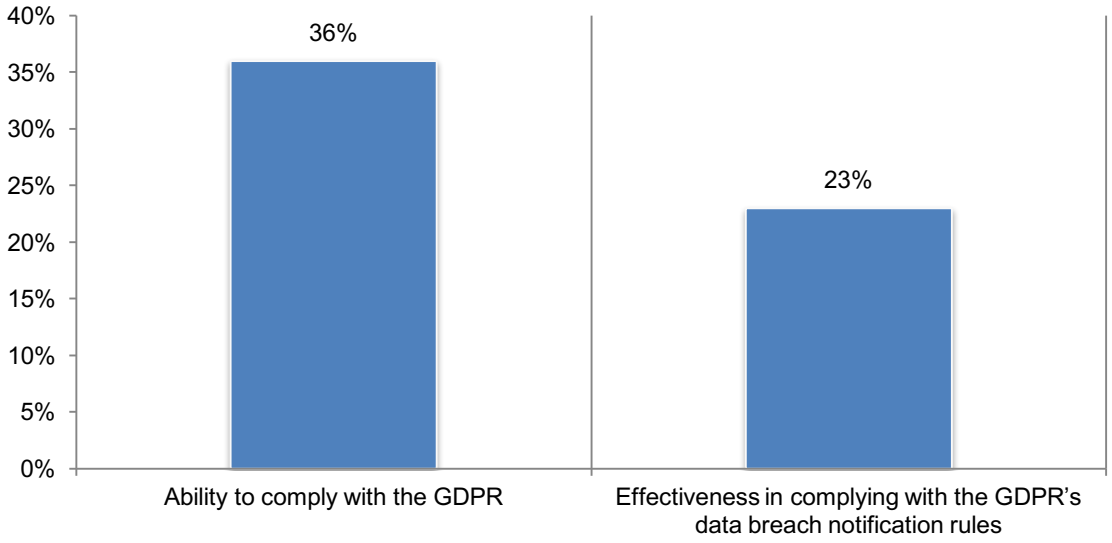


GDPR data breach notification rules are difficult to comply with. According to the GDPR Notice rule, in the event of a data breach involving personally identifiable information, the organization must notify the supervisory authority within 72 hours. If there is a delay, the controller must provide a "reasoned justification."

Respondents were asked to rate their ability to comply with the notification rule on a scale of 1 = no ability to 10 = high ability. According to Figure 12, only 36 percent of respondents say their organization has a high ability. In addition, when asked to rate their organizations' effectiveness in complying with the notification rule on a 10-point scale from 1 = low to 10 = high effectiveness, only 23 percent of respondents say their organizations are effective in achieving compliance.

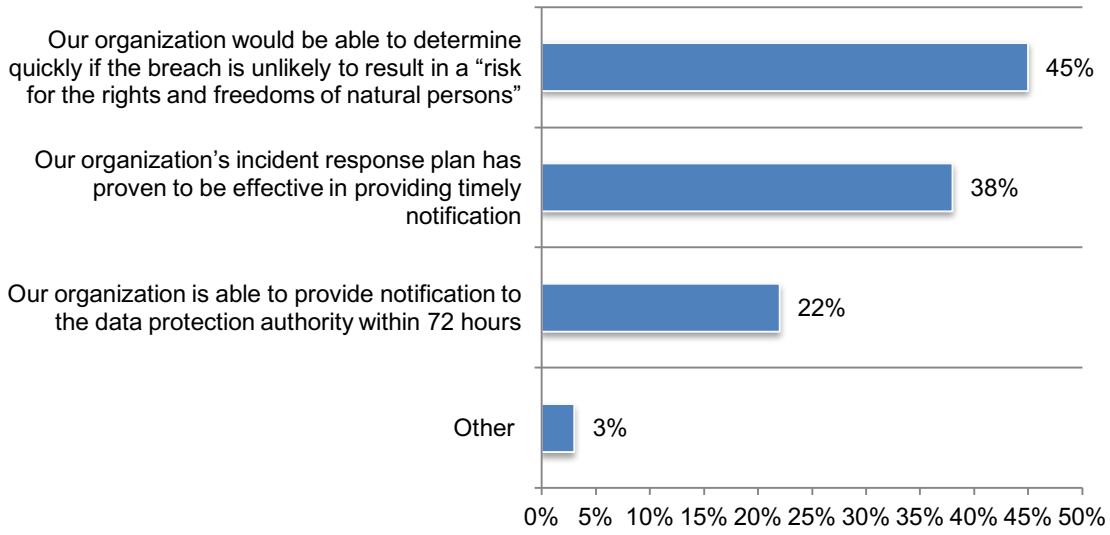
Figure 12. Ability to comply with the GDPR and effectiveness in complying with the GDPR's data breach notification rules

From 1 = No ability to 10 = high ability, and 1 = low effectiveness to 10 = high effectiveness, 7+ responses reported



The ability to determine quickly if the breach resulted in a "risk for the rights and freedoms of natural persons" is an indication compliance is very effective. Of the 23 percent of respondents who rate their organizations as highly effective, 45 percent say they are confident in their effectiveness because they would be able to determine quickly if the breach resulted in a risk to natural persons. Thirty-eight percent of respondents say their incident response plans enables timely notification.

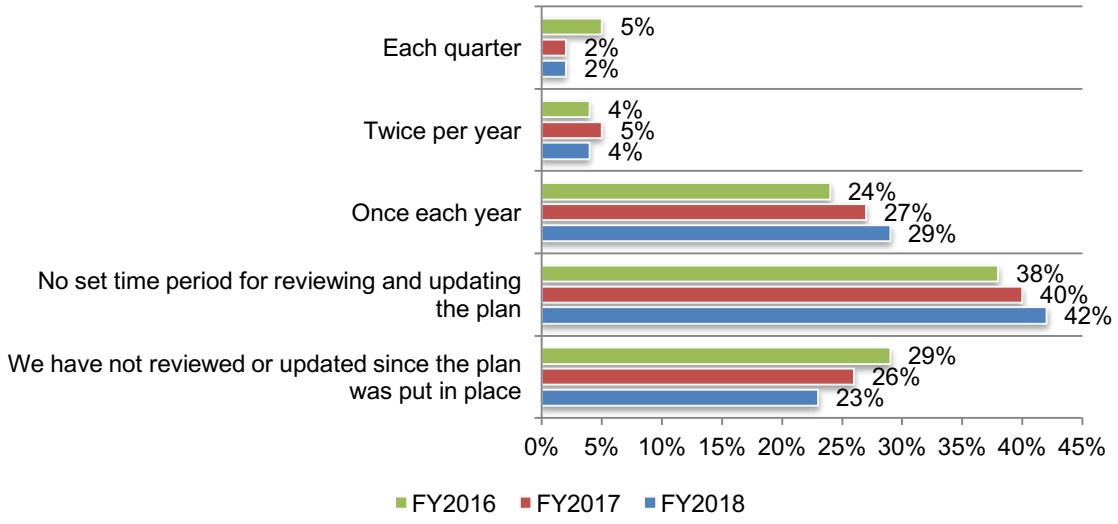
Figure 13. Why organizations believe they are effective in complying with GDPR's data breach notification rules
From the 23 percent of respondents that are effective in complying with GDPR



Data breach response plan effectiveness

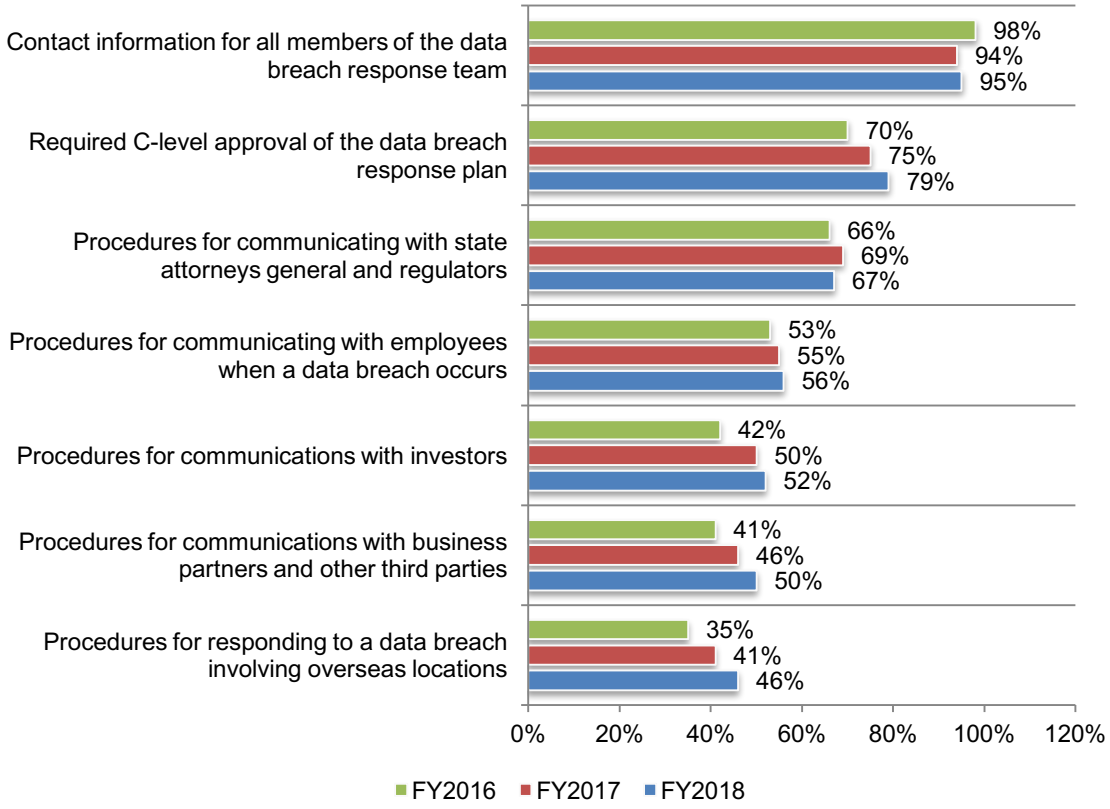
Most companies have a data breach response plan, but it is not regularly reviewed. Ninety-two percent of respondents say their organizations have a data breach notification plan in place. However, as shown in Figure 14, 65 percent of respondents have no set time for reviewing and updating the plan or have not reviewed the plan since it was put in place.

Figure 14. How often does your company update the data breach response plan?



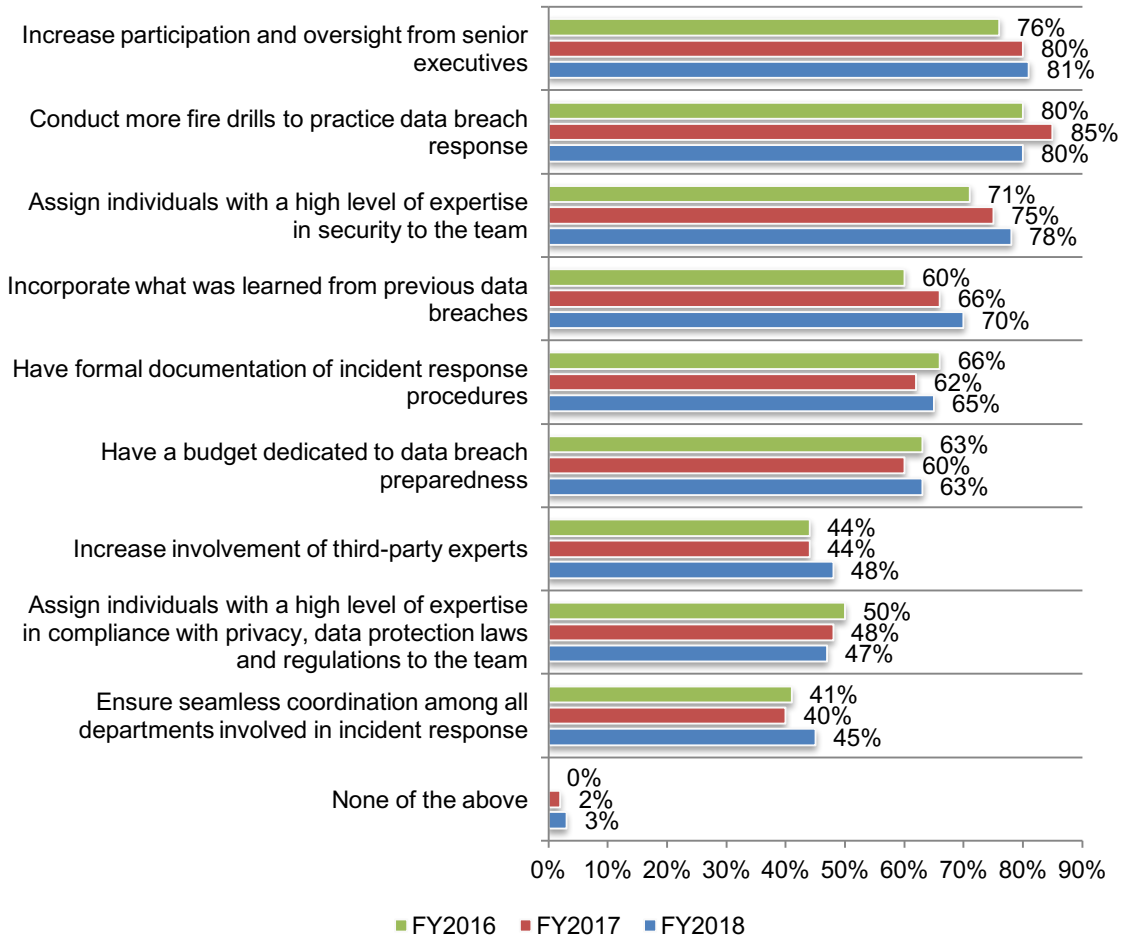
More data breach response plans are requiring C-level approval, communications with investors and third parties and responding to a data breach involving overseas locations. A comprehensive plan requires many activities to minimize the consequences of a data breach. As revealed in Figure 15, most of 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 15. What are the requirements in your company's data breach response plan?
More than one response permitted



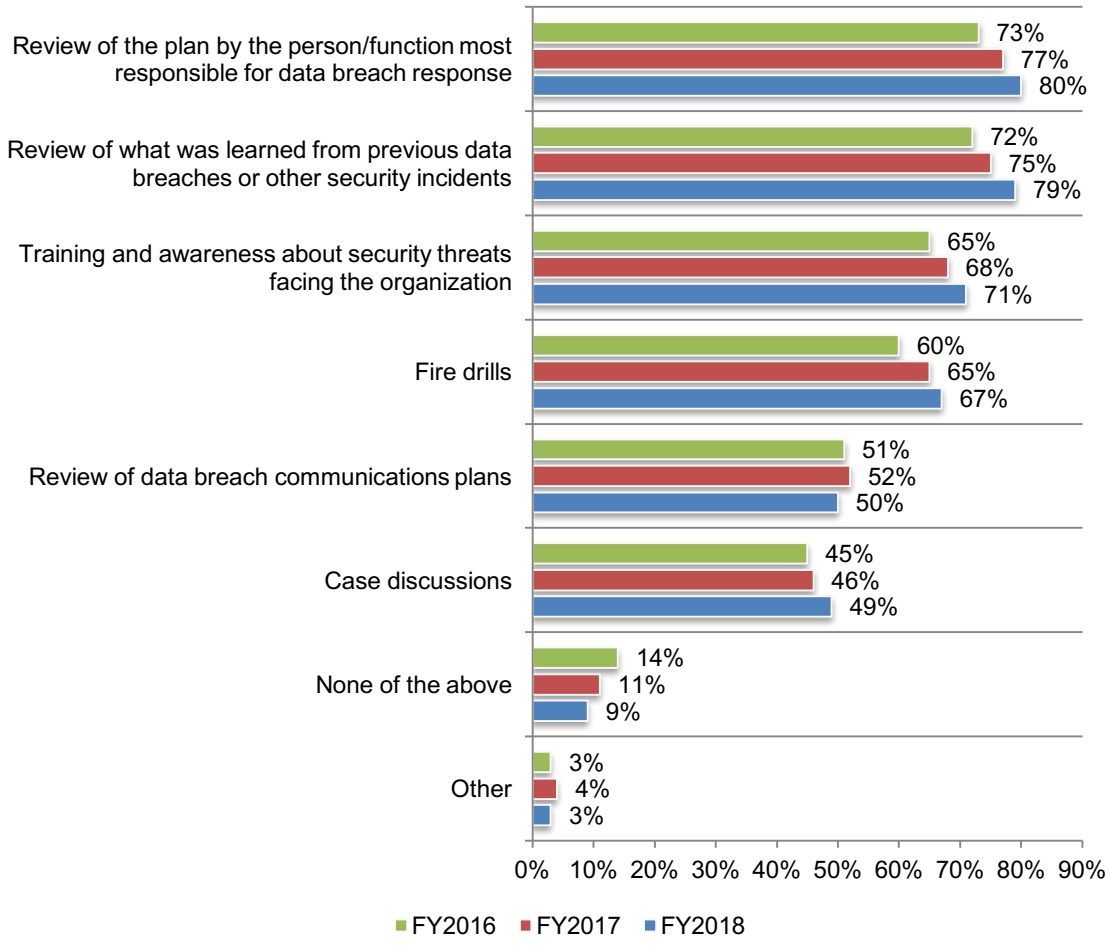
To be effective, data breach response plans need senior level involvement. As discussed previously, those at the top are not actively engaged in the data breach response plan. According to Figure 16, most organizations believe an increase in participation and oversight from senior executives, more fire drills to practice data breach response and assign individuals with a high level of expertise in security to the team will help them have a more effective response plan.

Figure 16. How could your data breach response plan become more effective?
More than one response permitted



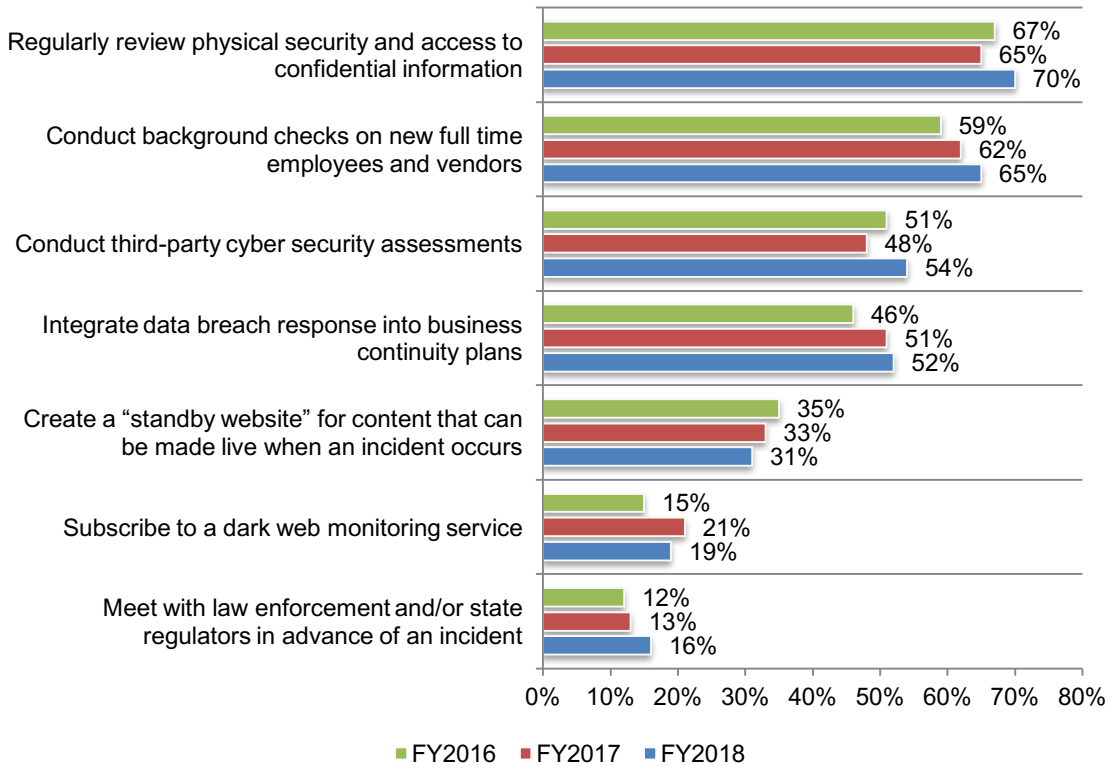
Most respondents say their organization's data breach response practice includes a review of the plan by those most responsible for data breach response. This is followed by a review of what was learned from previous data breaches or other security incidents (79 percent of respondents) and training and awareness about security threats facing the organization (71 percent of respondents), as shown in Figure 17.

Figure 17. What is included in the data breach response practice?
More than one response permitted



More organizations are integrating data breach response into business continuity plans. Figure 18 reveals that 70 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 (65 percent of respondents). The integration of data breach response into business continuity plans has increased from 46 percent of respondents in 2016 to 52 percent of respondents in 2018.

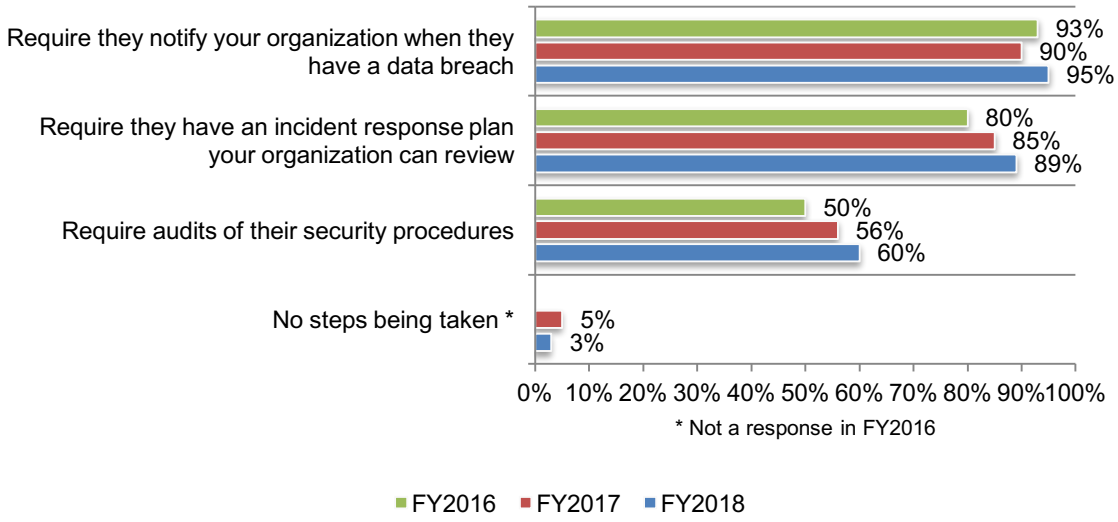
Figure 18. Does your organization take any special steps to prepare for a data breach?
More than one response permitted



More companies are requiring audits of third-party security procedures. Ninety-seven 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 19.

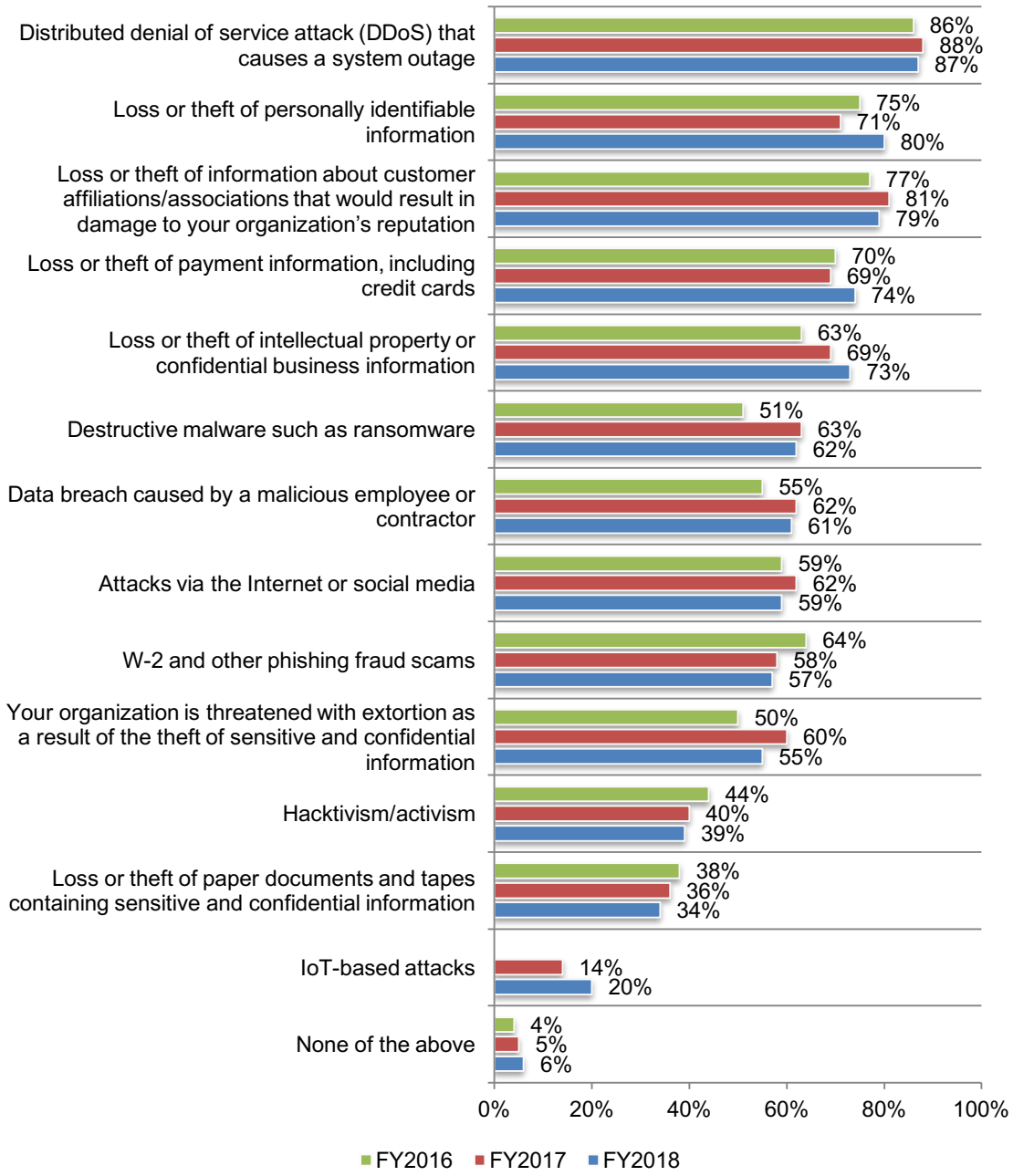
To reduce the negative consequences of a third-party data breach, more companies are requiring audits of their security procedures. Currently, 60 percent of respondents say they have such a requirement. Since 2016, the requirement that third parties have an incident response plan for their organizations to review has increased from 80 percent of respondents to 89 percent of respondents.

Figure 19. How companies minimize the consequences of a third-party data breach
More than one response permitted



More companies' incident response plans are providing guidance about how to deal with the loss or theft of PII and intellectual property. As shown in Figure 20, since 2016, there have been significant increases in the guidance provided on the following security incidents: loss or theft of personally identifiable information, loss or theft of intellectual property or confidential business information, destructive malware such as ransomware, data breaches caused by malicious employee or contractor and the threats of extortion.

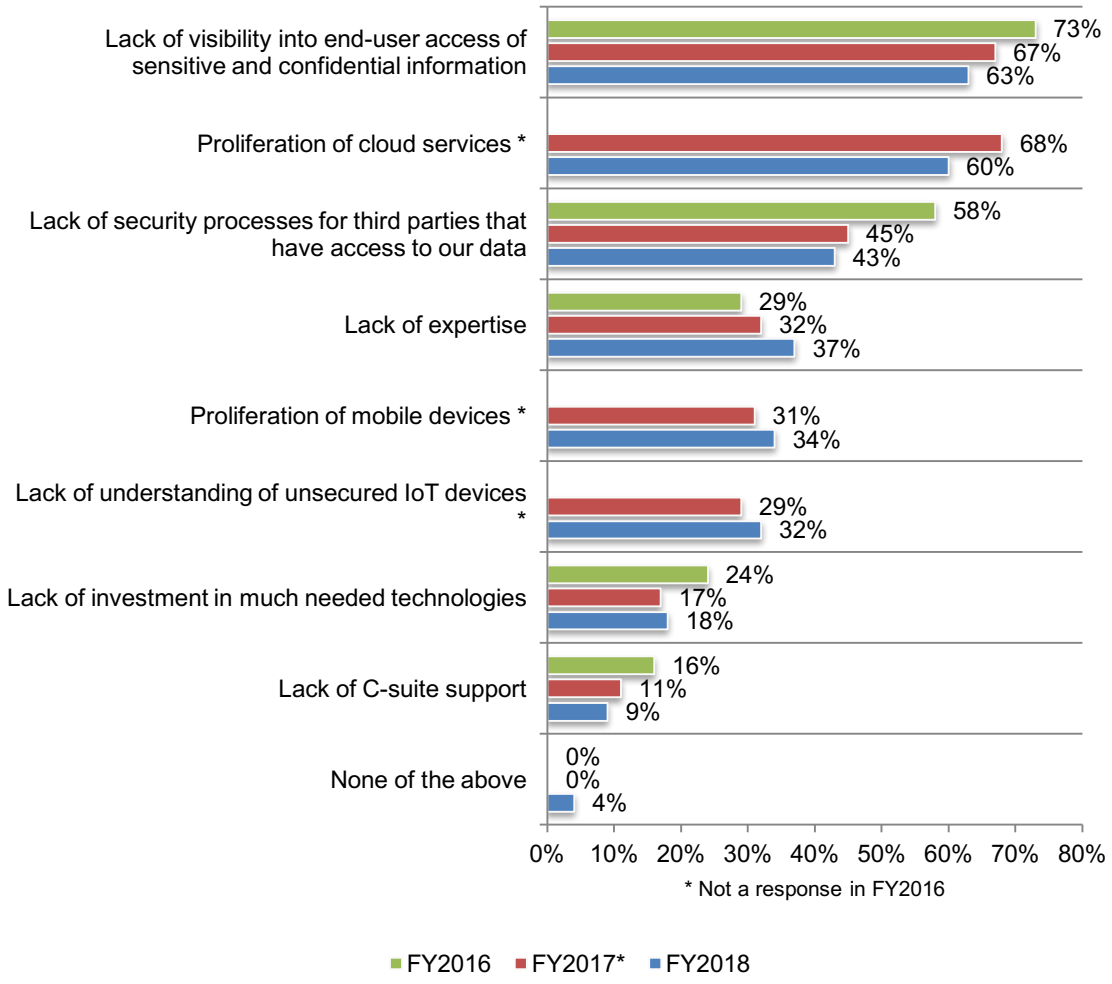
Figure 20. What guidance does the incident response plan provide on dealing with security incidents?
More than one response permitted



Threats that affect data breach preparedness

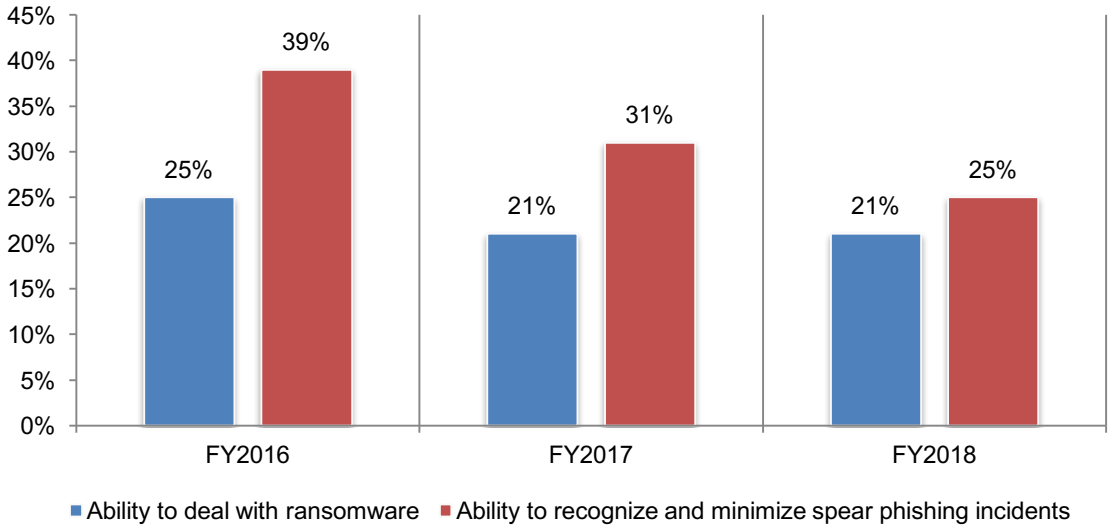
The lack of visibility and proliferation of cloud services continues to be the biggest barriers to improving IT security's ability to respond to a data breach. According to Figure 21, respondents continue to recognize the difficulty in dealing with the lack of visibility into end-user access of sensitive and confidential information and proliferation of cloud services as serious barriers to responding to a data breach. The lack of expertise as a barrier to responding to a data breach has increased significantly since 2016.

Figure 21. What are the biggest barriers to improving the ability of IT security to respond to a data breach?
Two responses permitted



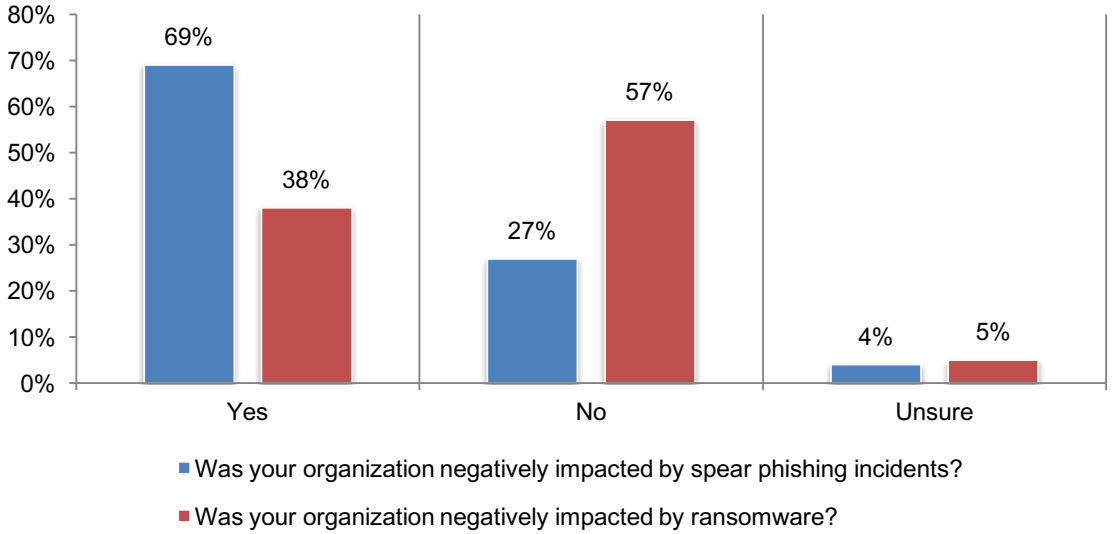
Almost every company in the study has no confidence in being able to deal with ransomware and spear phishing attacks. Despite efforts to educate employees about the threat of ransomware and spear phishing, only 21 percent of respondents are very confident in their ability to deal with ransomware and only 25 percent of respondents are confident about their ability to minimize spear phishing incidents, as shown in Figure 22.

Figure 22. Confidence in the ability to deal with a ransomware or spear phishing incident
Very confident and Confident responses combined



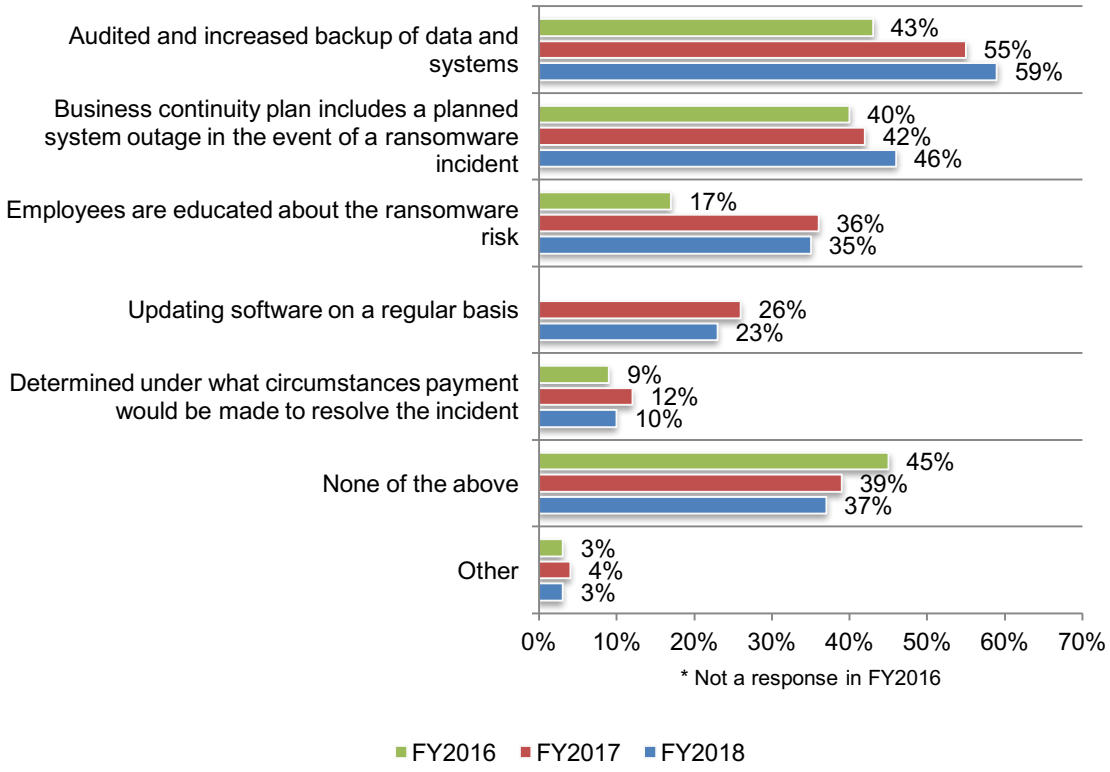
More companies were negatively impacted by spear phishing incidents than ransomware. Sixty-nine percent of respondents say their organizations have been negatively impacted by spear phishing attacks and 38 percent of respondents say they experienced ransomware attacks, as shown in Figure 23.

Figure 23. Was your organization negatively impacted by spear phishing and ransomware?



More companies are increasing backup of data and systems to prepare for a ransomware incident. According to Figure 24, more respondents report they are increasing the backup of data and systems and have a business continuity plan in place that addresses a system outage in the event of a ransomware incident.

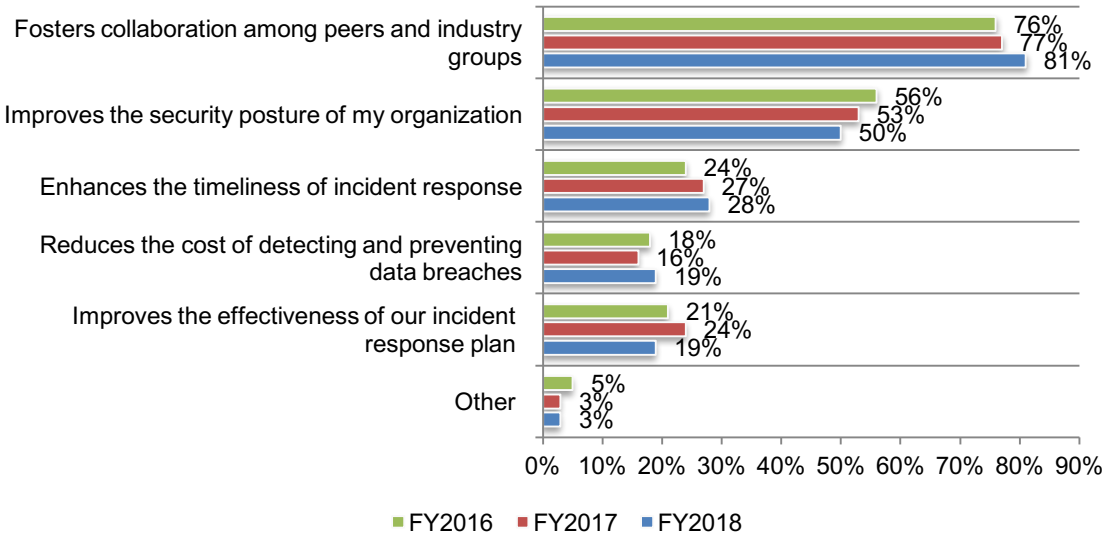
Figure 24. Have you taken the following steps to prepare for a ransomware incident?
More than one response permitted



Sharing intelligence about data breach experiences and incident response plans can improve the ability to respond to a data breach. Fifty-one percent of respondents say their organization participates or plans to participate in an initiative or program for sharing information with government and industry peers about data breaches and incident response.

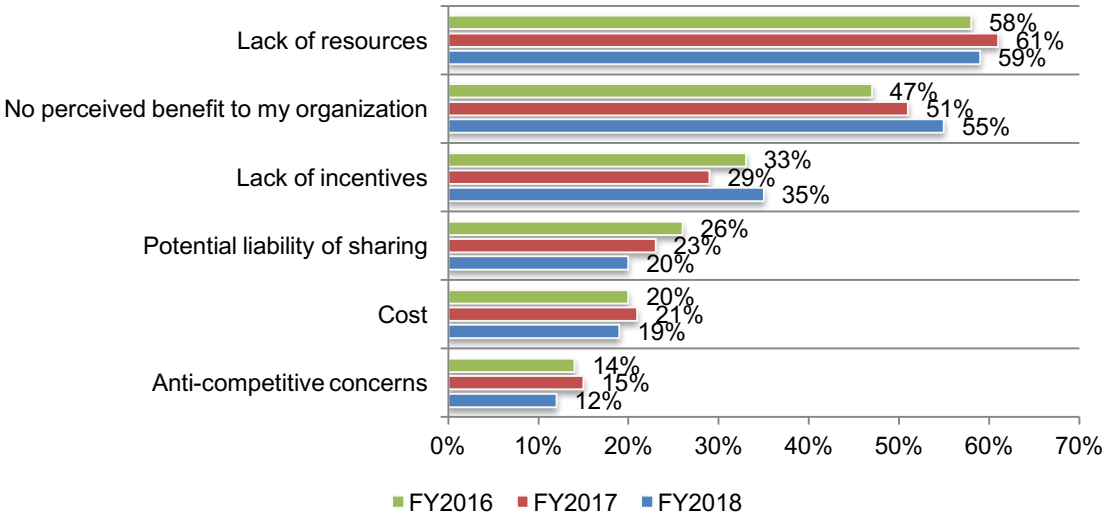
Consistent with previous years, as shown in Figure 25, the most important reason for sharing is the benefits from fostering collaboration among peers and industry groups (81 percent of respondents). Enhancing the timeliness of incident response has increased since 2016.

Figure 25. Why do you share information about your data breach experience and incident response plans?
Two responses permitted



The main reason for not sharing is the lack of resources (59 percent of respondents) and no perceived benefit to the organization (55 percent of respondents), according to Figure 26. The potential liability of sharing continues to decline as a deterrent to sharing by most companies.

Figure 26. Reasons for not sharing information
More than one response permitted

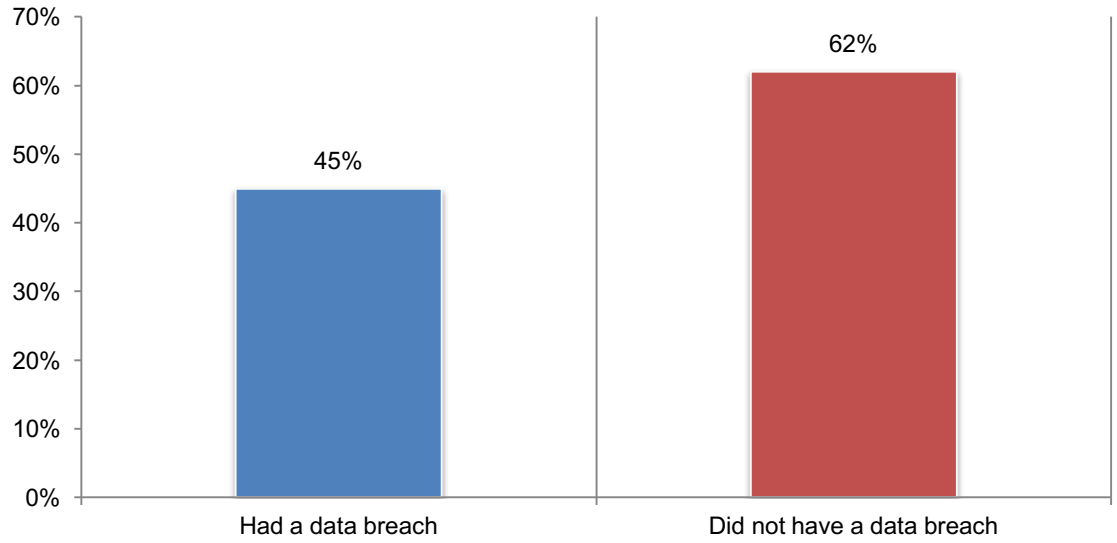


Lessons from organizations that did not have a data breach

In this year's study, 29 percent of the total respondents self-reported that their organizations did not have a data breach versus the 59 percent of respondents who say their organizations experienced at least one breach. Are there lessons to be learned from those organizations that were able to avoid such an incident? In this section, we compare the findings of organizations that did not experience a data breach to those that did.

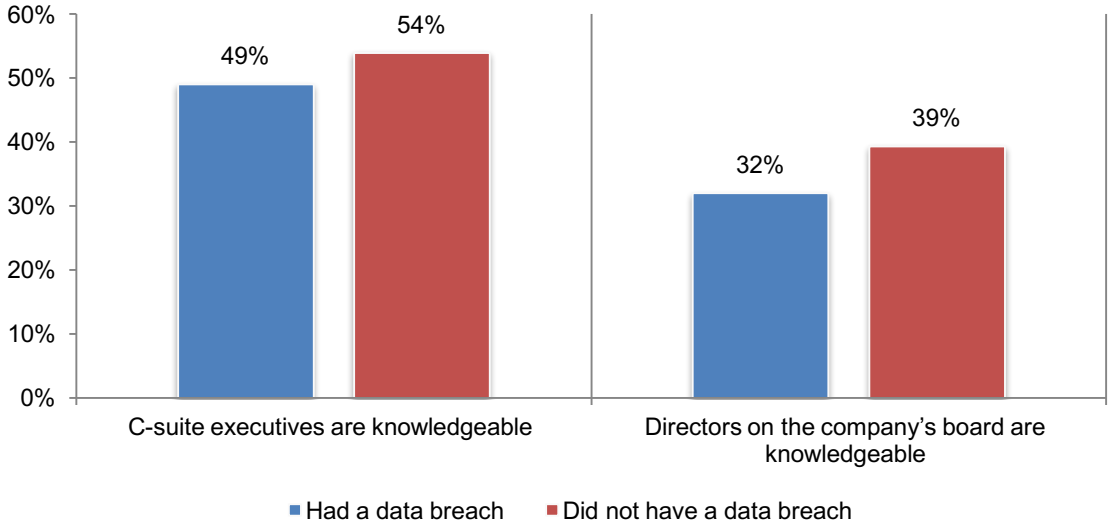
Companies that did not have a breach are more likely to rate their data breach plan as highly effective. Respondents were asked to rate the effectiveness of their data breach plans as 1 = very low effectiveness and 10 = very high effectiveness. As shown in Figure 27, 62 percent of respondents in companies that did not have a breach say these plans are very effective. In contrast, only 45 percent of respondents in companies that had a data breach rate their plans as highly effective.

Figure 27. How effective is your company's data breach response plan?
1 = very low effectiveness to 10 = very high effectiveness, 7+ responses presented



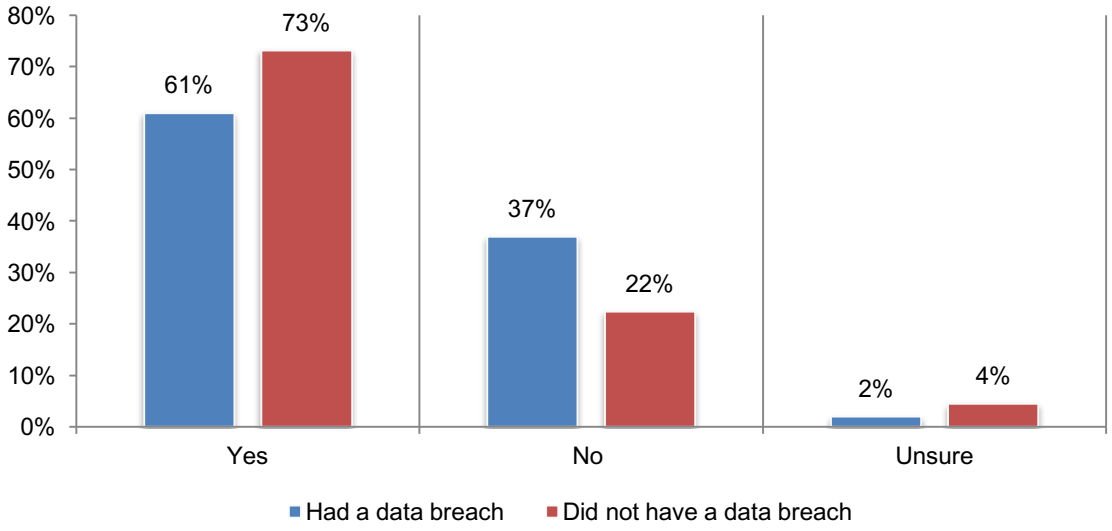
Boards of directors and C-suite executives knowledgeable and engaged in incident response plans can reduce the likelihood of a data breach. According to Figure 28, 54 percent of respondents in organizations that did not have a breach vs. 49 percent in organizations that had a data breach say their C-suite executives are informed about how their privacy and IT security functions plan to deal with a data breach. While it is still a low percentage of respondents, they are more likely to have a knowledgeable board (39 percent vs. 32 percent of respondents.

Figure 28. Do you believe your company's C-suite and boards of directors are knowledgeable about its plans to deal with a possible data breach?
Strongly agree and *Agree* responses combined



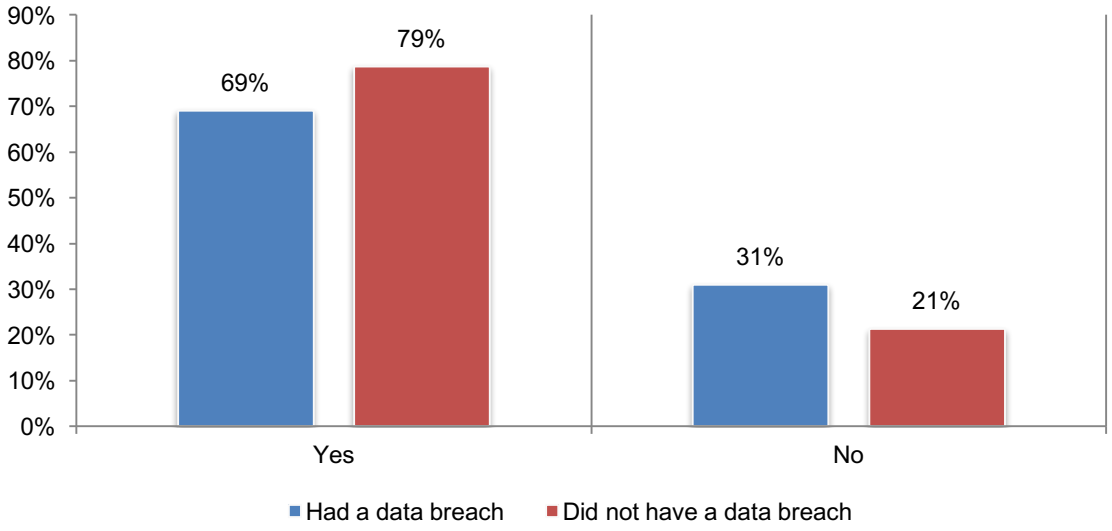
Investments in technologies that improve detection of and response to a data breach seem to pay off. As shown in Figure 29, 73 percent of respondents say their organizations increased their investment in technologies specifically to better detect and respond quickly to a data breach.

Figure 29. In the past 12 months, has your organization increased its investment in security technologies to better detect and respond quickly to a data breach?



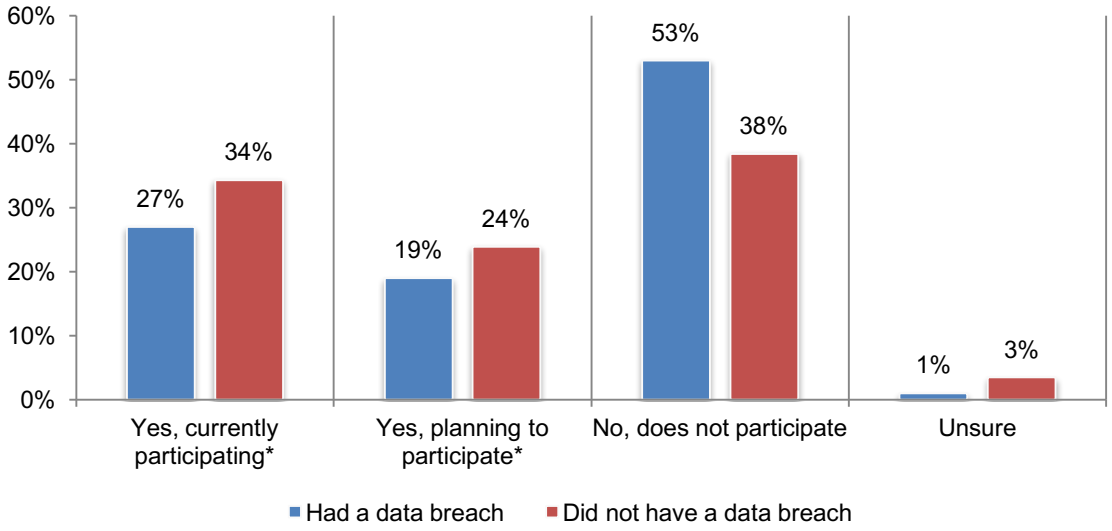
Privacy and data protection awareness and training programs have a positive impact on reducing the likelihood of a data breach. Privacy and data protection awareness programs that specifically target employees and other stakeholders who have access to sensitive or confidential personal information are shown to reduce the likelihood of a data breach. According to Figure 30, 79 percent of respondents whose organizations did not have a data breach say they provide such training vs. 69 percent of respondent in the data breach group.

Figure 30. Does your organization have a privacy/data protection awareness and training program for those who have access to sensitive information?



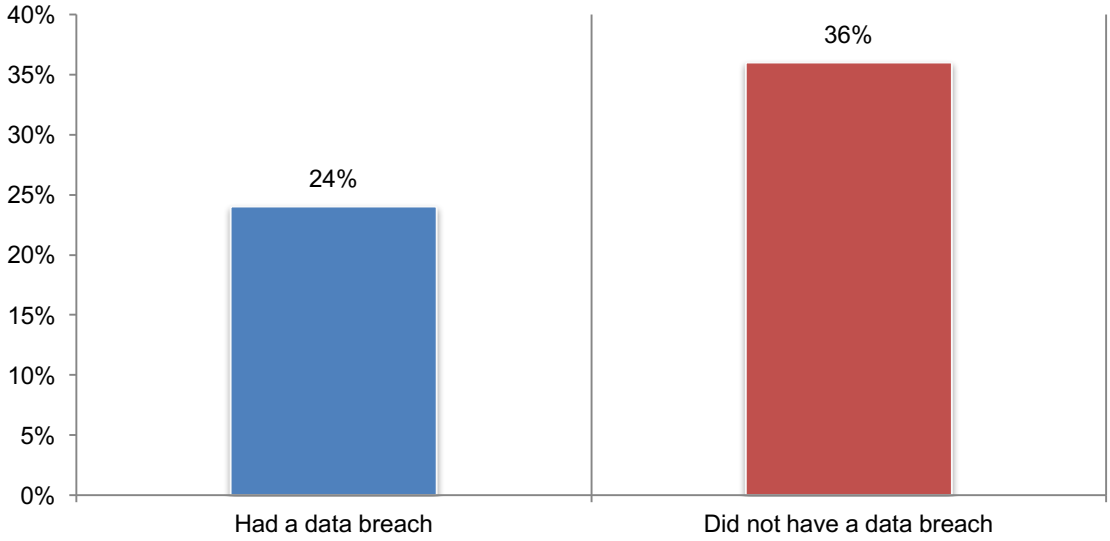
Participating in programs to share information about data breaches and incident response supports an organization's ability to avoid a data breach. Learning from industry peers and government agencies about how to better prepare and respond to a data breach can strengthen an organization's security posture and the ability to avoid a data breach. As shown in Figure 31, organizations that did not have a data breach are far more likely to participate or plan to participate in such an initiative (59 percent vs. 46 percent of respondents).

Figure 31. Does your organization participate in a program for sharing information with government and industry peers about data breaches and incident response?



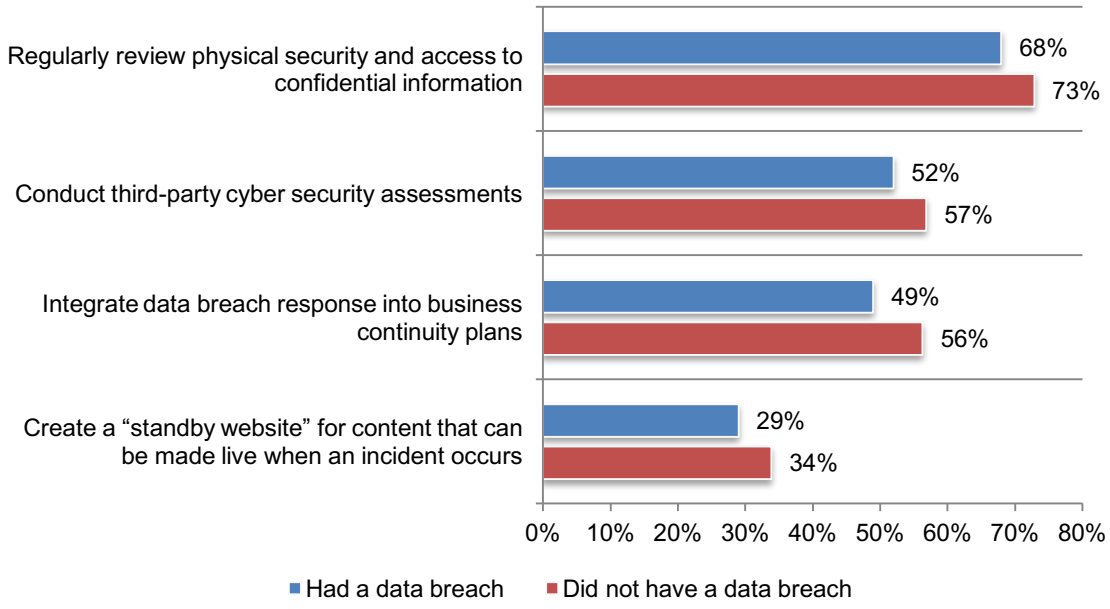
Companies that have avoided a data breach are more confident in their ability to respond to an international data breach. Companies that did not have a data breach are more likely to have an incident response plan that includes how to manage an international data breach (65 percent vs. 55 percent).

Figure 32. How confident is your company in being able to manage an international data breach?
Very confident and Confident responses combined



Companies that did not have a data breach are more likely to take steps to prepare for a data breach. As shown in Figure 33, more companies that managed to prevent a data breach regularly review physical security and access to confidential information, conduct third-party cybersecurity assessments, integrate data breach response into business continuity plans and create a "standby website" for content that can be made live when an incident occurs.

Figure 33. Steps taken to prepare for a data breach
More than one response permitted



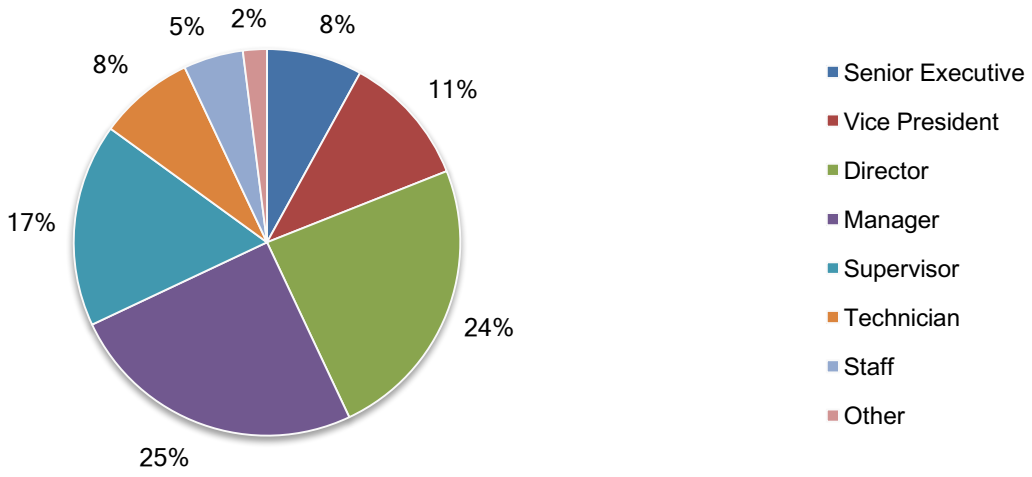
Part 3. Methods

A sampling frame of 15,986 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 702 total returns. Screening and reliability checks required the removal of 59 surveys. Our final sample consisted of 643 surveys or a 4.0 percent response rate.

Table 1. Sample response	Freq	Pct%
Sampling frame	15,986	100.0%
Total returns	702	4.4%
Rejected or screened surveys	59	0.4%
Final sample	643	4.0%

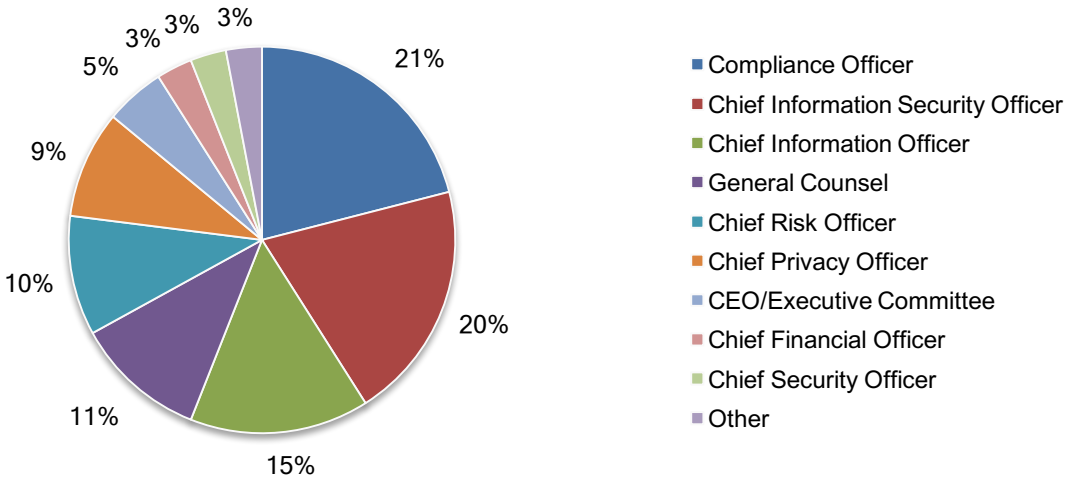
Pie Chart 1 reports the respondent's organizational level within participating organizations. By design, a majority of respondents (85 percent) are at or above the supervisory levels.

Pie Chart 1. Current position within the organization



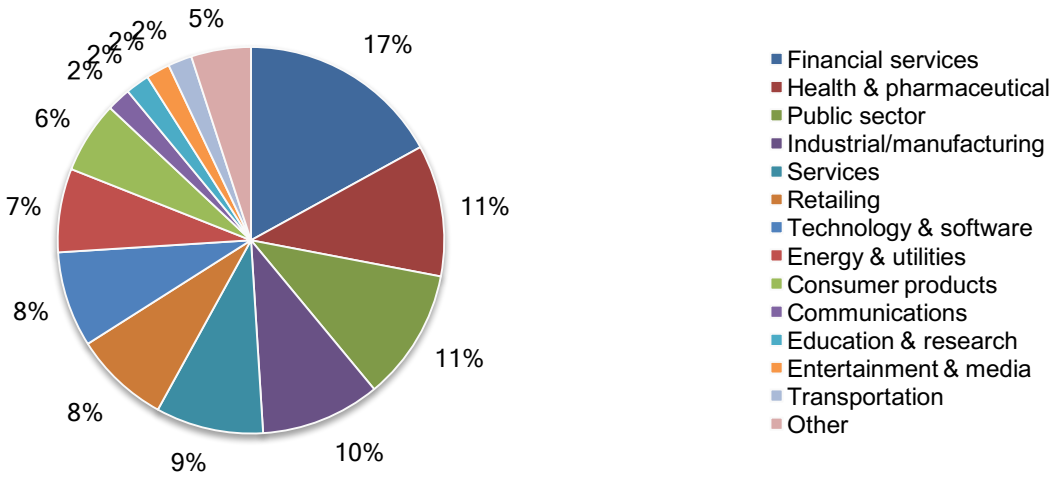
Pie Chart 2 reveals that 21 percent of respondents report to the Compliance Officer, 20 percent of respondents report to the Chief Information Security Officer, and 15 percent of respondents report to the Chief Information Officer.

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



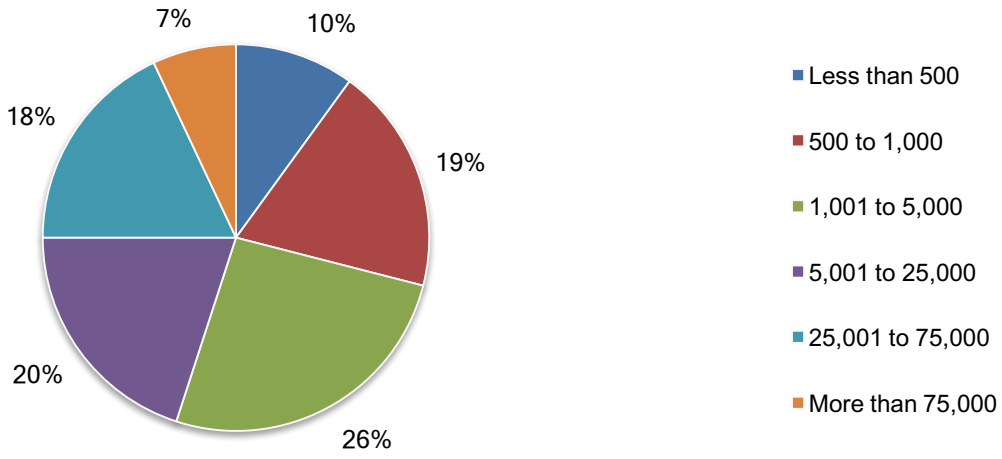
Pie Chart 3 reports the industry classification of respondents' organizations. This chart identifies financial services (17 percent of respondents) as the largest segment, followed by health and pharmaceutical (11 percent of respondents), public sector (11 percent of respondents) and industrial/manufacturing (10 percent of respondents).

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 between November 7 and November 21, 2018.

Survey response	FY2018	FY2017	FY2016
Sampling frame	15,986	15,402	14,878
Total returns	702	679	665
Rejected or screened surveys	59	55	46
Final sample	643	624	619
Response rate	4.0%	4.1%	4.2%

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?	FY2018	FY2017	FY2016
Yes	59%	56%	52%
No	29%	31%	34%
Unsure	12%	13%	14%
Total	100%	100%	100%

Q1b. If yes, how frequently did these incidents occur during the past 2 years?	FY2018	FY2017	FY2016
Only once	27%	30%	34%
2 to 3 times	35%	37%	35%
4 to 5 times	27%	23%	20%
More than 5 times	11%	10%	11%
Total	100%	100%	100%

Q1c. If yes, were any of these breaches international or global in scope?	FY2018	FY2017
Yes	43%	39%
No	50%	53%
Unsure	7%	8%
Total	100%	100%

Attributions. Please rate each statement using the scale provided below each item. Strongly agree and agree response	FY2018	FY2017	FY2016
Q2. My organization is prepared to respond to the theft of sensitive and confidential information that requires notification to victims and regulators.	65%	62%	59%
Q3. My organization is prepared to respond to a data breach involving business confidential information and intellectual property.	36%	40%	41%
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%	40%	39%

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.	41%	36%	34%
Q6. My organization's incident response plan includes breaches involving IoT devices.	35%	29%	
Q7. My organization is confident in its ability to minimize the financial and reputational consequences of a material data breach.	21%	25%	27%
Q8. Following a data breach, a credit monitoring and/or identity theft protection product is the best protection for consumers.	59%	57%	59%

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?	FY2018	FY2017	FY2016
Yes	75%	71%	67%
No	25%	29%	33%
Total	100%	100%	100%

Q9b. If yes, how long should identity theft protection be provided?	FY2018	FY2017	FY2016
2 to 3 years	47%	49%	47%
4 to 7 years	35%	30%	29%
8 to 10 years	13%	16%	18%
More than 10 years	5%	5%	6%
Total	100%	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?	FY2018	FY2017	FY2016
Free identity theft protection and credit monitoring services	75%	72%	71%
A sincere and personal apology (not a generic notification)	28%	33%	37%
Discounts on products or services	46%	43%	40%
Gift cards	43%	42%	45%
Access to a call center to respond to their concerns and provide information	35%	37%	35%
None of the above would make a difference	25%	25%	22%
Total	252%	252%	250%

Q11. Which of the following issues would have the greatest impact on your organization's reputation? Please select one choice.	FY2018	FY2017	FY2016
Poor customer service	29%	28%	31%
Labor or union dispute	2%	3%	2%
Environmental incident	9%	8%	7%
Data breach	27%	25%	23%
Regulatory fines	5%	4%	5%
Publicized lawsuits	9%	10%	12%
Product recall	18%	20%	19%
CEO's salary	1%	2%	1%
Total	100%	100%	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?	FY2018	FY2017	FY2016
Yes	51%	48%	43%
No	49%	52%	57%
Total	100%	100%	100%

Q12b. If yes, why do you believe your company's C-suite executives are knowledgeable? Please select all that apply.	FY2018	FY2017	FY2016
They regularly participate in detailed reviews of our data breach response plan	22%	19%	17%
They understand the specific security threats facing our organization	37%	36%	34%
They provide detailed feedback about the data breach response plan	24%	25%	20%
They assume responsibility for the successful execution of the incident response plan	23%	25%	26%
They have requested to be notified ASAP if a material data breach occurs	49%	45%	40%
They participate in a high level review of the organization's data protection and privacy practices	13%	15%	16%
Total	168%	165%	153%

Q13a. Do you believe directors on your company's board are knowledgeable about plans to deal with a possible data breach?	FY2018	FY2017
Yes	35%	39%
No	65%	61%
Total	100%	100%

Q13b. If yes, why do you believe board members are knowledgeable? Please select all that apply.	FY2018	FY2017
They regularly participate in detailed reviews of our data breach response plan	10%	11%
They understand the specific security threats facing our organization	35%	40%
They provide detailed feedback about the data breach response plan	23%	21%
They assume responsibility for the successful execution of the incident response plan	13%	15%
They have requested to be notified ASAP if a material data breach occurs	49%	56%
They participate in a high level review of the organization's data protection and privacy practices	12%	9%
Total	142%	152%

Q14. What types of data loss is your organization most concerned about? Please select the top two.	FY2018	FY2017	FY2016
Loss or theft of customer information	60%	63%	
Loss or theft of employee personal data	34%	40%	42%
Loss or theft of medical data	12%	11%	10%
Loss or theft of consumer data*	21%	20%	53%
Loss or theft of intellectual property	60%	54%	71%
Loss or theft of payment card data	13%	12%	24%
Total	200%	200%	200%

*Customer information is included in the consumer data for FY2016

Q15. What are the biggest barriers to improving the ability of IT security to respond to a data breach? Please select the top three	FY2018	FY2017*	FY2016
Lack of investment in much needed technologies	18%	17%	24%
Lack of expertise	37%	32%	29%
Lack of C-suite support	9%	11%	16%
Lack of security processes for third parties that have access to our data	43%	45%	58%
Lack of visibility into end-user access of sensitive and confidential information	63%	67%	73%
Lack of understanding of unsecured IoT devices	32%	29%	
Proliferation of mobile devices	34%	31%	
Proliferation of cloud services	60%	68%	
None of the above	4%	0%	0%
Total	300%	300%	200%

FY2016 required only 2 choices

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?	FY2018	FY2017	FY2016
Yes	66%	63%	58%
No	31%	34%	38%
Unsure	3%	3%	4%
Total	100%	100%	100%

Q17. How confident is your organization in its ability to deal with ransomware?	FY2018	FY2017	FY2016
Very confident	11%	10%	12%
Confident	10%	11%	13%
Somewhat confident	20%	18%	19%
Not confident	34%	36%	30%
No confidence	25%	25%	26%
Total	100%	100%	100%

Q18. Does your organization train employees to recognize and minimize spear phishing incidents?	FY2018	FY2017
Yes	47%	45%
No	53%	55%
Total	100%	100%

Q19. How confident is your organization in its ability to recognize and minimize spear phishing incidents?	FY2018	FY2017	FY2016
Very confident	13%	15%	19%
Confident	12%	16%	20%
Somewhat confident	26%	25%	23%
Not confident	30%	26%	20%
No confidence	19%	18%	18%
Total	100%	100%	100%

Q20a. Was your organization negatively impacted by spear phishing incidents?	FY2018	FY2017
Yes	69%	70%
No	27%	25%
Unsure	4%	5%
Total	100%	100%

20b. Was your organization negatively impacted by ransomware?	FY2018	FY2017
Yes	38%	34%
No	57%	60%
Unsure	5%	6%
Total	100%	100%

Q21. Have you taken the following steps to prepare for a ransomware incident? Please select all that apply.	FY2018	FY2017	FY2016
Determined under what circumstances payment would be made to resolve the incident	10%	12%	9%
Audited and increased back up of data and systems	59%	55%	43%
Business continuity plan includes a planned system outage in the event of a ransomware incident	46%	42%	40%
Employees are educated about the ransomware risk	35%	36%	17%
Updating software on a regular basis	23%	26%	
None of the above	37%	39%	45%
Other	3%	4%	3%
Total	213%	214%	157%

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?	FY2018	FY2017	FY2016
Yes	73%	68%	61%
No	27%	32%	37%
Total	100%	100%	98%

Q22b. If yes, how often is training conducted?	FY2018	FY2017	FY2016
As part of employee orientation	51%	45%	42%
Every six months	2%	3%	3%
Annually	26%	27%	26%
Sporadically	21%	24%	29%
Unsure	0%	1%	0%
Total	100%	100%	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?	FY2018	FY2017	FY2016
Yes	60%	54%	50%
No	35%	42%	45%
Unsure	5%	4%	5%
Total	100%	100%	100%

Q23. How significant is the influence of employee negligence on your organization's overall security posture?	FY2018	FY2017
Very significant	45%	39%
Significant	39%	41%
Not significant	11%	14%
Minimal	5%	6%
Total	100%	100%

Q24a. Does your organization have a data breach or cyber insurance policy?	FY2018	FY2017	FY2016
Yes	47%	45%	38%
No	53%	55%	62%
Total	100%	100%	100%

Q24b. If no, does your organization plan to purchase a data breach or cyber insurance policy?	FY2018	FY2017	FY2016
Yes, within the next six months	24%	21%	19%
Yes, within the next year	23%	24%	24%
Yes, within the next two years	9%	11%	14%
No plans to purchase	42%	40%	40%
Unsure	2%	4%	3%
Total	100%	100%	100%

Q25. What types of incidents does your organization's cyber insurance cover? Please select all that apply.	FY2018	FY2017	FY2016
External attacks by cyber criminals	81%	80%	78%
Malicious or criminal insiders	56%	63%	58%
System or business process failures	33%	35%	37%
Human error, mistakes and negligence	39%	36%	33%
Incidents affecting business partners, vendors or other third parties that have access to your company's information assets	64%	60%	55%
Ransomware attacks	50%	54%	49%
Major security vulnerability in a product, website or service	45%	44%	47%
Other	5%	9%	8%
Unsure	6%	7%	6%
Total	379%	388%	371%

Q26. What coverage does this insurance offer your company? Please select all that apply.	FY2018	FY2017	FY2016
Identity protection services to victims	67%	64%	
Call center support	60%	59%	
Forensics and investigative costs	62%	63%	65%
Notification costs to data breach victims	70%	69%	63%
Communication costs to regulators	10%	13%	12%
Employee productivity losses	9%	8%	9%
Replacement of lost or damaged equipment	45%	49%	53%
Revenue losses	20%	23%	25%
Legal defense costs	71%	70%	71%
Regulatory penalties and fines	35%	39%	44%
Third-party liability	67%	61%	58%
Brand damages	6%	5%	4%
IoT enabled device protection	13%	9%	
Other	6%	7%	8%
Unsure	4%	5%	6%
Total	545%	544%	418%

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.	FY2018	FY2017	FY2016
Require they have an incident response plan your organization can review	89%	85%	80%
Require they notify your organization when they have a data breach	95%	90%	93%
Require audits of their security procedures	60%	56%	50%
No steps being taken	3%	5%	
Total	247%	236%	223%

Q28a. Does your organization participate in an initiative or program for sharing information with government and industry peers about data breaches and incident response?	FY2018	FY2017	FY2016
Yes, currently participating*	30%	26%	41%
Yes, planning to participate*	21%	21%	
No, does not participate	47%	53%	59%
Unsure	2%	0%	
Total	100%	100%	100%

* Only one Yes response in FY2016

Q28b. If your organization shares information about its data breach experience and incident response plans, what are the main reasons? Please select only three top choices.	FY2018	FY2017	FY2016
Improves the security posture of my organization	50%	53%	56%
Improves the effectiveness of our incident response plan	19%	24%	21%
Enhances the timeliness of incident response	28%	27%	24%
Reduces the cost of detecting and preventing data breaches	19%	16%	18%
Fosters collaboration among peers and industry groups	81%	77%	76%
Other	3%	3%	5%
Total	200%	200%	200%

Q28c. If no, why does your organization not participate in a threat-sharing program? Please select only two top choices.	FY2018	FY2017	FY2016
Cost	19%	21%	20%
Potential liability of sharing	20%	23%	26%
Anti-competitive concerns	12%	15%	14%
Lack of resources	59%	61%	58%
Lack of incentives	35%	29%	33%
No perceived benefit to my organization	55%	51%	47%
Other	0%	0%	2%
Total	200%	200%	200%

Part 3. Data breach response plan

Q29a. Does your organization have a data breach response plan in place?	FY2018	FY2017	FY2016
Yes	92%	88%	86%
No	8%	12%	14%
Total	100%	100%	100%

Q29b. If no, why not?	FY2018	FY2017	FY2016
No resources or budget	36%	38%	41%
Not important to have data breach response plan in place	11%	13%	15%
Lack of C-level support	23%	20%	21%
Outsourced to consultants	29%	29%	23%
Other	1%	0%	0%
Total	100%	100%	100%

Q30. How often does your company update the data breach response plan?	FY2018	FY2017	FY2016
Each quarter	2%	2%	5%
Twice per year	4%	5%	4%
Once each year	29%	27%	24%
No set time period for reviewing and updating the plan	42%	40%	38%
We have not reviewed or updated since the plan was put in place	23%	26%	29%
Total	100%	100%	100%

Q31. In addition to documenting and practicing your data breach plan, does your organization take any of the following additional steps to prepare?	FY2018	FY2017	FY2016
Conduct third-party cyber security assessments	54%	48%	51%
Integrate data breach response into business continuity plans	52%	51%	46%
Create a “standby website” for content that can be made live when an incident occurs	31%	33%	35%
Regularly review physical security and access to confidential information	70%	65%	67%
Meet with law enforcement and/or state regulators in advance of an incident	16%	13%	12%
Subscribe to a dark web monitoring service	19%	21%	15%
Conduct background checks on new full time employees and vendors	65%	62%	59%
Total	307%	293%	285%

Q32. Does your data breach response plan include the following requirements? Please select all that apply.	FY2018	FY2017	FY2016
Required C-level approval of the data breach response plan	79%	75%	70%
Contact information for all members of the data breach response team	95%	94%	98%
Contact information for all members of the data breach backup response team	44%	40%	41%
Procedures for communicating with employees when a data breach occurs	56%	55%	53%
Procedures for responding to a data breach involving overseas locations	46%	41%	35%
Procedures for communicating with state attorneys general and regulators	67%	69%	66%
Procedures for communications with investors	52%	50%	42%
Procedures for communications with business partners and other third parties	50%	46%	41%
Review of a third party or business partner's incident response plan	36%	32%	28%
Procedures for determining and offering identity theft protection services	37%	39%	40%
Procedures for reporting results of the forensics investigation to senior management	33%	28%	23%
Procedures for incorporating findings from the forensics investigations into the security strategy	31%	28%	25%
None of the above	5%	4%	8%
Total	631%	601%	570%

Q33. Does your data breach response plan offer guidance on managing the following security incidents? Please check all that apply.	FY2018	FY2017	FY2016
Loss or theft of payment information, including credit cards	74%	69%	70%
Loss or theft of personally identifiable information	80%	71%	75%
Destructive malware such as ransomware	62%	63%	51%
IoT-based attacks	20%	14%	
Hacktivism/activism	39%	40%	44%
Attacks via the Internet or social media	59%	62%	59%
W-2 and other phishing fraud scams	57%	58%	64%
Distributed denial of service attack (DDoS) that causes a system outage	87%	88%	86%
Loss or theft of information about customer affiliations/associations that would result in damage to your organization's reputation	79%	81%	77%
Loss or theft of intellectual property or confidential business information	73%	69%	63%
Data breach caused by a malicious employee or contractor	61%	62%	55%
Your organization is threatened with extortion as a result of the theft of sensitive and confidential information	55%	60%	50%
Loss or theft of paper documents and tapes containing sensitive and confidential information	34%	36%	38%
None of the above	6%	5%	4%
Total	786%	778%	736%

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.	FY2018	FY2017
1 to 2	35%	38%
3 to 4	26%	30%
5 to 6	19%	15%
7 to 8	12%	10%
9 to 10	8%	7%
Total	100%	100%
Extrapolated value	4.14	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.	FY2018	FY2017	FY2016
1 to 2	11%	10%	13%
3 to 4	12%	15%	17%
5 to 6	25%	26%	28%
7 to 8	32%	30%	26%
9 to 10	20%	19%	16%
Total	100%	100%	100%
Extrapolated value	6.26	6.16	5.80

Q36. How could your data breach response plan become more effective? Please select the top three choices.	FY2018	FY2017	FY2016
Conduct more fire drills to practice data breach response	80%	85%	80%
Have formal documentation of incident response procedures	65%	62%	66%
Incorporate what was learned from previous data breaches	70%	66%	60%
Ensure seamless coordination among all departments involved in incident response	45%	40%	41%
Increase participation and oversight from senior executives	81%	80%	76%
Assign individuals with a high level of expertise in security to the team	78%	75%	71%
Assign individuals with a high level of expertise in compliance with privacy, data protection laws and regulations to the team	47%	48%	50%
Have a budget dedicated to data breach preparedness	63%	60%	63%
Increase involvement of third-party experts	48%	44%	44%
None of the above	3%	2%	0%
Total	580%	562%	551%

Q37a. Does your organization practice responding to a data breach?	FY2018	FY2017	FY2016
Yes	73%	71%	68%
No	27%	29%	32%
Total	100%	100%	100%

Q37b. If yes, how often is the response practiced? Please check all that apply.	FY2018	FY2017	FY2016
At least twice a year	50%	44%	39%
Once each year	16%	19%	18%
Every two years	5%	4%	5%
More than two years	7%	9%	12%
Never	0%	0%	
No set schedule	22%	24%	26%
Total	100%	100%	100%

Q37c. If yes, what is included in the practice response? Please check all that apply.	FY2018	FY2017	FY2016
Fire drills	67%	65%	60%
Case discussions	49%	46%	45%
Training and awareness about security threats facing the organization	71%	68%	65%
Review of the plan by the person/function most responsible for data breach response	80%	77%	73%
Review of data breach communications plans	50%	52%	51%
Review of what was learned from previous data breaches or other security incidents	79%	75%	72%
None of the above	9%	11%	14%
Other	3%	4%	3%
Total	408%	398%	383%

Q37d. If no, why not? Please check all that apply.	FY2018	FY2017	FY2016
Not enough budget	33%	37%	39%
We are confident in our ability to respond to a data breach	40%	45%	46%
Too difficult to schedule a practice response	78%	73%	76%
Not a priority	57%	61%	64%
Total	208%	216%	225%

Q38a. Does your incident response plan include processes to manage an international data breach?	FY2018	FY2017	FY2016
Yes	59%	54%	51%
No	37%	41%	42%
Unsure	4%	5%	7%
Total	100%	100%	100%

Q38b. If yes, is your organization's plan specific to each location where it operates?	FY2018	FY2017
Yes	51%	50%
No	45%	46%
Unsure	4%	4%
Total	100%	100%

Q39. How confident is your organization in its ability to deal with an international data breach?	FY2018	FY2017	FY2016
Very confident	12%	11%	13%
Confident	17%	17%	18%
Somewhat confident	28%	26%	25%
Not confident	33%	34%	31%
No confidence	10%	12%	13%
Total	100%	100%	100%

Q40. Is your company subject to GDPR?	FY2018
Yes	86%
Unsure	8%
No	6%
Total	100%

Q41. If yes, Using the following 10-point scale, please rate your organization's ability to comply with the GDPR. 1 = No ability to 10 = high ability	FY2018
1 to 2	14%
3 to 4	25%
5 to 6	25%
7 to 8	21%
9 to 10	15%
Total	100%
Extrapolated value	5.46

Q42a. If yes, how effective is your organization in complying with the GDPR's data breach notification rules? According to the Notice rule, in the event of a personal data breach, the organization must notify the supervisory authority within 72 hours. If there is a delay, the controller must provide a "reasoned justification." Please use the following scale 1 = low effectiveness to 10 = high effectiveness	FY2018
1 to 2	20%
3 to 4	33%
5 to 6	24%
7 to 8	14%
9 to 10	9%
Total	100%
Extrapolated value	4.68

Q42b. If you rated your effectiveness 7 or higher to comply with the GDPR's data breach notification rules, why is your organization effective?	FY2018
Our organization has the necessary security technologies in place to be able to detect the occurrence of a data breach quickly	54%
Our organization's incident response plan has proven to be effective in providing timely notification	38%
Our organization is able to provide notification to the data protection authority within 72 hours	22%
Our organization would be able to determine quickly if the breach is unlikely to result in a "risk for the rights and freedoms of natural persons"	45%
Other (please specify)	3%
Total	162%

Part 4. Organizational characteristics & respondent demographics

D1. What organizational level best describes your current position?	FY2018	FY2017	FY2016
Senior Executive	8%	7%	9%
Vice President	11%	10%	8%
Director	24%	25%	27%
Manager	25%	26%	23%
Supervisor	17%	18%	18%
Technician	8%	7%	9%
Staff	5%	6%	5%
Contractor	1%	1%	0%
Other	1%	0%	1%
Total	100%	100%	100%

D2. Check the **Primary Person** you report to within your organization.	FY2018	FY2017	FY2016
CEO/Executive Committee	5%	5%	4%
Chief Financial Officer	3%	4%	5%
General Counsel	11%	12%	11%
Chief Privacy Officer	9%	10%	9%
Chief Information Officer	15%	15%	15%
Compliance Officer	21%	19%	21%
Human Resources VP	1%	0%	1%
Chief Security Officer	3%	3%	4%
Chief Risk Officer	10%	10%	8%
Chief Information Security Officer	20%	21%	20%
Other	2%	1%	2%
Total	100%	100%	100%

D3. What industry best describes your organization's industry focus?	FY2018	FY2017	FY2016
Agriculture & food service	1%	1%	0%
Communications	2%	2%	3%
Consumer products	6%	5%	5%
Defense & aerospace	1%	0%	0%
Education & research	2%	1%	2%
Energy & utilities	7%	6%	5%
Entertainment & media	2%	3%	2%
Financial services	17%	18%	19%
Health & pharmaceutical	11%	11%	10%
Hospitality	1%	1%	2%
Industrial/manufacturing	10%	11%	8%
Public sector	11%	10%	12%
Retailing	8%	9%	9%
Services	9%	9%	9%
Technology & software	8%	8%	9%
Transportation	2%	2%	3%
Other	2%	3%	2%
Total	100%	100%	100%

D4. What is the worldwide headcount of your organization?	FY2018	FY2017	FY2016
Less than 500	10%	11%	12%
500 to 1,000	19%	18%	19%
1,001 to 5,000	26%	24%	25%
5,001 to 25,000	20%	22%	20%
25,001 to 75,000	18%	17%	16%
More than 75,000	7%	8%	8%
Total	100%	100%	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.

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.