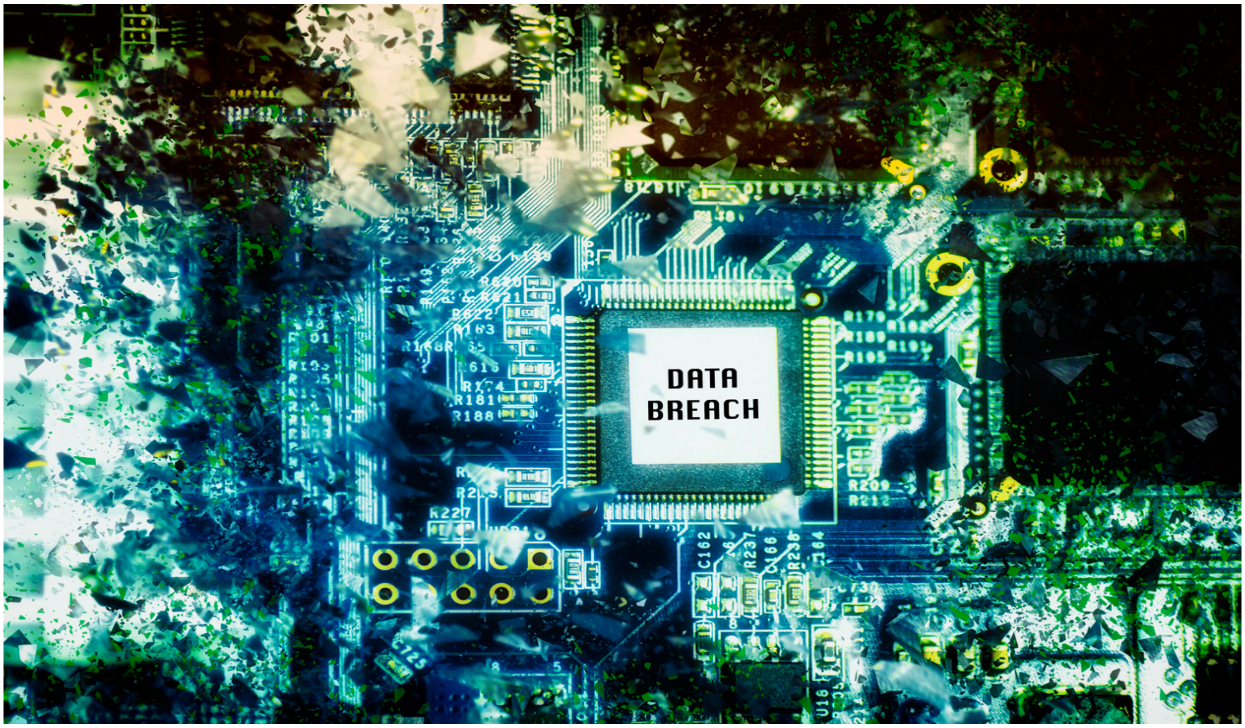


Seventh Annual Study: Is Your Company Ready for a Big Data Breach?

Sponsored by Experian® Data Breach Resolution

Independently conducted by Ponemon Institute LLC

Publication Date: February 2020

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

Ponemon Institute, February 2020

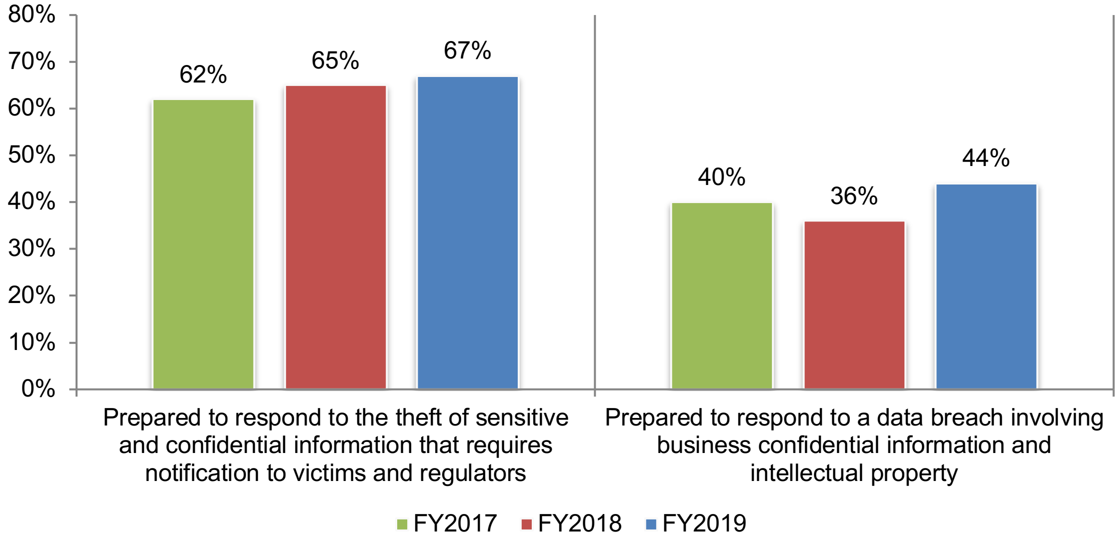
Part 1. Introduction

The *Seventh Annual Study: Is Your Company Ready for a Big Data Breach?* sponsored by Experian® Data Breach Resolution and conducted by Ponemon Institute tracks the steps companies are taking, or not taking, to respond to a data breach. According to the findings, since 2017 significantly more organizations are having data breaches, highlighting the importance of being prepared.

This year, we surveyed 650 professionals in the United States 456 in EMEA[1]. A comparison of the US and EMEA findings are presented in Part 3 of this report. All respondents work in IT and IT security, compliance and privacy and are involved in data breach response plans in their organizations. In the context of this research, we define a data breach as the loss or theft of information assets, including intellectual property such as trade secrets, contact lists, business plans and source code. Data breaches happen for various reasons including human errors and system glitches. They also happen as a result of malicious attacks, hactivism or criminal attacks that seek to obtain valuable data, disrupt business operation or tarnish reputation.

Organizations are challenged to respond to the loss or theft of confidential business information and intellectual property. Sixty-seven percent of respondents say their organizations are most concerned about the loss or theft of intellectual property. However, as shown in Figure 1, since 2017 the ability to respond to a data breach involving this type of information has not improved significantly. Organizations are better able to respond to breaches that require notification to victims and regulators.

Figure 1. Trends in the ability to respond to a data breach?
Strongly agree and Agree responses combined



[1] Countries included in the EMEA cluster: United Kingdom, France, Germany, Benelux, Nordics, UAE and Saudi Arabia

In this year's research, we introduced the following new topics:

- The maturity of organizations' privacy and data protection program
- The frequency, consequences and preparedness to deal with spear phishing attacks
- The frequency, consequences and preparedness to deal with ransomware
- The impact of the General Data Protection Regulation (GDPR) and the California Consumer Privacy Act (CCPA) on data breach preparedness

The following findings describe organizations' abilities to respond to a big data breach

Investments in security technologies are increasing to improve the ability to determine and respond quickly to a data breach. More data breaches are occurring. As a result, 68 percent of respondents say their organizations have increased their investments in security technologies in order to be able to detect and respond quickly to a data breach.

C-suite executives are more knowledgeable than the board of directors about data breach preparedness plans. The C-suite's knowledge about the data breach preparedness plans is much higher than the board of directors (55 percent of respondents vs. 40 percent of respondents).

Most training and awareness programs are conducted when employees are hired. Seventy-two percent of respondents have a privacy and training program for employees and other stakeholders who have access to sensitive or confidential information. Almost half (49 percent of respondents) say training is conducted during the on-boarding of new employees.

Cyber insurance coverage is focused on attacks by cyber criminals and malicious or criminal insiders. About half of respondents (49 percent) say their organizations have a data breach and cyber insurance policy. Of the 51 percent of respondents who currently do not have a cyber insurance policy, 58 percent will purchase one within the next two years. Eighty-three percent of respondents say it covers incidents caused by cyber criminals and 65 percent of respondents say it covers malicious or criminal insiders. Only 38 percent of respondents say it covers human error, one of the major causes of a data breach.

Since 2017, the coverage of identity protection services to victims has increased significantly. The top areas of coverage are legal defense costs and identity protection and notification costs to data breach victims. Seventy-two percent of respondents say identity protection services are covered, an increase from 64 percent in 2017.

The primary benefit of sharing information about data breach experiences and incident response plans is collaborating with peers. Fifty-seven percent of respondents currently or are planning to participate in a sharing program about data breaches and incident response plans. The primary benefit is that it fosters collaboration among peers and industry groups.

Effectiveness of data breach response plans continues to improve. Since 2017, more respondents say their data breach response plans are very or highly effective. An increase from 49 percent of respondents to 57 percent of respondents. However, 66 percent of respondents say their organizations have not reviewed or updated the plan since it was put in place or have not set a specific time to review and update the plan. Only 26 percent of respondents say it is reviewed annually.

The majority of organizations practice responding to a data breach. Seventy-five percent of respondents say they practice their ability to respond to a data breach. Of these, 45 percent of respondents say they do this twice per year.

More organizations are regularly reviewing physical security and access to confidential information. The primary steps being taken to prepare for a data breach are regular reviews of physical security and access to confidential information (73 percent of respondents) and conducting background checks on new full-time employees and vendors (69 percent of respondents).

Organizations are not confident in their ability to minimize reputational consequences and prevent the loss of customers. To prevent the loss of customers, 62 percent of respondents believe credit monitoring protection for victims is the best protection for consumers and the most effective in keeping customers. However, only 23 percent of respondents say their organization is confident in its ability to minimize the financial and reputational consequences of a material data breach and only 38 percent of respondents say they are 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.

Spear phishing attacks are pervasive and confidence in dealing with them is declining. Sixty-nine percent of respondents had one or more spear phishing attacks and 67 percent of respondents say the negative consequences of these attacks was very significant or significant. Despite the frequency of these attacks, 50 percent of respondents do not train their employees to recognize and minimize spear phishing incidents. Since 2017, respondents who say their organizations are very confident or confident in their ability to deal with spear phishing attacks has declined from 31 percent to 23 percent.

Respondents are even less confident in their ability to deal with ransomware. Only 20 percent of respondents are very confident in their ability. Thirty-six percent of respondents say their organizations had a ransomware attack. The average ransom was $6,128 and 68 percent of respondents say it was paid.

More breaches are international or global in scope and only 34 percent of respondents say they are confident in their organizations' ability to respond to these breaches. As discussed previously, 63 percent of respondents say their organization had a data breach in the past two years. Forty-five percent of respondents say one more of these breaches were global. Since 2017, respondents reporting that their incident response plan includes processes to manage an international data breach increased significantly from 54 percent to 64 percent. Fifty-seven percent say the plan is specific to each location it operates.

Now that the General Data Protection Regulation (GDPR) has been in effect for more than a year, organizations have improved their ability to comply with it. Fifty-four percent of respondents say they have a high or very high ability to comply with the regulation (an increase from 36 percent) and 50 percent of respondents have a high or very high effectiveness in complying with the data breach notification rules (an increase from 23 percent). Having the necessary security technologies in place to detect the occurrence of a data breach quickly is the number one reason for being effective.

CCPA results in organizations having to make comprehensive changes in business practices. Fifty-six percent of respondents say they are aware of the CCPA and of these respondents, 47 percent of respondents say they are subject to the Act. The top two challenges to compliance with the CCPA are similar to achieving compliance with the GDPR, which are the need to change business practices and not enough budget to hire additional staff.

Lessons learned from organizations with a mature privacy and data protection program

The report presents a special analysis on how the maturity of organizations' privacy and data protection programs can affect data breach preparedness. Nineteen percent of respondents self-reported that their organization have a mature program, which means that activities are fully defined, maintained across the enterprise and measured with KPIs. In addition, C-level executives are regularly informed about the program's effectiveness. The following findings are persuasive in showing how making the needed investments to achieve maturity will improve data breach preparedness.

- Mature privacy and data protection programs have fewer data breaches. Fifty-five percent of respondents in mature programs say their organizations had a data breach in the past two years. In contrast, a minimum of 60 percent of respondents in the other levels of maturity report having a data breach.

- Mature programs are more adept at preventing negative public opinion and media coverage. Fifty-five percent of respondents say they are effective in managing the risk of negative opinions and media coverage following a material data breach. In contrast, only 37 percent of respondents in programs that are in the middle stage say they are effective.

- More mature programs represented in this study are increasing investments in security technologies to be able to detect and respond quickly to a data breach.

- Mature programs are more likely to participate in sharing information about their data breach and incident response experiences with government and industry peers.

- Mature programs are better prepared to manage an international data breach. Seventy-one percent of respondents in mature programs say their incident response plan includes processes to manage an international data breach.

Part 2. Key findings

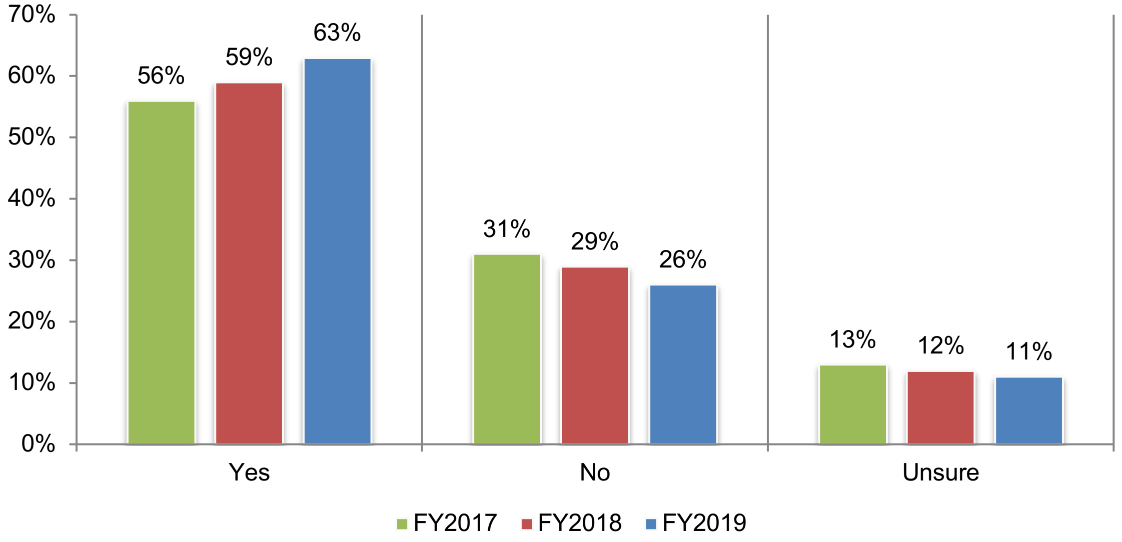
In this section, we provide an analysis of the US results over the past two to three years as shown. The complete audited findings are presented in the Appendix of this report. We have organized this report according to the following topics. Part 3 of the report presents the differences between the US and EMEA.

- How organizations are preparing for a data breach
- Data breach response plans
- Steps to maintain customer loyalty following a data breach
- Ransomware, phishing and IoT increase the likelihood of a data breach
- Data breaches have no boundaries
- Regulations that affect data breach preparedness
- Lessons learned from organizations with mature privacy and data protection program

How organizations are preparing for a data breach

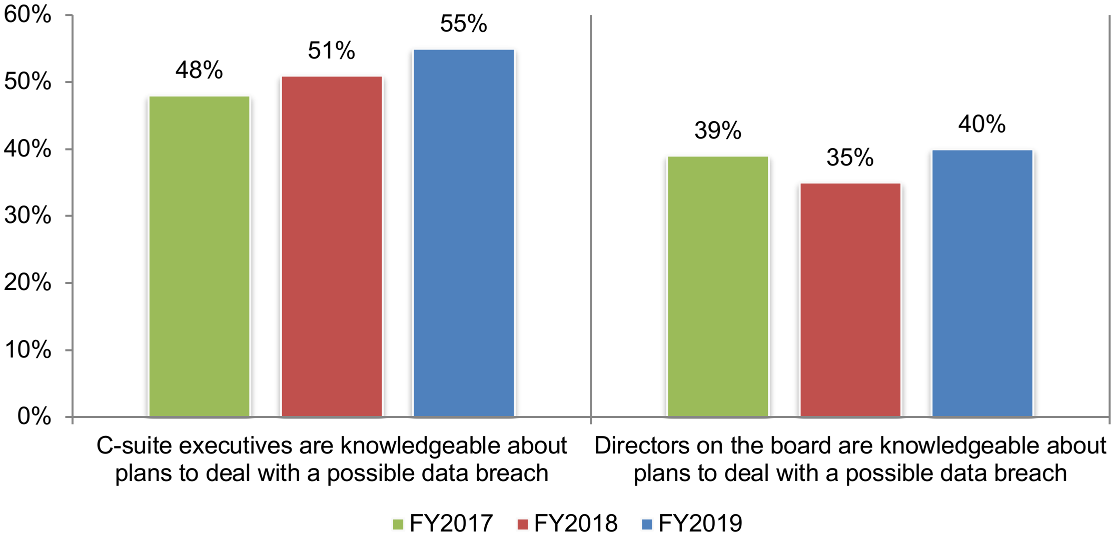
Investments in security technologies are increasing to improve the ability to determine and respond quickly to a data breach. Sixty-eight percent of respondents say their organizations have increased their investments in security technologies in order to be able to detect and respond quickly to a data breach. As shown in Figure 1, more respondents are reporting that their organizations have had a data breach involving the loss or theft of more than 1,000 records in the past two years.

Figure 2. Did your organization have a data breach involving the loss or theft of more than 1,000 records containing sensitive or confidential information in the past two years?



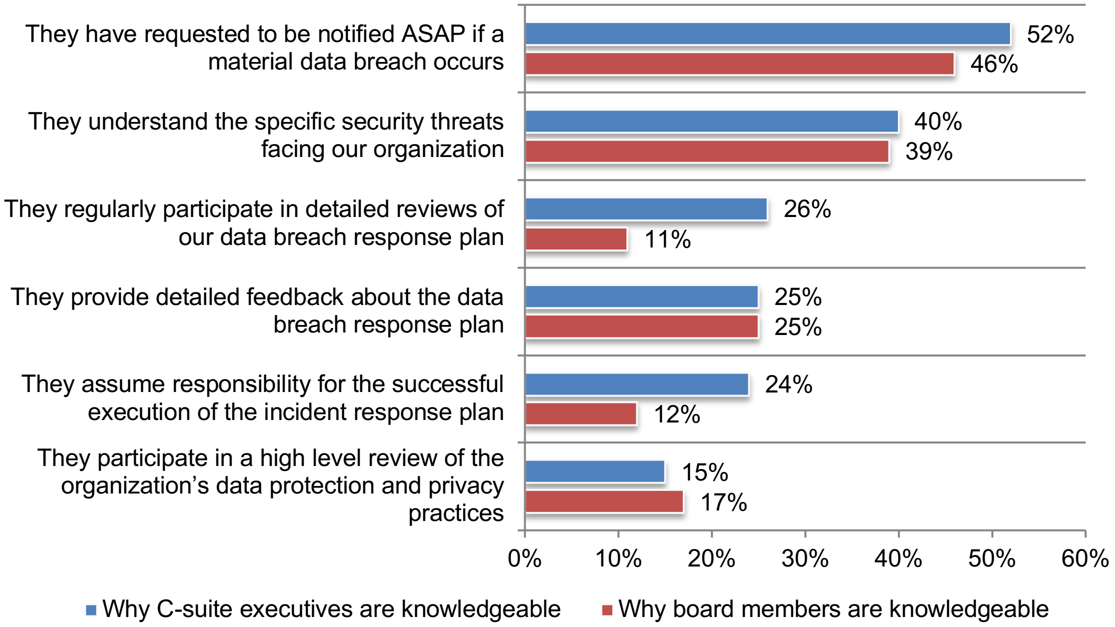
C-suite executives are more knowledgeable than the board of directors about data breach preparedness plans. According to Figure 3, the C-suite's knowledge about the data breach preparedness plans is much higher than the board of directors (55 percent of respondents vs. 40 percent of respondents).

Figure 3. Do you believe your company's C-suite executives and board of directors are knowledgeable about your organization's data breach preparedness plans?
Yes responses presented



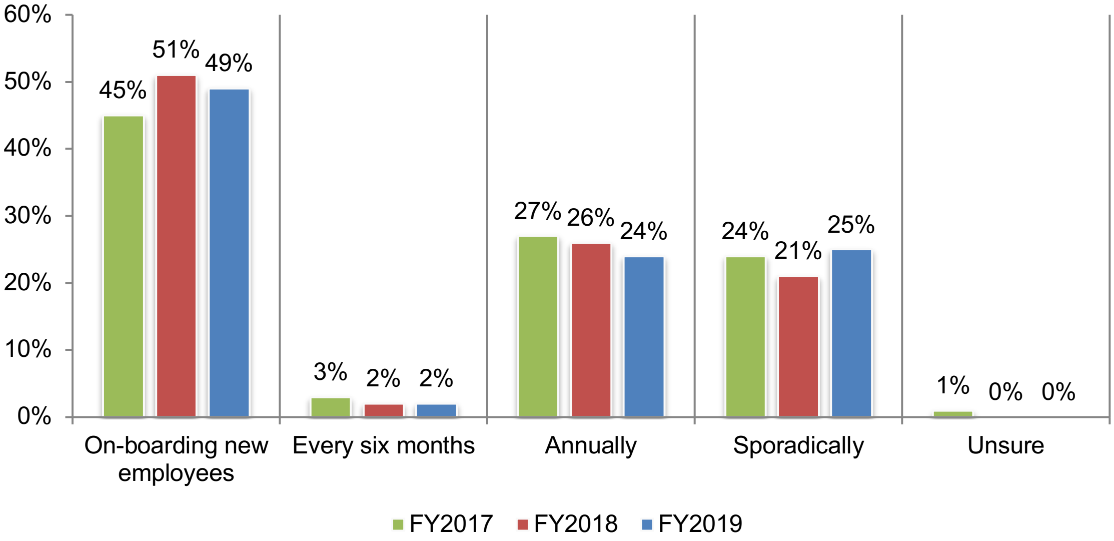
Indications of knowledge are presented in Figure 4. The top two indications are requests to be notified ASAP if a material data breach occurs and an understanding of the specific security threats facing our organization.

Figure 4. Why do you believe your company's C-suite and board of directors are knowledgeable?
More than one response permitted



Most training and awareness programs are conducted when employees are hired. Seventy-two percent of respondents have a privacy and training program for employees and other stakeholders who have access to sensitive or confidential information. As shown in Figure 5, there has been little change in how organizations are scheduling their privacy and data protection awareness training programs. Almost half (49 percent of respondents) say training is conducted during the on-boarding of new employees.

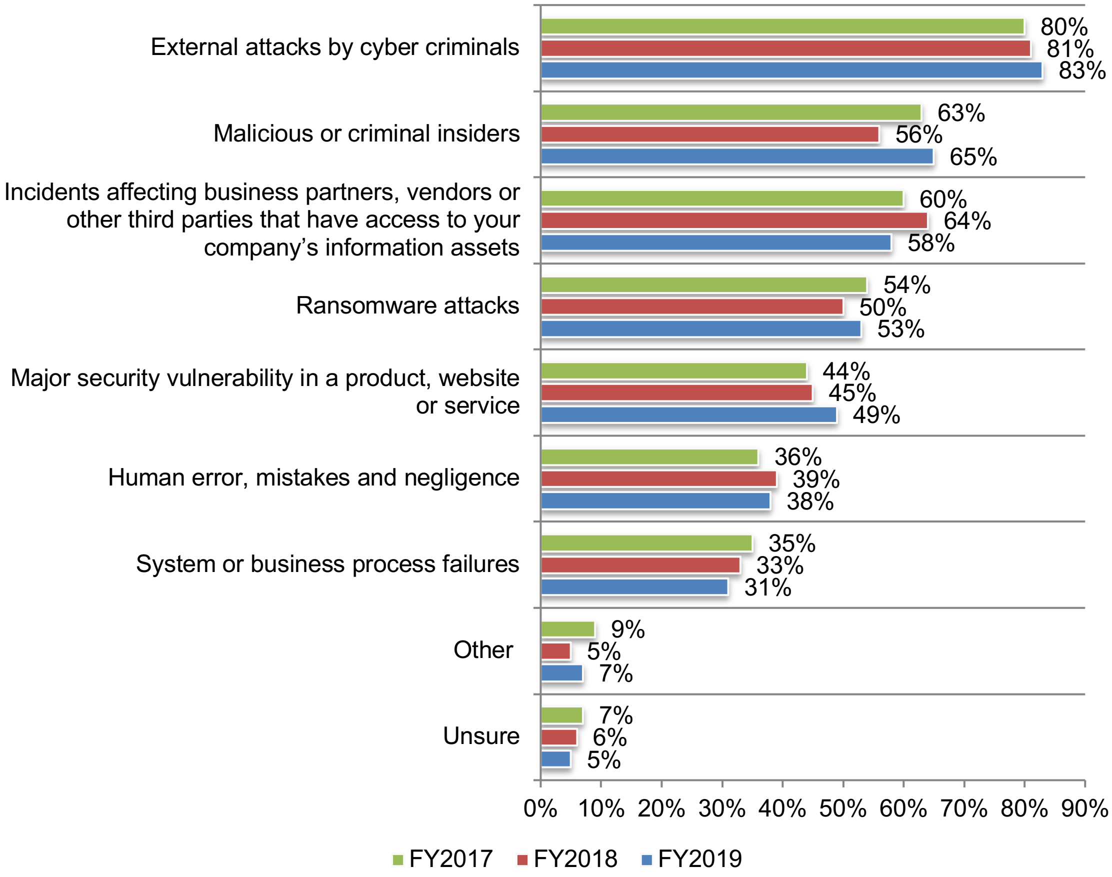
Figure 5. How often are privacy and data protection awareness training programs conducted?



Cyber insurance coverage is focused on attacks by cyber criminals and malicious or criminal insiders. About half of respondents (49 percent) say their organizations have a data breach and cyber insurance policy. Of the 51 percent of respondents who currently do not have a cyber insurance policy, 58 percent will purchase one within the next two years.

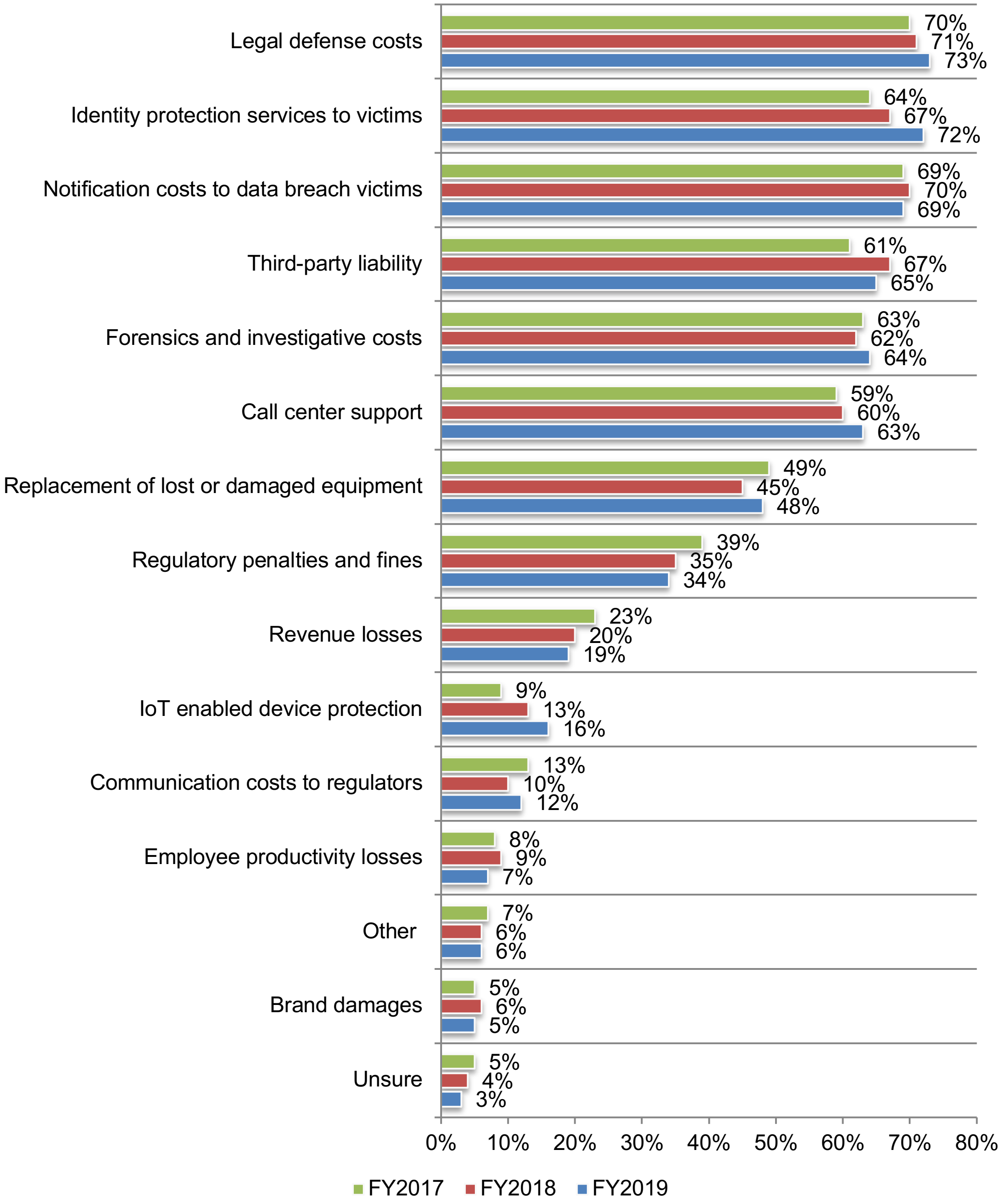
According to Figure 6, 83 percent of respondents say it covers incidents caused by cyber criminals and 65 percent of respondents say it covers malicious or criminal insiders. Only 38 percent of respondents say it covers human error, one of the major causes of a data breach.

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



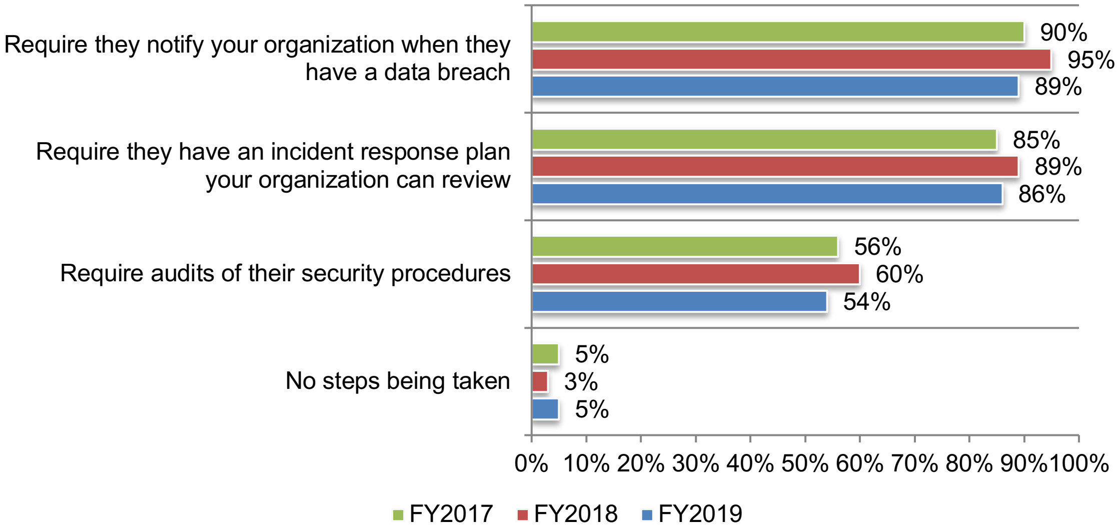
Since 2017, the coverage of identity protection services to victims has increased significantly. Figure 7 presents the coverage provided by the cyber insurance policy. The top areas of coverage are legal defense costs and identity protection and notification costs to data breach victims.

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



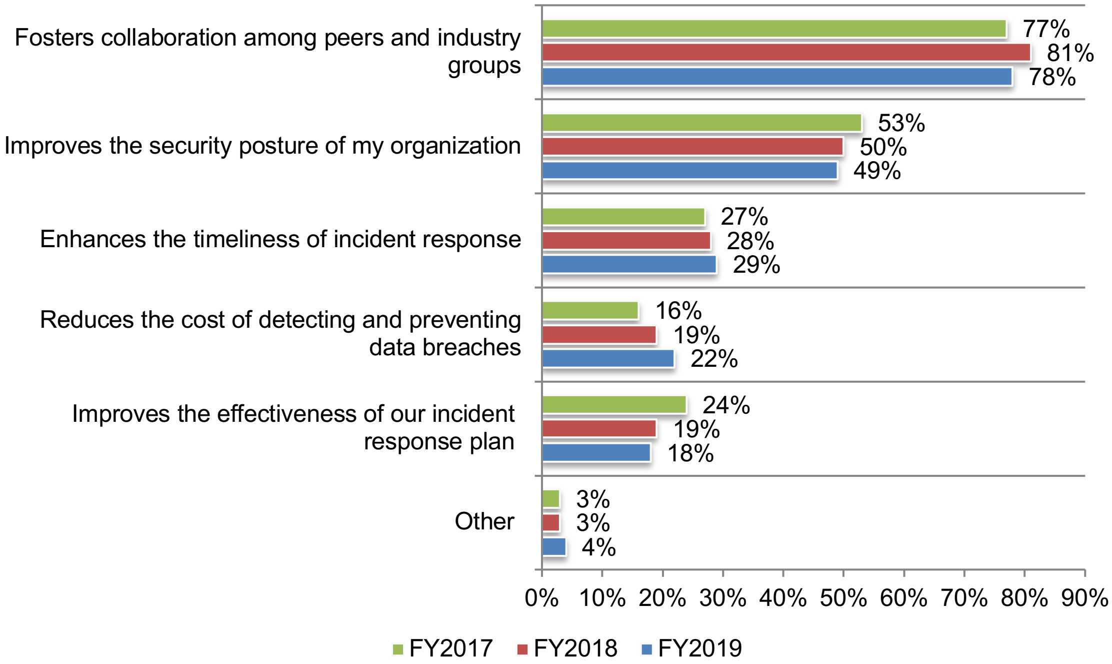
Organizations require data breach notification and incident response plans to minimize the consequences of a third-party data breach. According to Figure 8, consistent with previous years 89 percent of respondents say their organizations require third parties to notify them when they have a data breach and 86 percent of respondents say they require an incident response plan they can review.

Figure 8. What steps do you take to minimize the consequences of a data breach involving a third party?
More than one response permitted



The primary benefit of sharing information about data breach experiences and incident response plans is collaborating with peers. Fifty-seven percent of respondents currently or are planning to participate in a sharing program about data breaches and incident response plans. The primary benefit is that it fosters collaboration among peers and industry groups, as shown in Figure 9.

Figure 9. What are the reasons for sharing information about your organization's data breach experience and incident response plan?
More than one response permitted

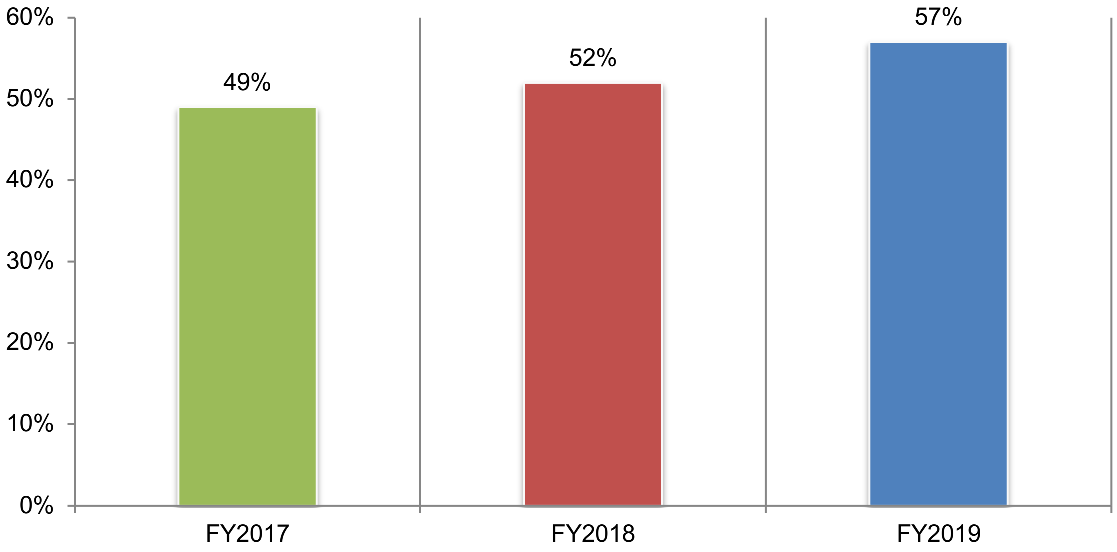


Data breach response plans

Effectiveness of data breach response plans continue to improve. Ninety-four percent of respondents have a data breach response plan. Organizations that don't have a plan cite the reasons as not having the resources or it is outsourced to consultants.

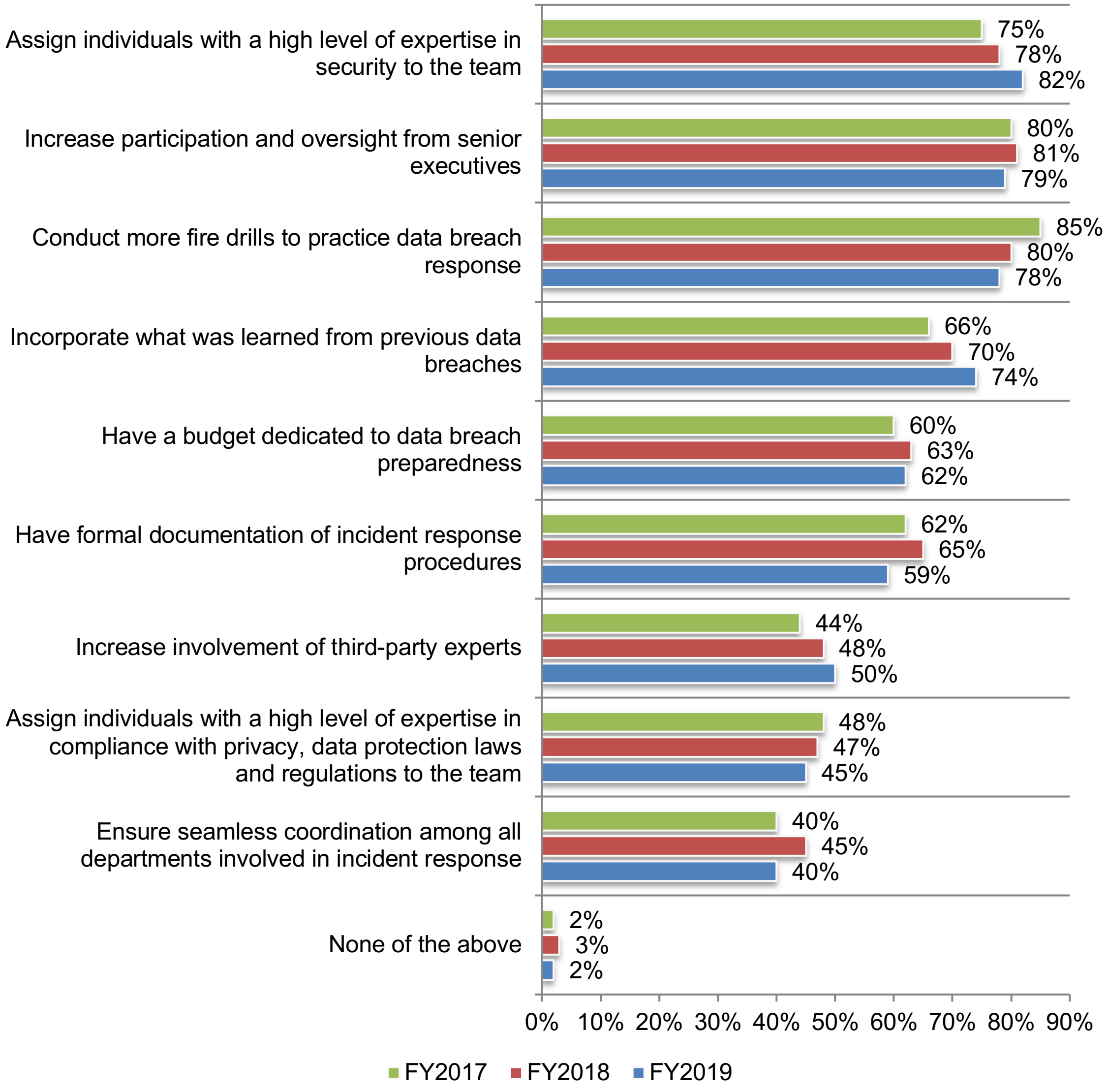
Respondents were asked to rate the effectiveness of their data breach response plans on a scale of 1 = low effectiveness to 10 = high effectiveness. Figure 10 presents the 7 + (highly effective) respondents. As shown, since 2017 effectiveness increased significantly from 49 percent of respondents to 57 percent of respondents.

Figure 10. How effective is your organization's data breach response plan?
On a scale of 1 = low effectiveness to 10 = high effectiveness, 7+ responses presented



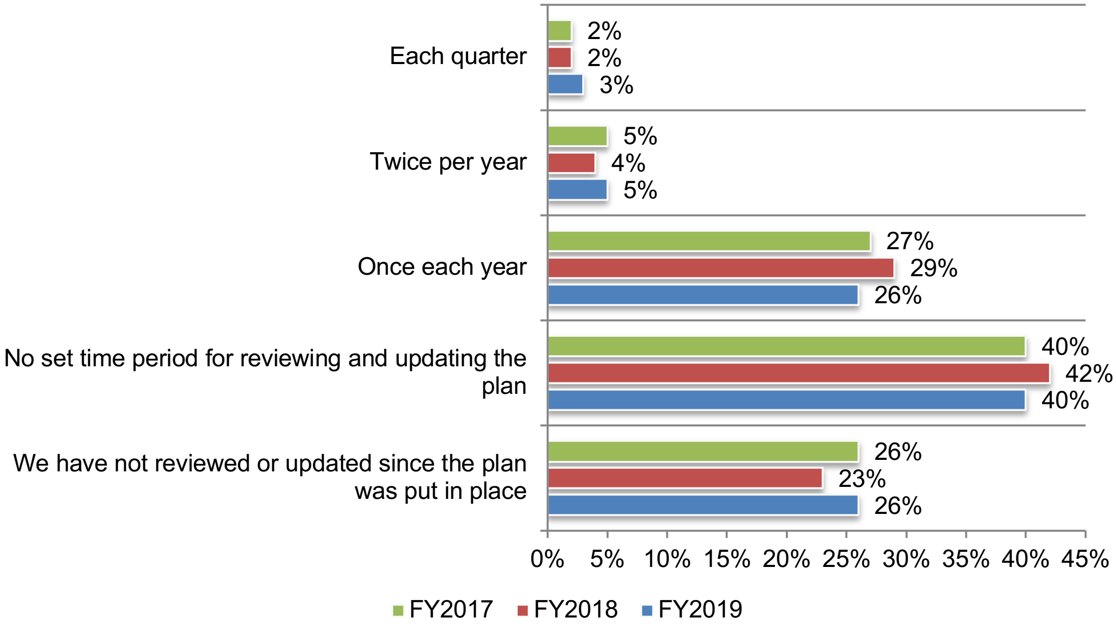
Expertise and senior executive participation and oversight improve the effectiveness of data breach response plans. We asked organizations with a data breach response plan how they could become more effective. According to Figure 11, since 2017 incorporation of what was learned from previous data breaches has increased significantly from 66 percent of respondents to 74 percent of respondents. The top two reasons are to assign individuals with a high level of security expertise to the incident response team and to increase participation and oversight from senior executives.

Figure 11. How could your data breach response plan become more effective?
More than one response permitted



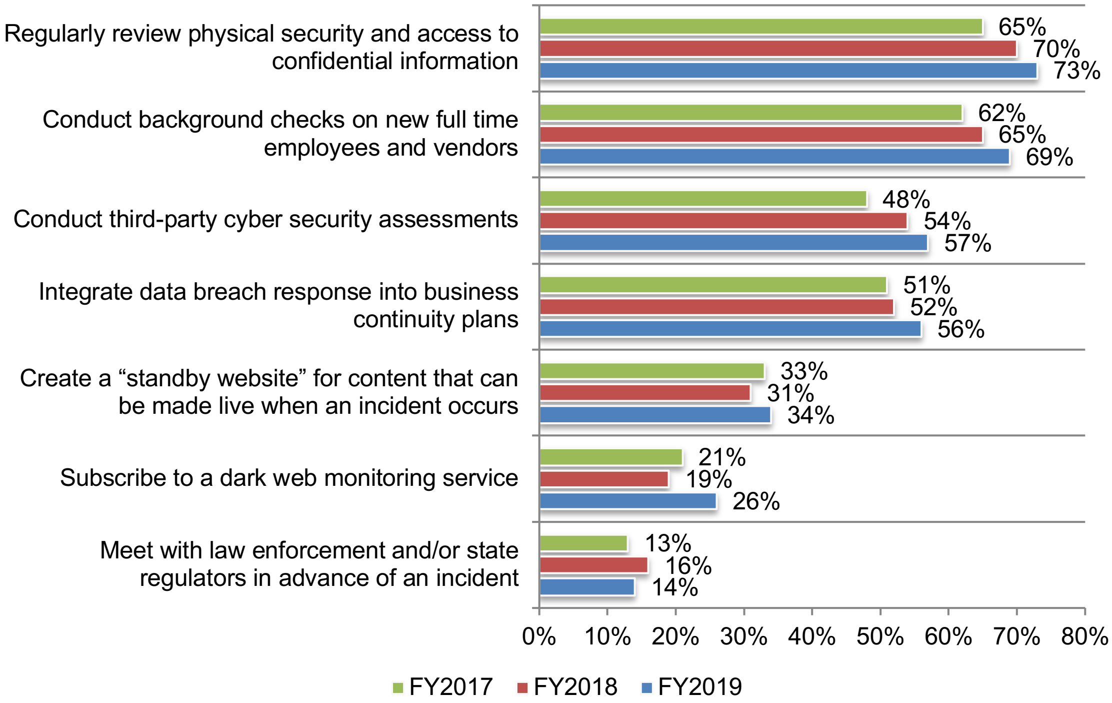
Data breach response plans are not regularly updated. As shown in Figure 12, 66 percent of respondents say their organizations have not reviewed or updated the plan since it was put in place (26 percent) or have not set a specific time to review and update the plan (40 percent). Only 26 percent of respondents say it is reviewed annually.

Figure 12. How often does your company update the data breach response plan?



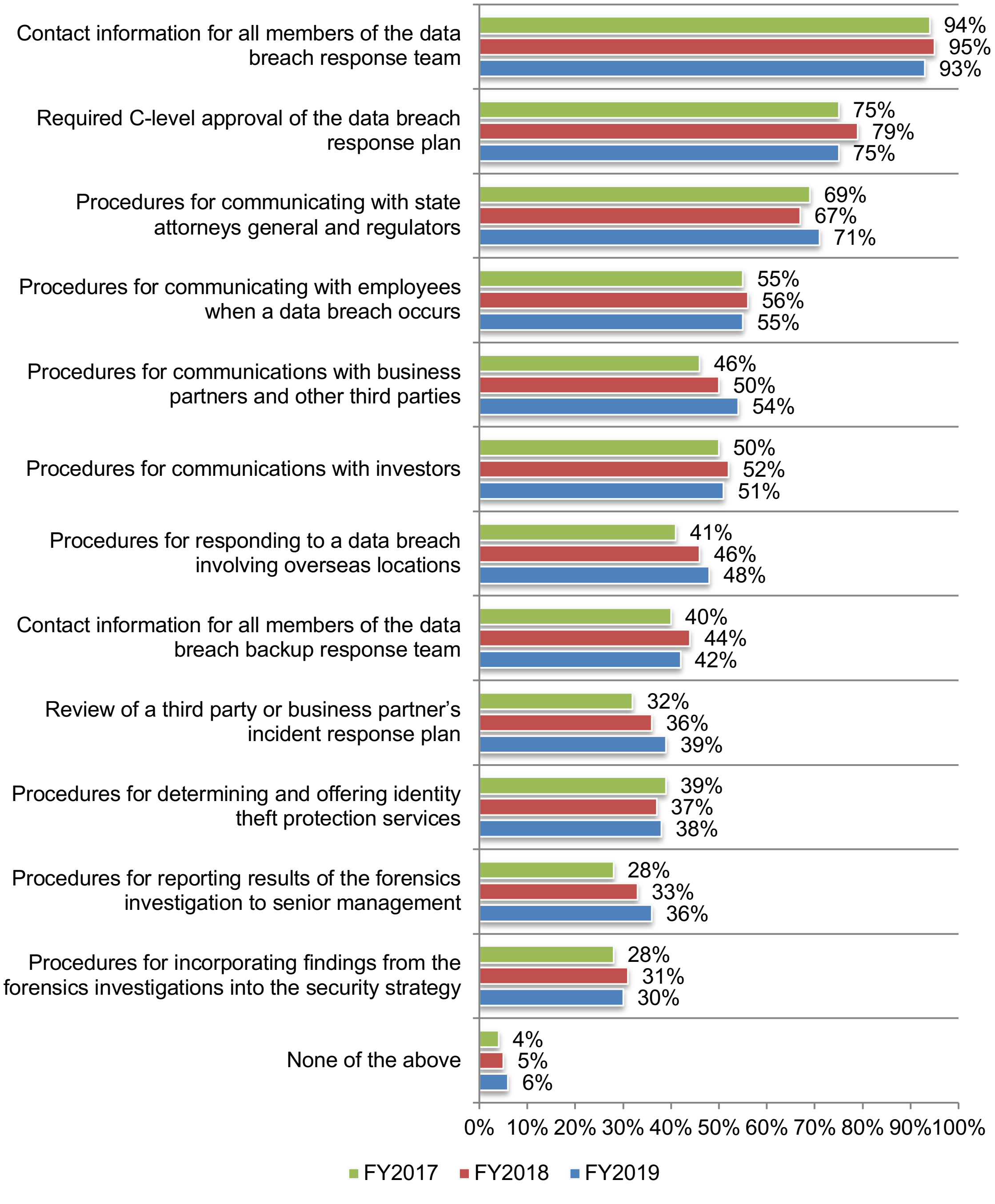
More organizations are regularly reviewing physical security and access to confidential information. According to Figure 13, the primary steps being taken to prepare for a data breach are regular reviews of physical security and access to confidential information (73 percent of respondents) and conducting background checks on new full-time employees and vendors (69 percent of respondents).

Figure 13. Does your organization take any of the following steps to prepare for a data breach?
More than one response permitted



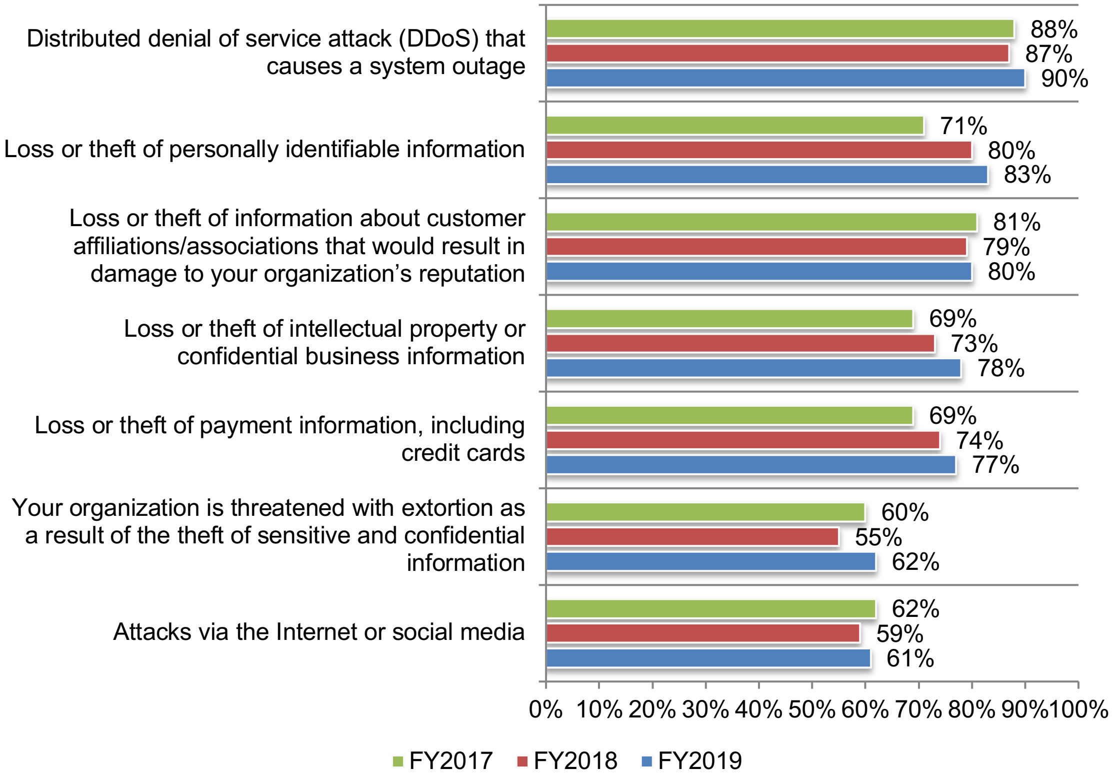
Consistent with previous years, contact information and C-level approval of the data breach response plan are the two primary steps included in the data breach response plan.

Figure 14. Does your data breach response plan include the following steps?
More than one response permitted



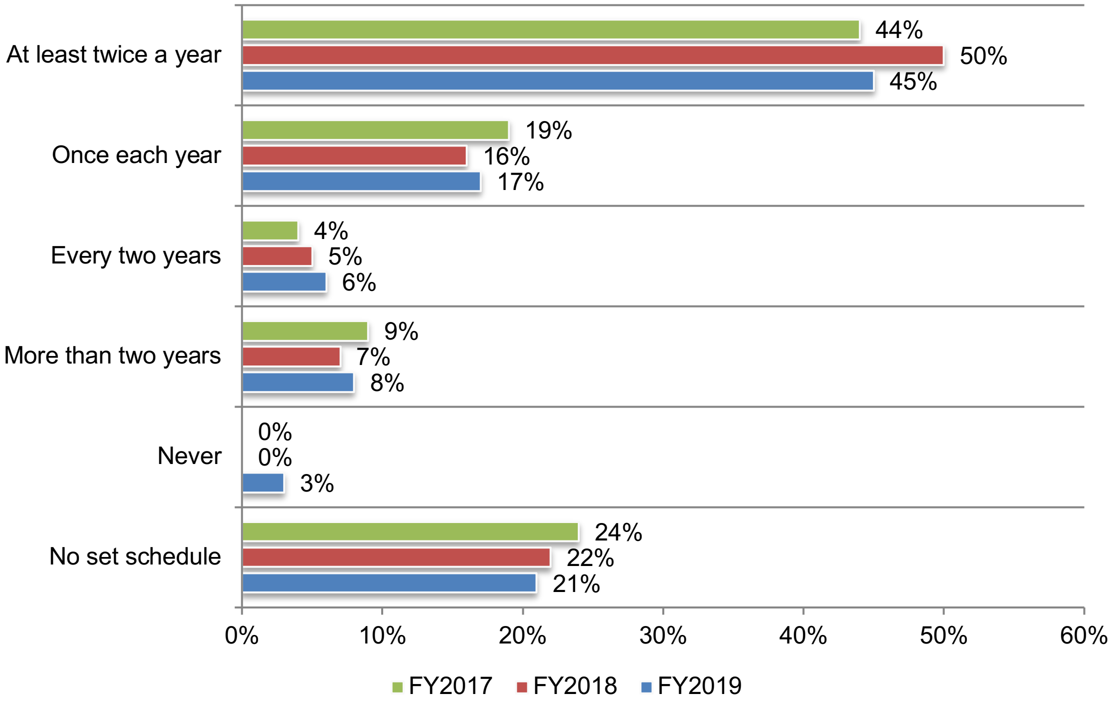
More organizations' data breach response plans offer guidance on the loss or theft of personally identifiable information. According to Figure 15, since 2017 the percentage of organizations represented in the research that offer guidance of the loss or theft of personally identifiable information has increased significantly from 71 percent to 83 percent. More organizations are including guidance on the loss or theft of intellectual property or confidential business information.

Figure 15. Does your data breach response plan offer guidance on managing the following security incidents?
More than one response permitted



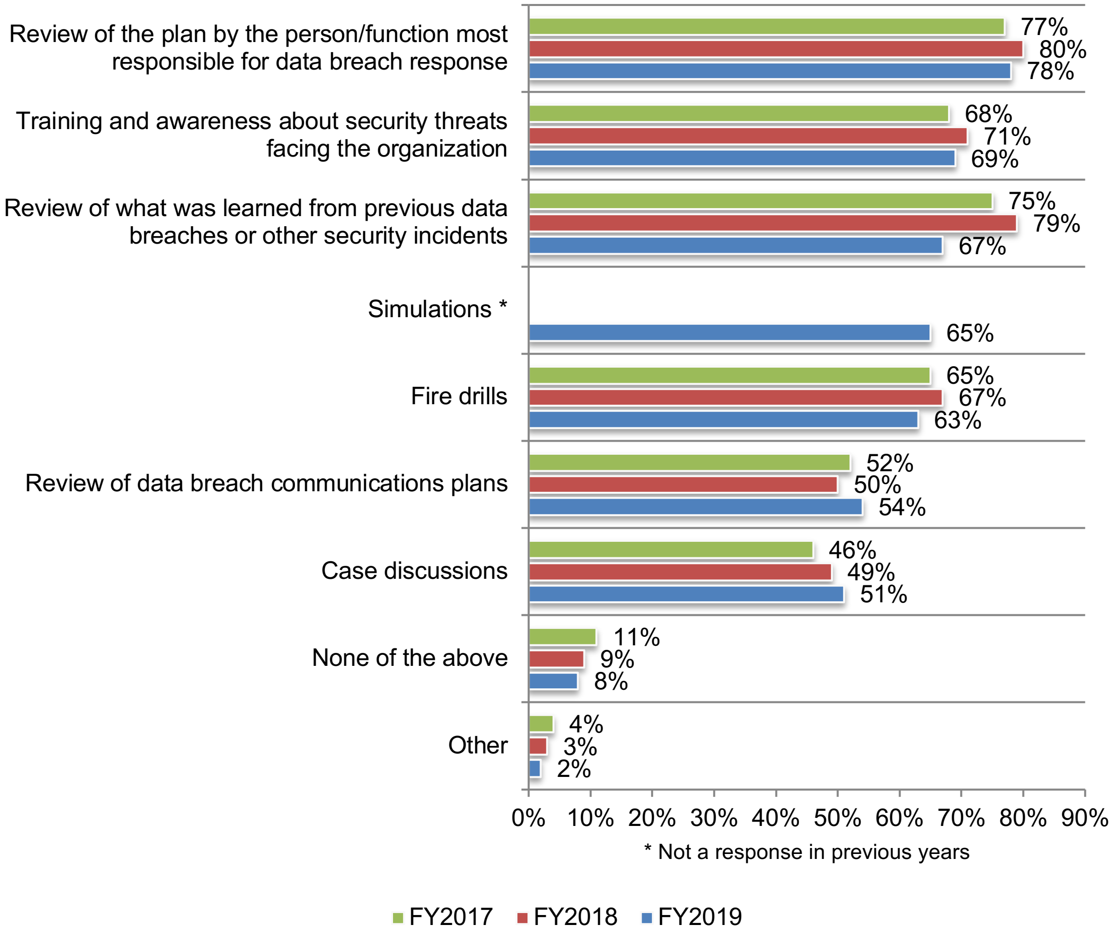
The majority of organizations (75 percent of respondents) practice responding to a data breach. As shown in Figure 16, of these respondents, 45 percent say they practice at least twice a year. This is consistent with previous studies.

Figure 16. Trends in practicing response plans



For the first time respondents were asked if they include simulations when practicing data breach plans. According to Figure 17, 65 percent of respondents say their organizations practice simulations. The top two steps are a review of the plan by the person or function most responsible for data breach response and training and awareness about security threats facing the organization.

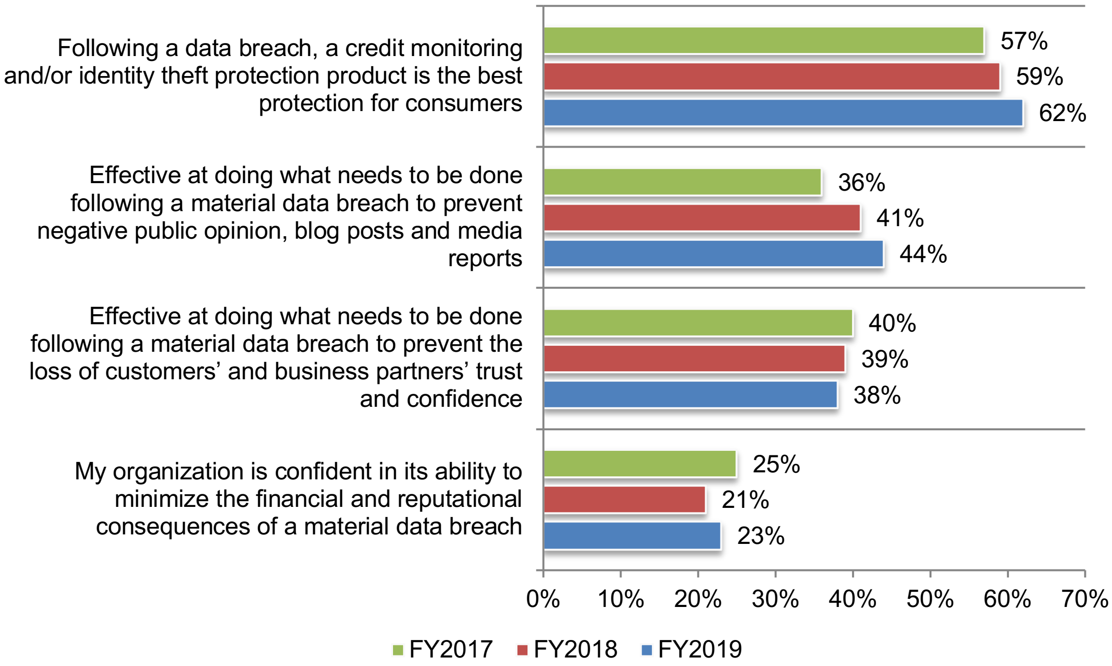
Figure 17. What steps are included in the practice response?



Maintaining customer loyalty following a data breach

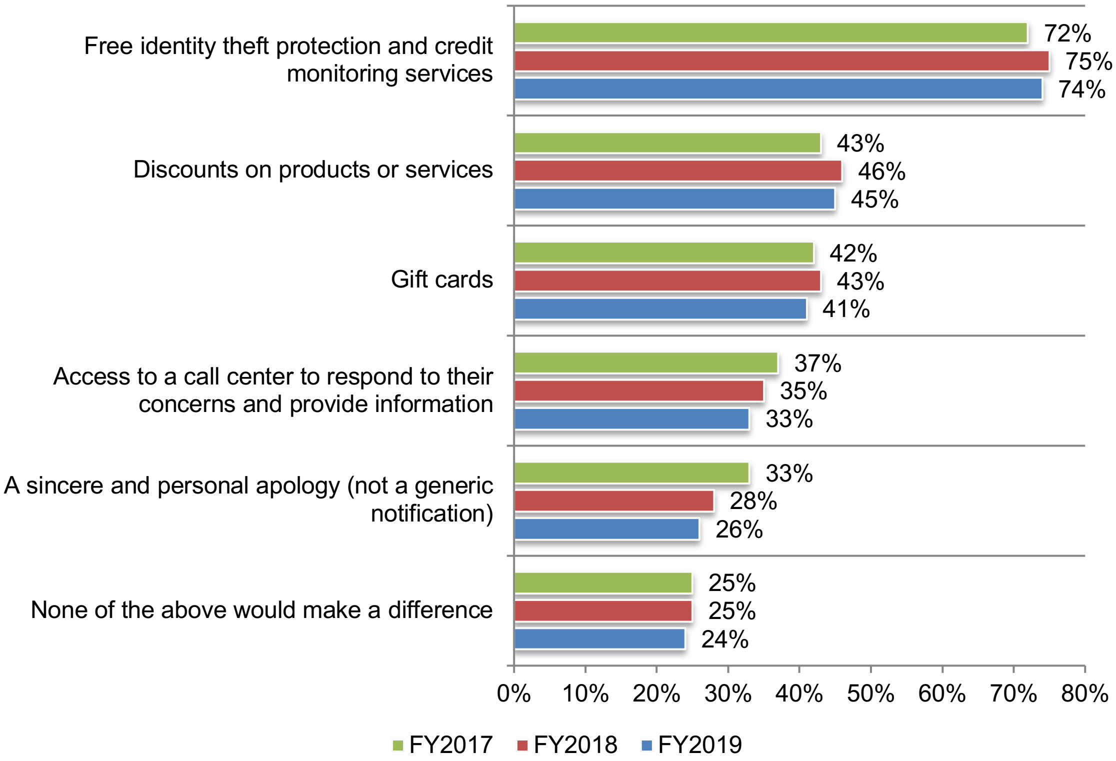
Organizations are not confident in their ability to minimize reputational consequences and prevent the loss of customers. As shown in Figure 18, to prevent the loss of customers, 62 percent of respondents believe credit monitoring protection for victims is the best protection for consumers. However, only 23 percent of respondents say their organization is confident in its ability to minimize the financial and reputational consequences of a material data breach and only 38 percent of respondents say they are 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.

Figure 18. Perceptions about the ability to maintain customer loyalty
Strongly agree and Agree responses combined



By far, free identity theft protection and credit monitoring services is most effective in keeping customers and maintaining their reputation.

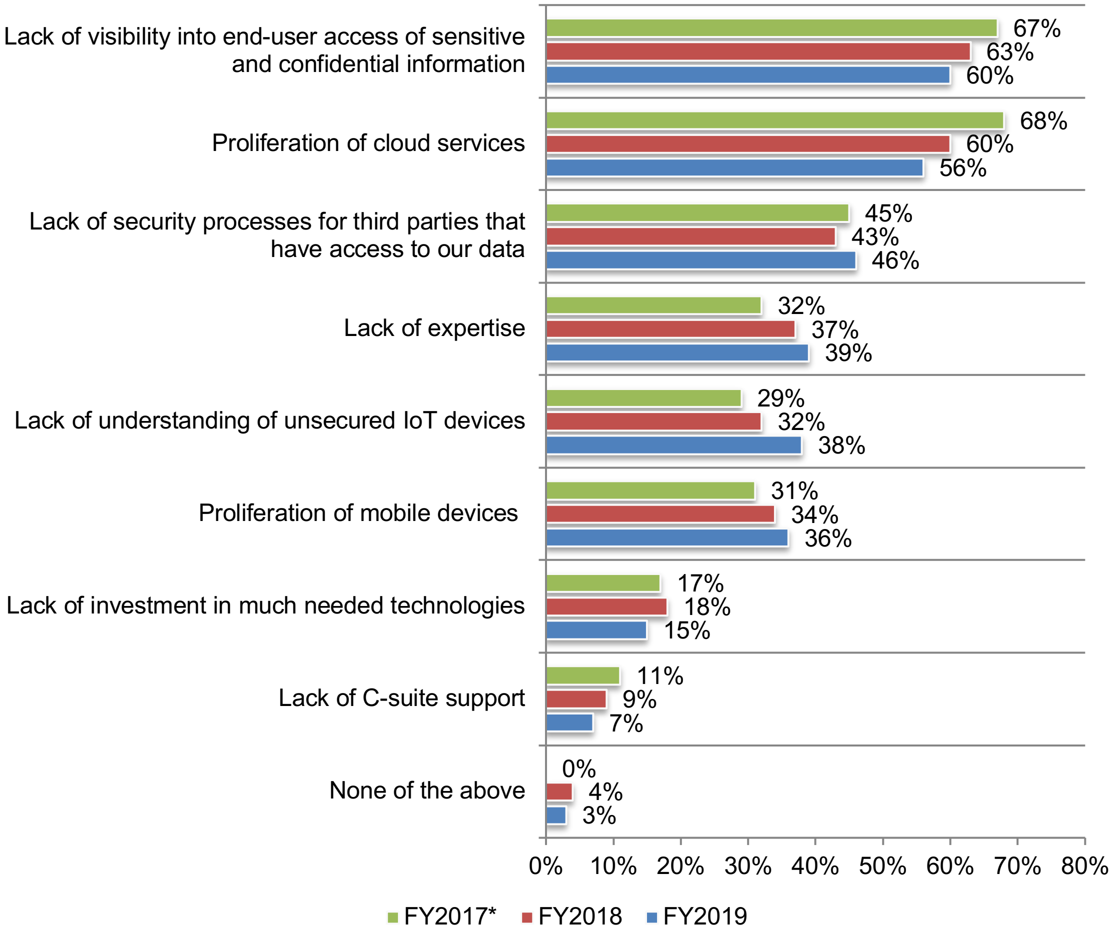
Figure 19. Following a data breach what is the best approach to keeping customers and maintaining reputation?
More than one response permitted



The threats of ransomware, phishing and IoT increase the likelihood of a data breach

Lack of visibility into end-user access of sensitive and confidential information is the number one barrier to improving data breach response. Barriers that are increasing, as shown in Figure 20, are the lack of expertise (an increase from 32 percent to 39 percent of respondents) and a lack of understanding of unsecured IoT devices in the workplace (an increase from 29 percent to 38 percent).

Figure 20. The biggest barriers to improving the ability of IT security to respond to a data breach
Three responses permitted

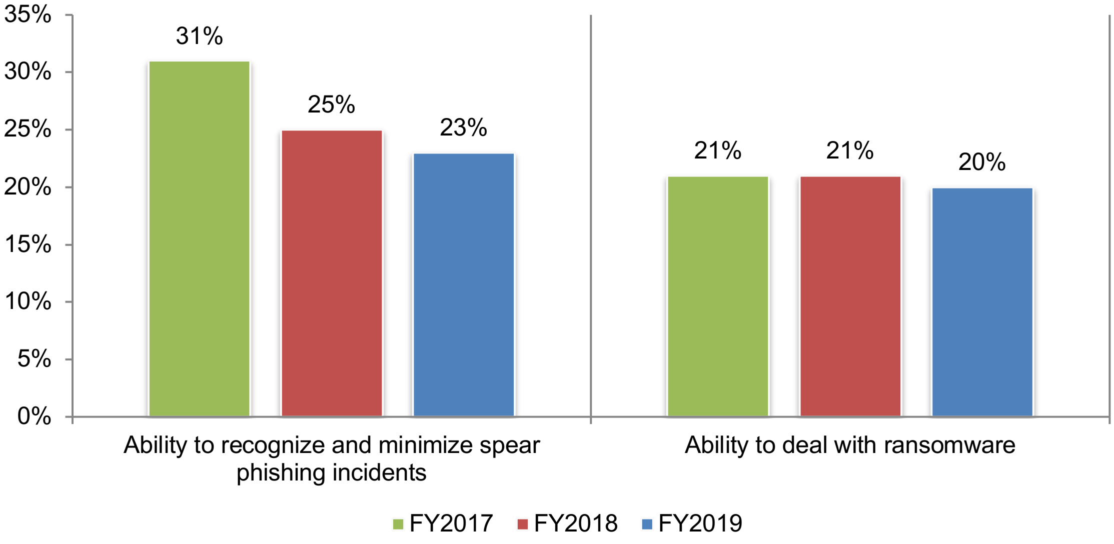


Spear phishing attacks are pervasive and confidence in dealing with them is declining. Sixty-nine percent of respondents had one or more spear phishing attacks and 67 percent of respondents say the negative consequences of these attacks was very significant or significant. Despite the frequency of these attacks, 50 percent of respondents do not train their employees to recognize and minimize spear phishing incidents.

As shown in Figure 21, since 2017 respondents who say their organizations are very confident or confident in their ability to deal with spear phishing attacks has declined from 31 percent to 23 percent.

Respondents are even less confident to deal with ransomware. Only 20 percent of respondents say they are very confident or confident.

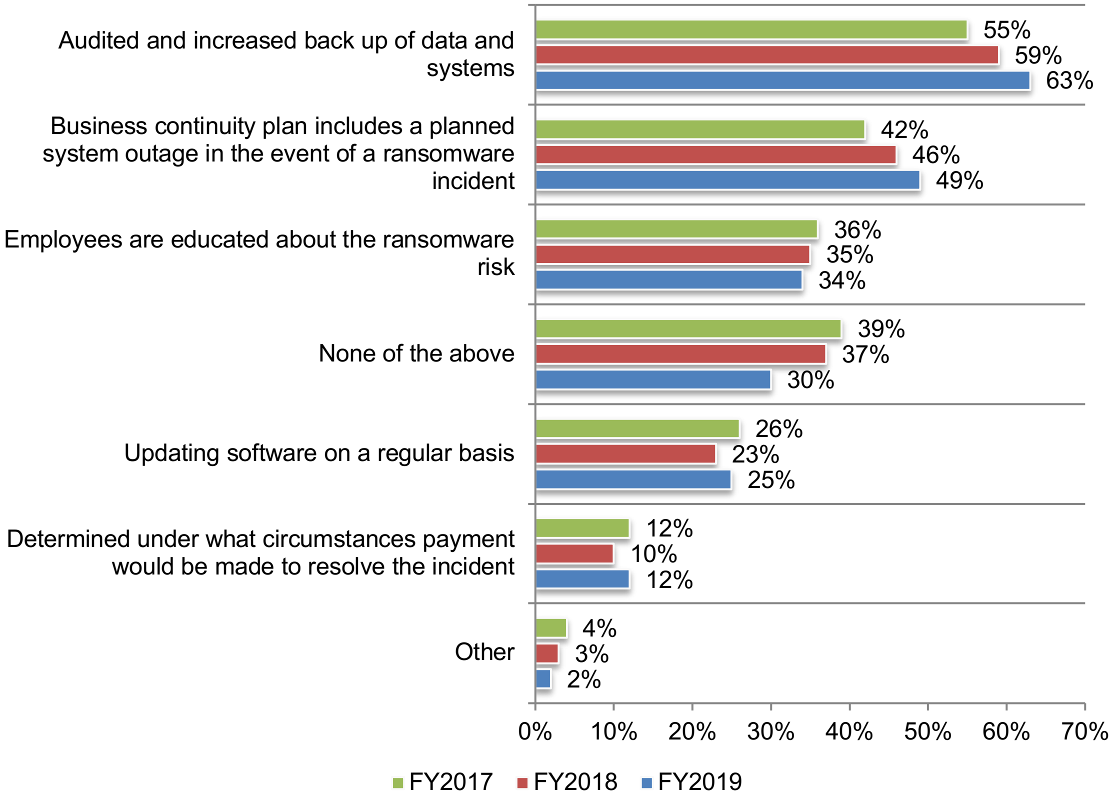
Figure 21. How confident is your organization in its ability to deal with spear phishing incidents and ransomware?
Very confident and Confident responses combined



Thirty-six percent of respondents say their organizations had a ransomware attack. The average ransom was $6,128 and 68 percent of respondents say it was paid.

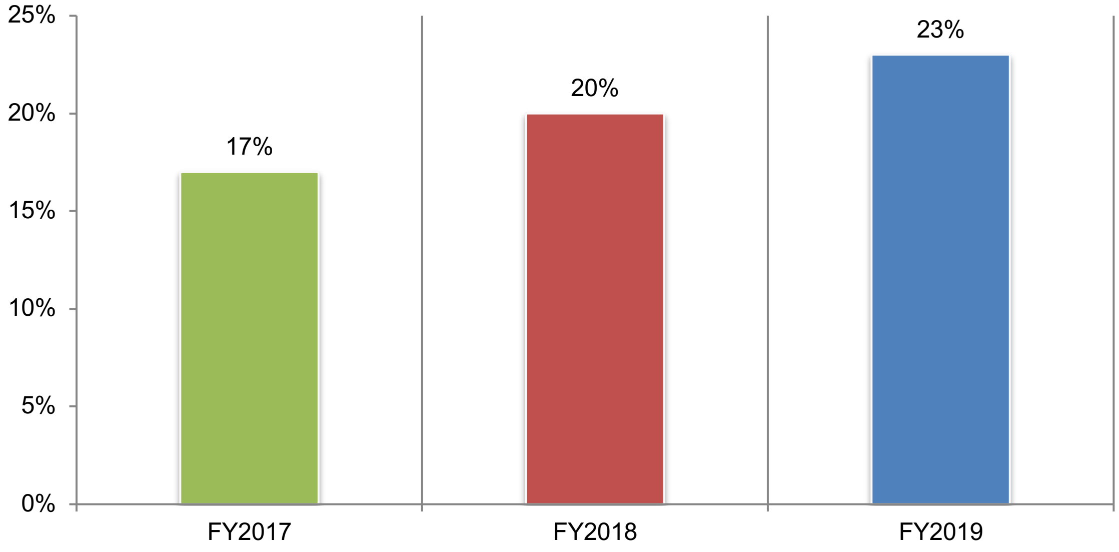
According to Figure 22, more respondents report that their organizations audited and increased backup of data and systems and their business continuity plan includes a planned system outage in the event of a ransomware incident.

Figure 22. Has your organization taken the following steps to prepare for a ransomware incident?
More than one response permitted



Respondents were asked to rate how well they are prepared to deal with IoT-based attacks on a scale from 1 = not prepared to 10 = fully prepared. Figure 23 presents the highly and fully prepared responses (7+). While confidence in the ability to deal with such attacks has increased significantly since 2017, it is still very low. As discussed previously, more respondents consider the lack of understanding of unsecured IoT devices as a barrier to improving the ability of IT security to respond to a data breach.

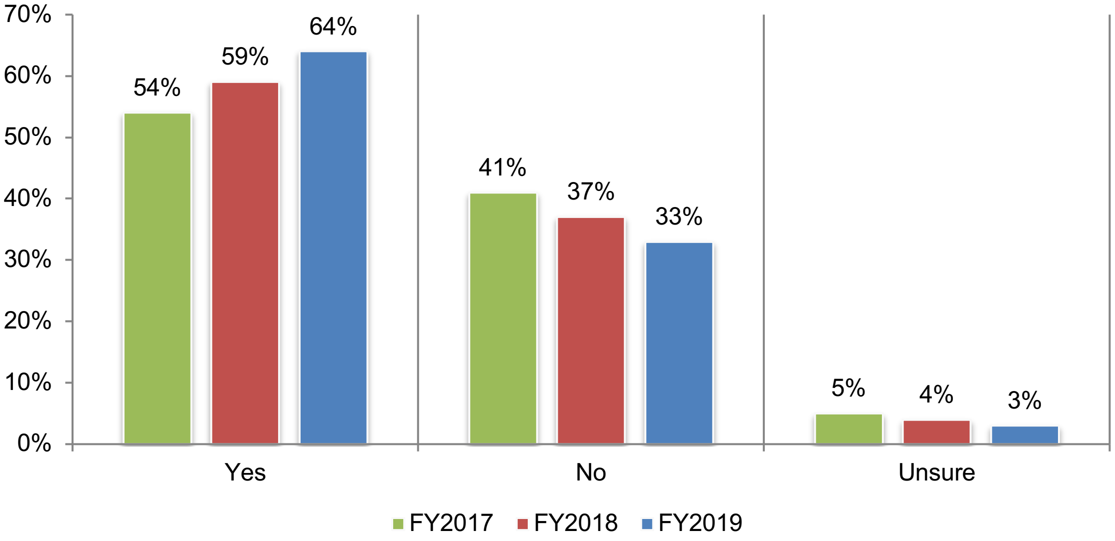
Figure 23. How prepared is your organization to deal with IoT-based attacks?
On a scale of 1 = not prepared to 10 = fully prepared, 7+ responses presented



Data breaches have no borders

More breaches are international or global in scope. As discussed previously, 63 percent of respondents say their organizations had a data breach in the past two years. Forty-five percent of respondents say one more of these breaches were global. According to Figure 24, since 2017, respondents reporting that their incident response plan includes processes to manage an international data breach increased significantly from 54 percent to 64 percent. Fifty-seven percent say the plan is specific to each location it operates.

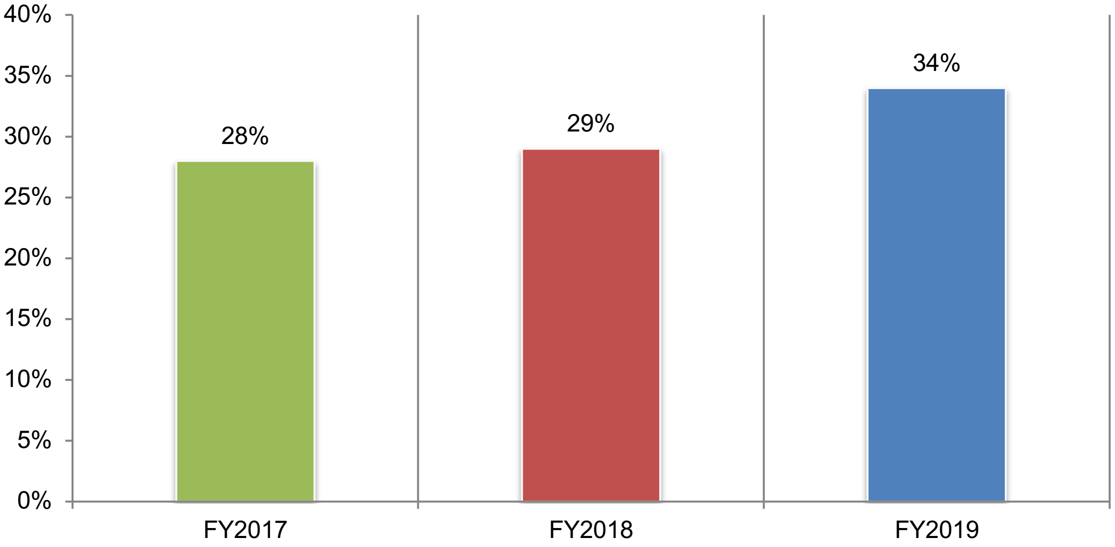
Figure 24. Does your incident response plan include processes to manage an international data breach?



Confidence in the ability to deal with an international data breach is still low, as shown in Figure 25. Only 34 percent of respondents are very confident or confident in their ability to deal with an international data breach.

Figure 25. How confident is your organization in its ability to deal with an international data breach?

Very confident and Confident responses combined

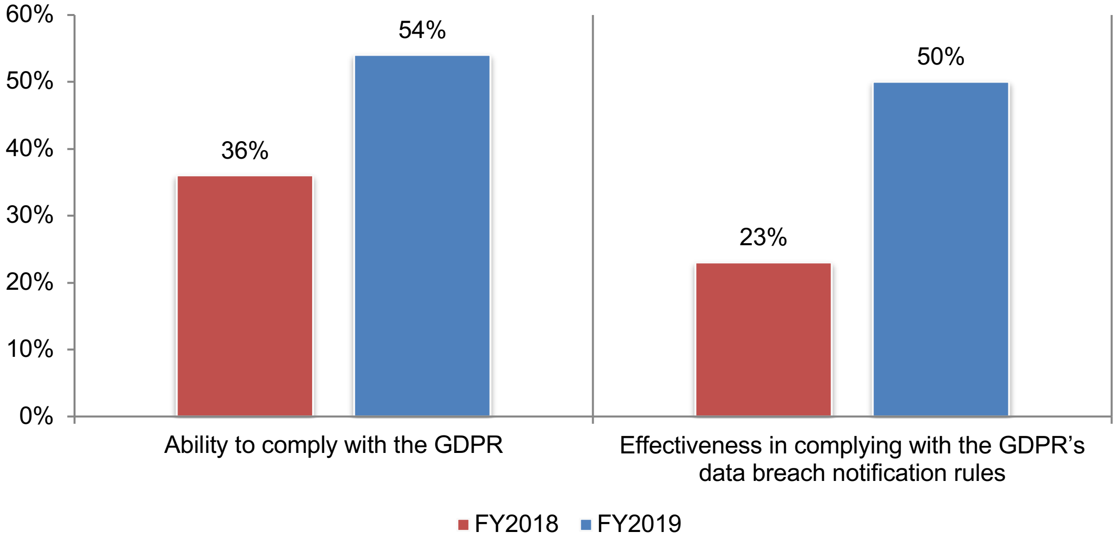


Regulations and data breach preparedness

Now that the General Data Protection Regulation (GDPR) has been in effect for more than a year, organizations have improved their ability to comply with it. Ninety percent of respondents say their organizations are required to comply with GDPR. Respondents were asked to rate their ability to comply with GDPR and their effectiveness to comply with data breach notification rules on a scale from 1 = no ability/effectiveness to 10 = high ability/effectiveness.

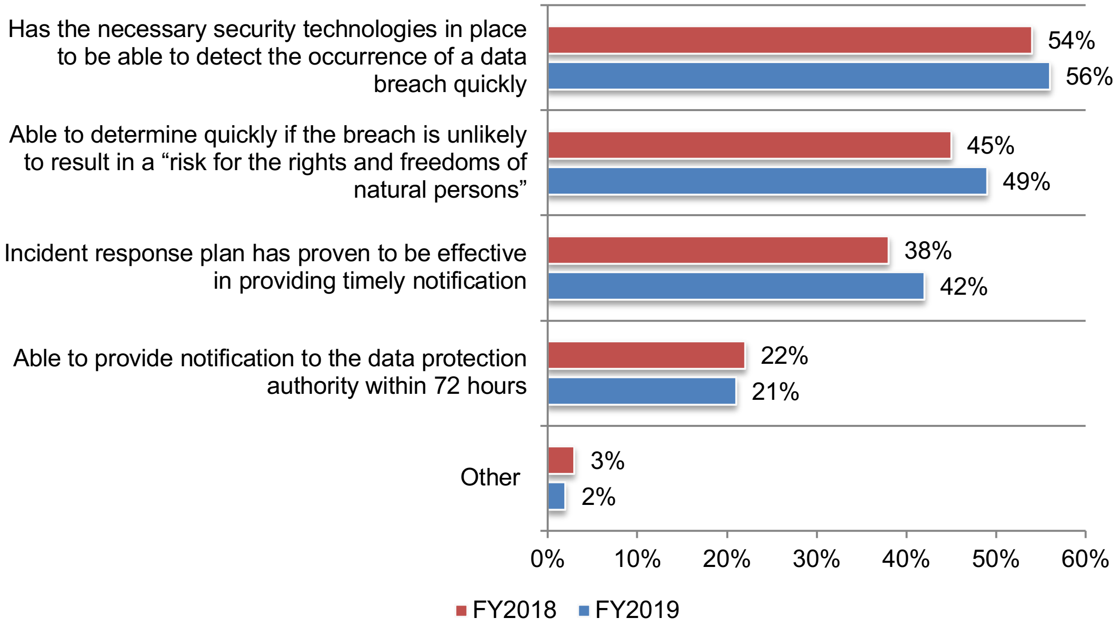
As shown in Figure 26, 54 percent of respondents say they have a high or very high ability to comply with the regulation (an increase from 36 percent) and 50 percent of respondents have a high or very high effectiveness in complying with the data breach notification rules (an increase from 23 percent).

Figure 26. Ability to comply with the GDPR and effectiveness in complying with its data breach notification rules
On a scale of 1 = No ability to 10 = high ability, 1 = low effectiveness to 10 = high effectiveness
7+ responses presented



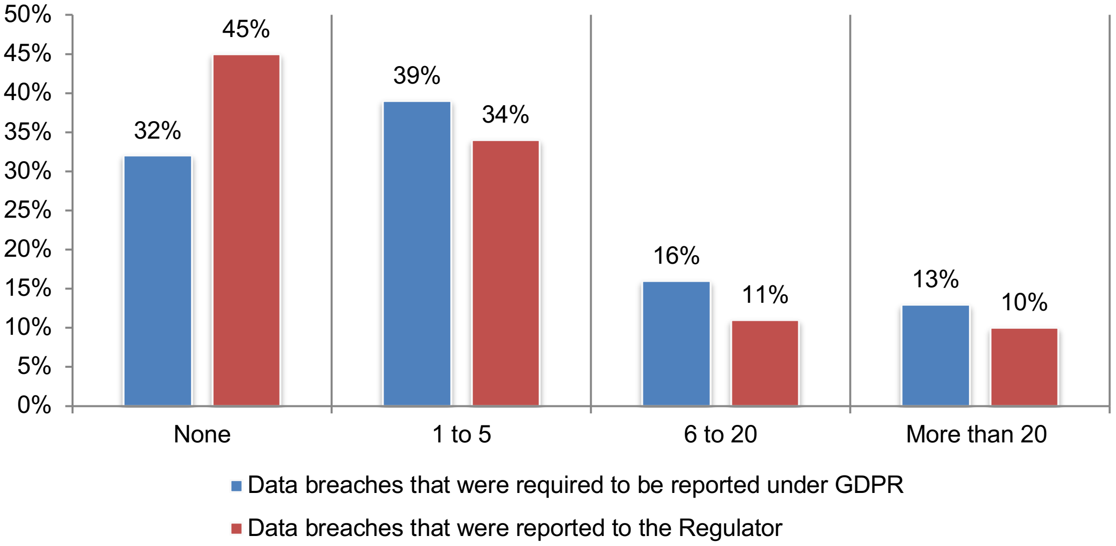
Respondents who rated their effectiveness in complying with the data breach notification rules as high or very high say it was because their organization has the necessary security technologies in place to be able to detect the occurrence of a data breach quickly and determine quickly if the breach is unlikely to result in a "risk for the rights and freedoms of natural persons" (56 percent and 49 percent of respondents), as shown in Figure 27.

Figure 27. Why is your organization effective in complying with the GDPR's data breach notification rules?



Organizations represented in this research say they had an average of seven personal data breaches that had to be reported under the GDPR since it went into effect. As shown in Figure 28, 68 percent of at least one of the breaches had to be reported under GDPR. Fifty-five percent of these breaches were reported.

Figure 28. Personal data breaches required to be reported under GDPR and the number of data breaches reported.



The California Consumer Privacy Act (CCPA) went into effect January 1, 2020 and grants the consumer the right to request a business to disclose the categories and specific pieces of personal information that it collects about the consumer, the categories of sources from which that information is collected, the business purposes for collecting or selling the information and the categories of third parties with which the information is shared. It also requires a business to make disclosures about the information the purposes for which it is used.

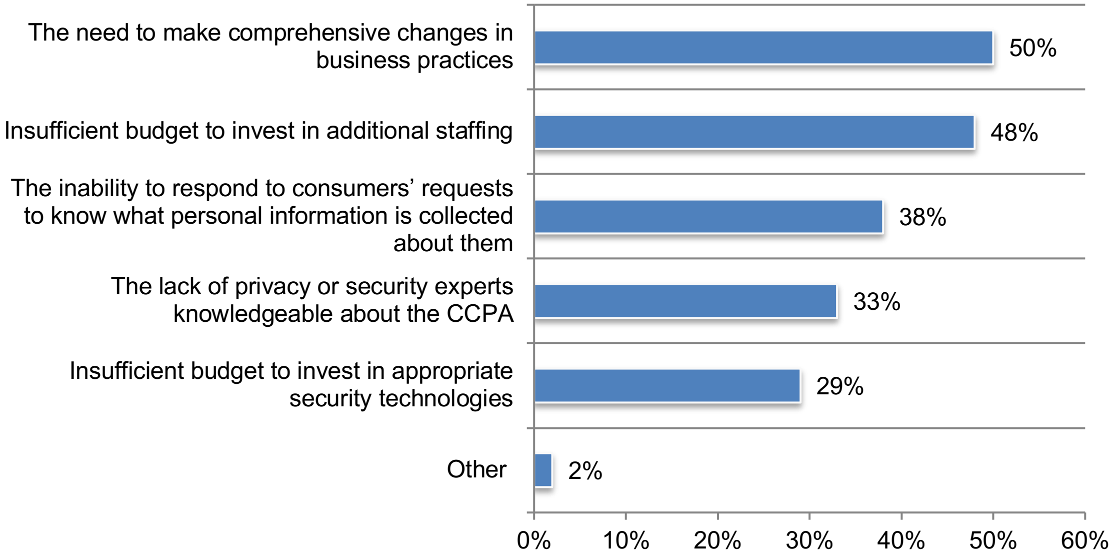
The CCPA applies to the following types of businesses:

- Annual gross revenues in excess of $25 million
- Annually buys, receives for the business' commercial purposes, sells or shares for commercial purposes, alone or in combination, the personal information of 50,000 or more consumers, households or devices

CCPA results in organizations having to make comprehensive changes in business practices. Fifty-six percent of respondents say they are aware of the CCPA and of these respondents, 47 percent of respondents say they are subject to the Act.

Figure 29 presents the challenges to achieving and maintaining CCPA compliance. The top two challenges are similar to achieving compliance with the GDPR, which are the need to change business practices and not enough budget to hire additional staff.

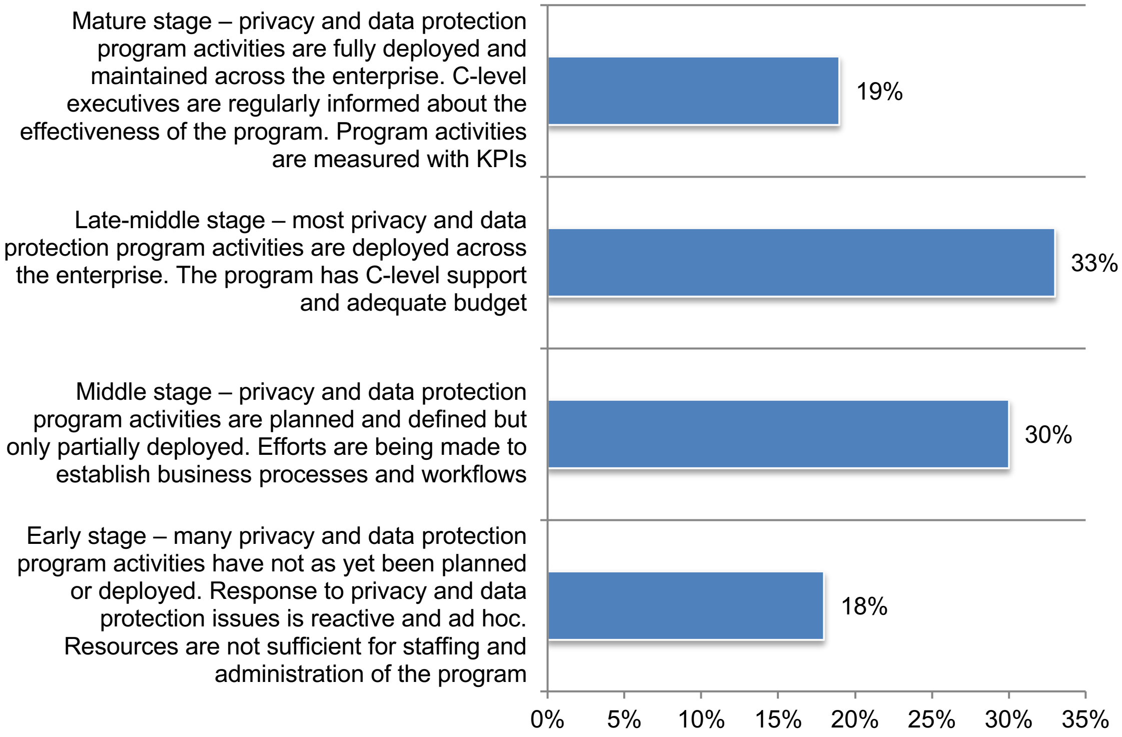
Figure 29. What are the challenges to achieving and maintaining CCPA compliance?
Two responses permitted



Lessons learned from organizations with mature privacy and data protection programs

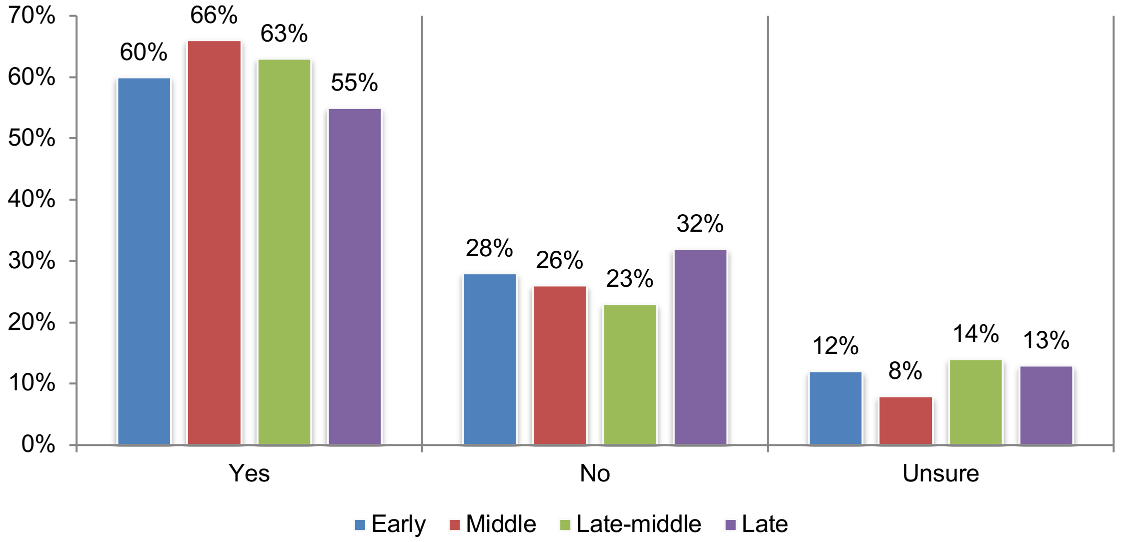
In this section, we analyze how the maturity of organizations' privacy and data protection programs can affect data breach preparedness. Figure 30 presents how respondents self-reported their organizations' stage of maturity. Most organizations are in the middle-and late-middle stage. In the mature stage privacy and data protection programs, activities are fully defined, maintained across the enterprise and measured with KPIs. C-level executives are regularly informed about the program's effectiveness.

Figure 30. What best describes the maturity of your organization's privacy and data protection program?



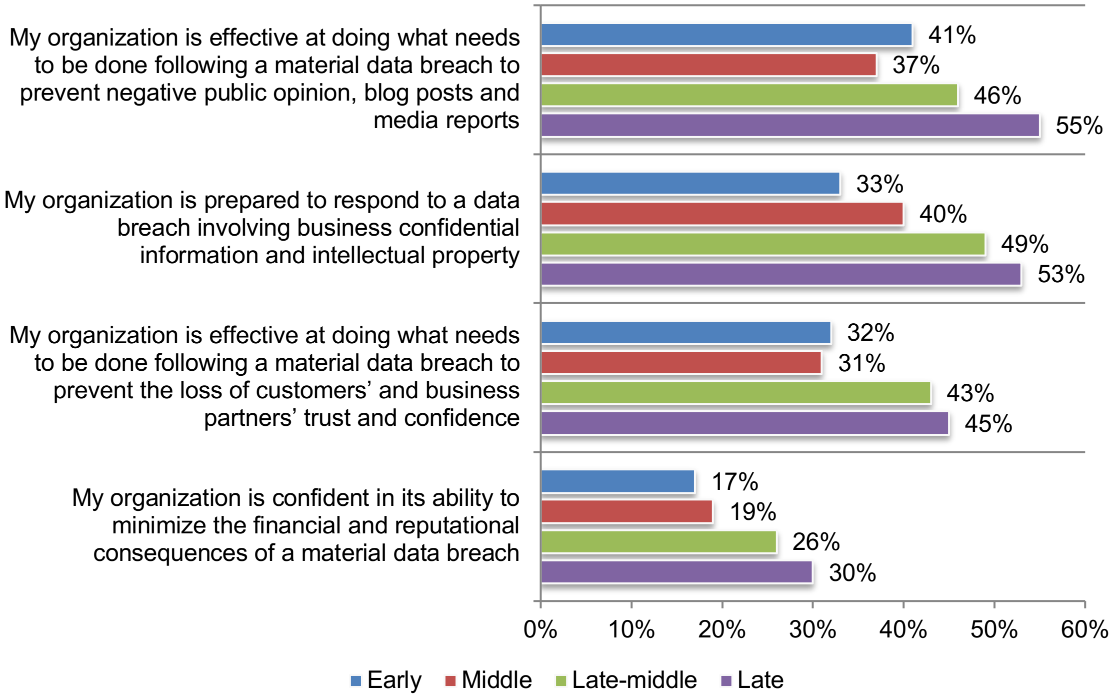
Mature privacy and data protection programs have fewer data breaches. An incentive to invest in having a mature program is to reduce the likelihood of having a data breach. As shown in Figure 31, 55 percent of respondents in mature programs say their organization had a data breach in the past two years. In contrast, a minimum of 60 percent of respondents in the other stages of maturity say their organizations had a data breach.

Figure 31. 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?



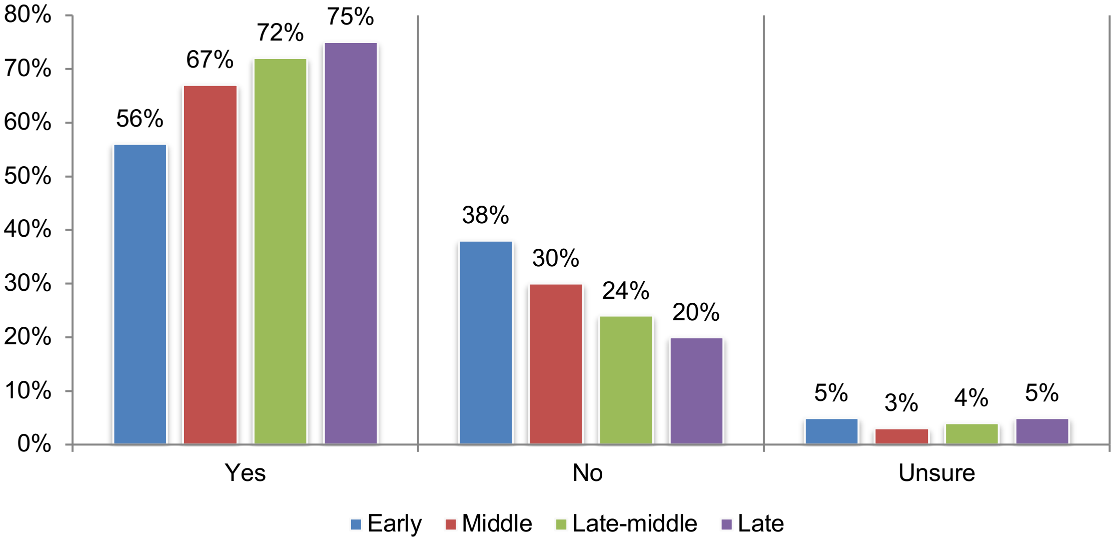
Mature programs are more adept at preventing negative public opinion and media coverage. According to Figure 32, 55 percent of respondents say their organizations are effective at reducing negative public opinion, blog posts and media reports following a material data breach. As organizations advance to a late-middle stage, data breach preparedness significantly improves. However, confidence to minimize the financial and reputational consequences of a data breach is low in all stages.

Figure 32. Perceptions about data breach preparedness
Strongly agree ad Agree responses combined



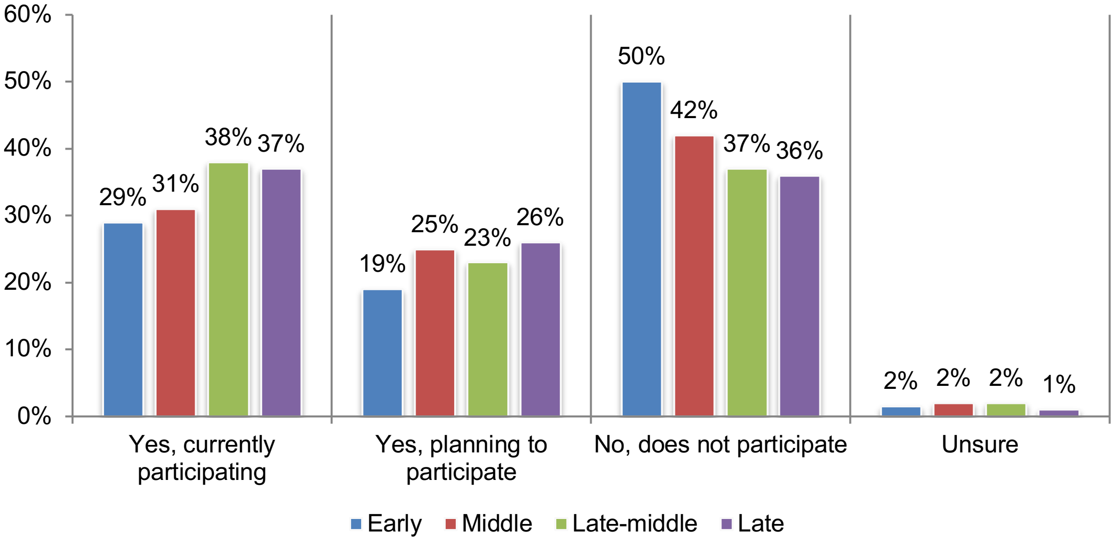
Organizations with mature programs are more likely to increase their investment in security technologies to improve their ability to detect and respond quickly to a data breach, as shown in Figure 33.

Figure 33. 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?



Late-middle and mature programs are more likely to share their data breach and incident response experiences with government and industry peers. As shown in Figure 32, 63 percent of respondents in mature programs and 61 percent of respondents in late-middle programs are currently participating in information sharing or plan to.

Figure 34. Does your organization participate in an initiative or program for sharing information with government and industry peers about data breaches and incident response?



Late-middle and mature programs are better prepared to manage an international data breach. According to Figure 35, late-middle and mature programs understand the importance of including processes to manage an international data breach.

Figure 35. Does your incident response plan include processes to manage an international data breach?

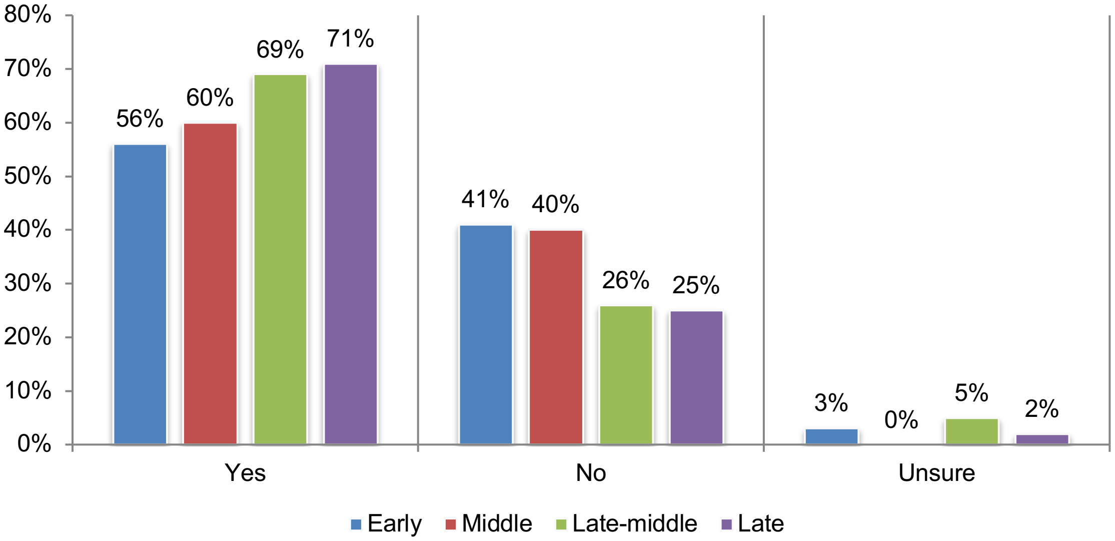
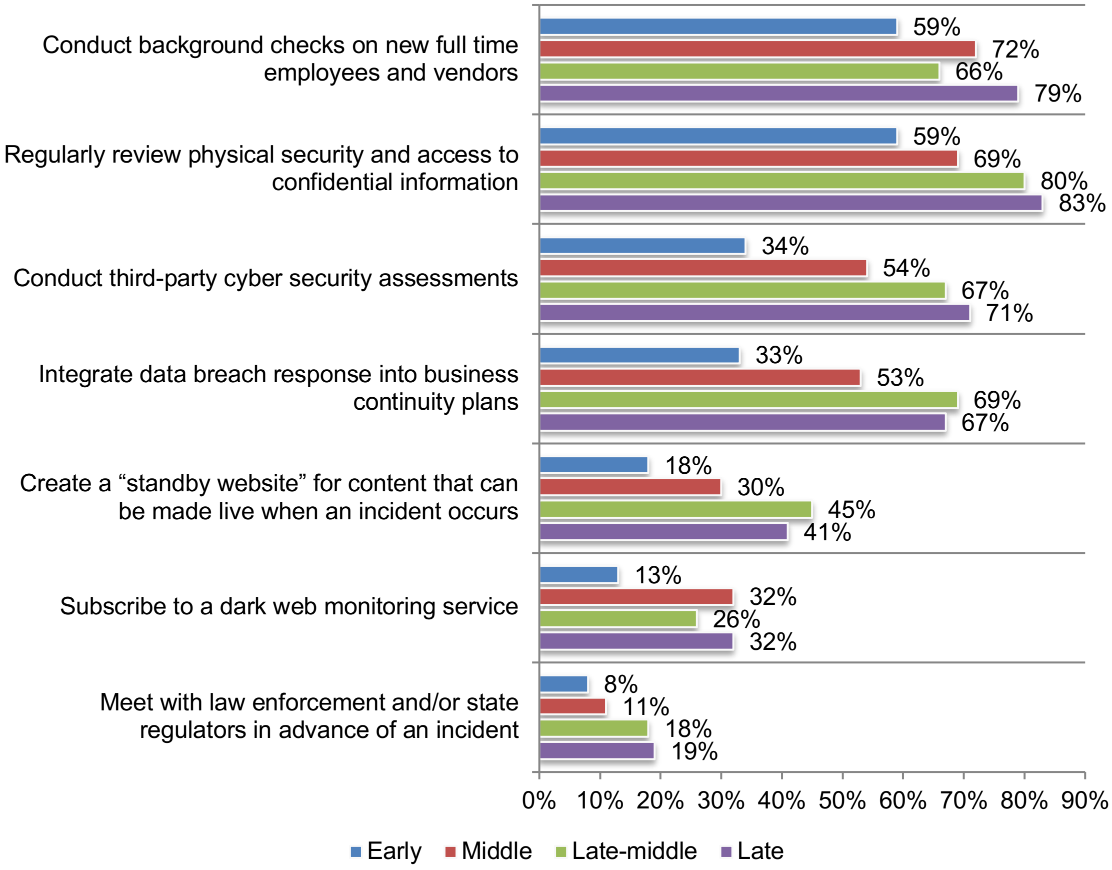


Figure 36 presents the additional steps organizations take to prepare for a data breach. Mature programs are more likely to conduct background checks on full-time employees and vendors, regularly review physical security and access to confidential information, conduct third-party cybersecurity assessments and meet with law enforcement and/or state regulators in advance of an incident.

Figure 36. What additional steps does your organization take to prepare for a data breach?

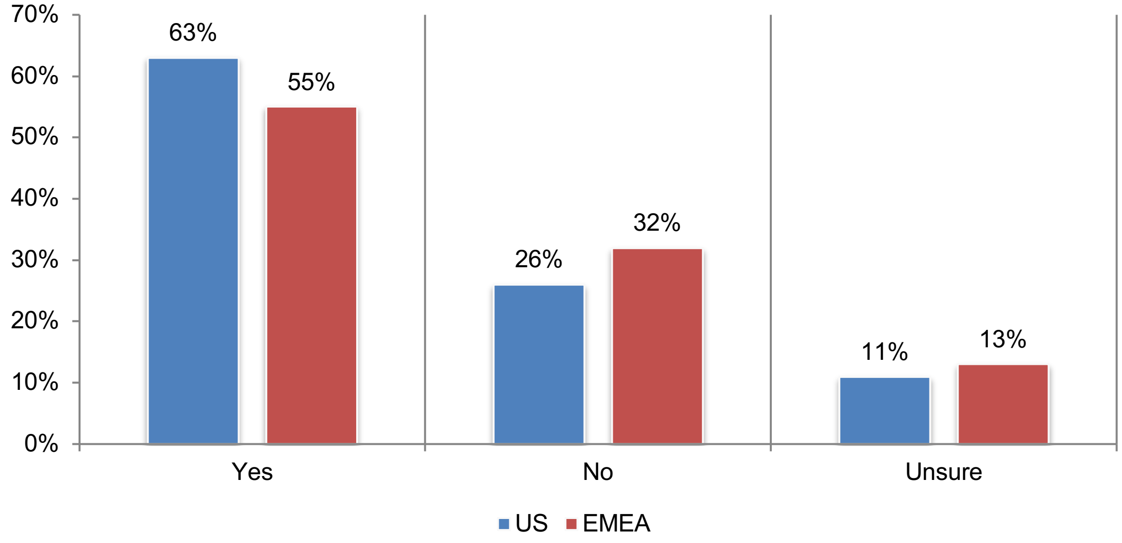


Part 3. Differences between the US and EMEA

In this section, we highlight the most significant differences in the research between the US (650 respondents) and EMEA (456 respondents).

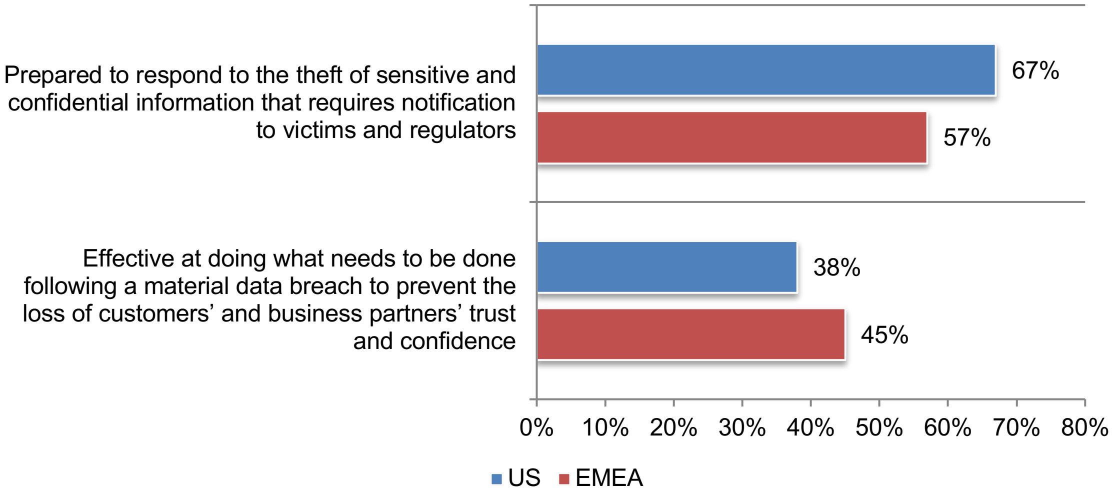
US organizations report having more data breaches than EMEA. According to Figure 37, 63 percent of US respondents report having had a data breach involving the loss or theft of more than 1,000 records containing sensitive or confidential information in the past two years. Fifty-five percent of EMEA respondents say they have had a data breach during this period.

Figure 37. Did your organization have a data breach involving the loss or theft of more than 1,000 records containing sensitive or confidential information in the past two years?



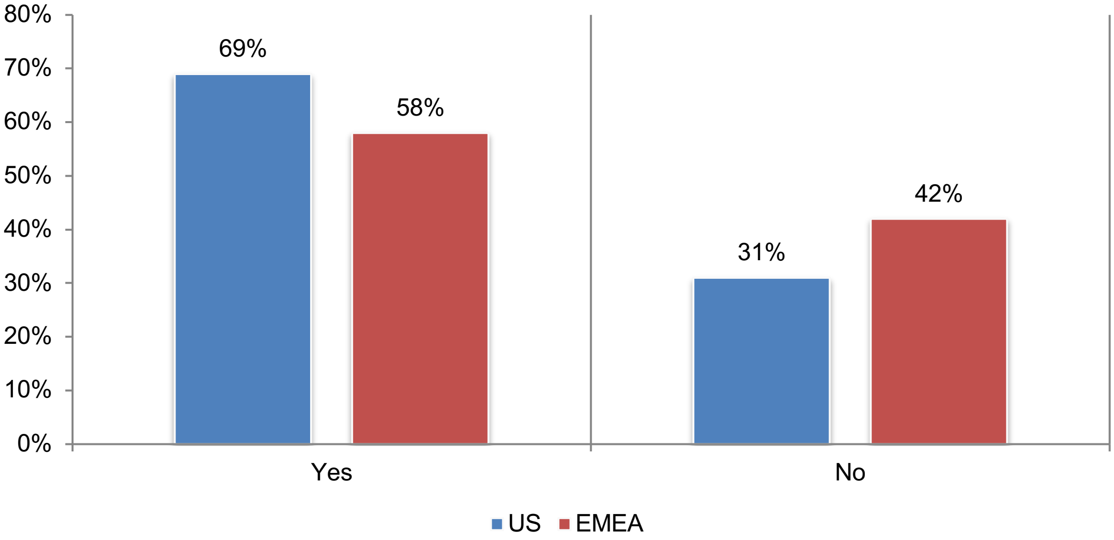
US organizations are better prepared to handle notification to victims and regulators. As shown in Figure 38, 67 percent of US respondents say their organizations are prepared to respond to data breaches that require notification to victims and regulators. More EMEA respondents say they are effective at doing what needs to be done following a material data breach to prevent the loss of customers' and business partners' trust and confidence.

Figure 38. Trends in the ability to respond to a data breach
Strongly agree and Agree responses combined



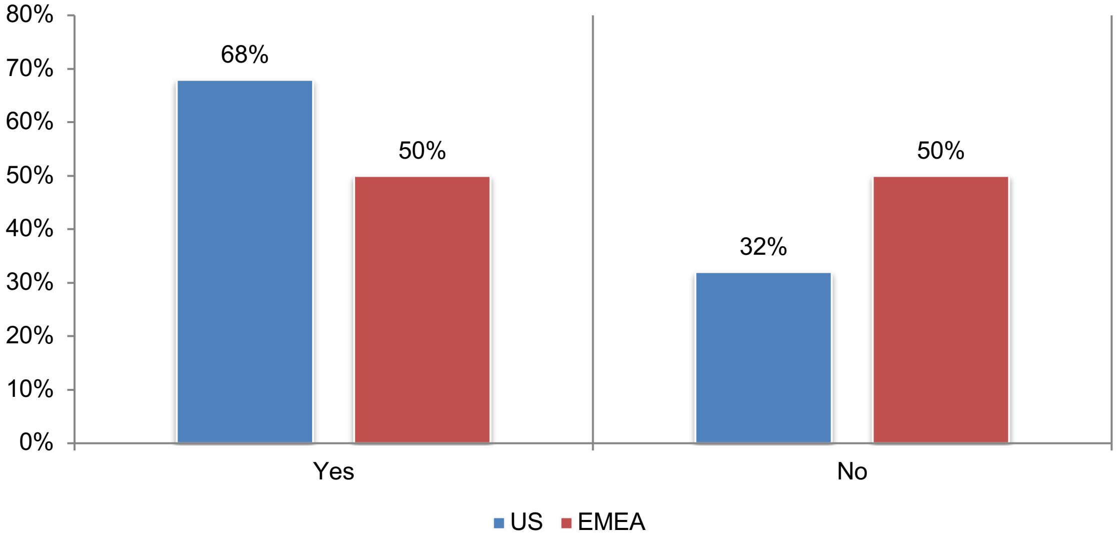
US organizations are more likely to have had one or more spear phishing attack in the past year. Sixty-nine percent of US respondents vs. 58 percent of EMEA respondents report having had a spear phishing attack.

Figure 39. In the past 12 months, did your organization experience one or more spear phishing attacks?



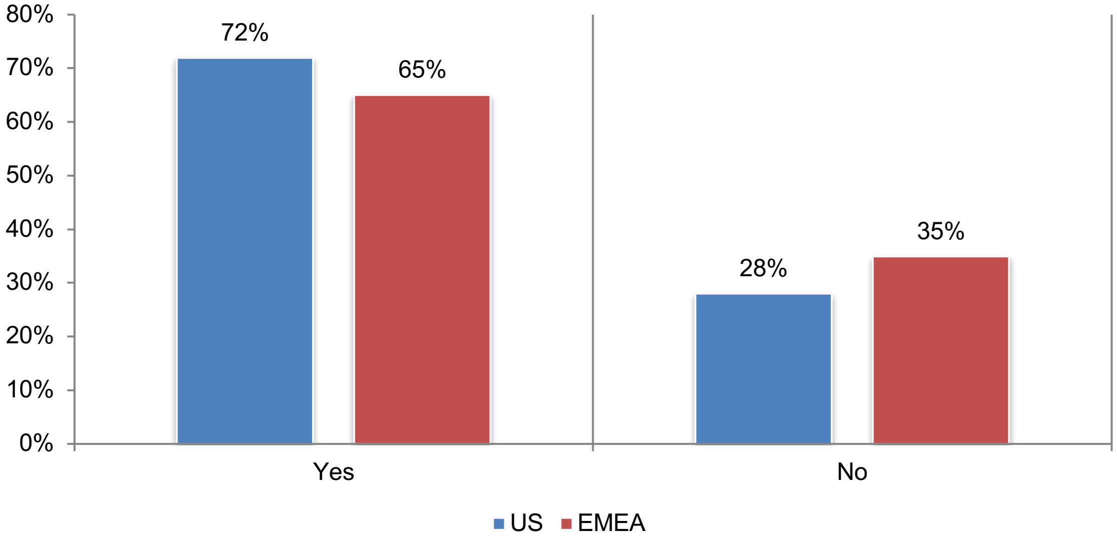
More US organizations that experienced a ransomware attack paid the ransom. Thirty-six percent of US respondents and 35 percent of EMEA respondents say they have had a ransomware attack. Of these, 68 percent of US respondents say they paid an average of $6,128 and 50 percent of EMEA respondents paid an average of $4,274 (in US dollars).

Figure 40. Did your company pay the ransom?



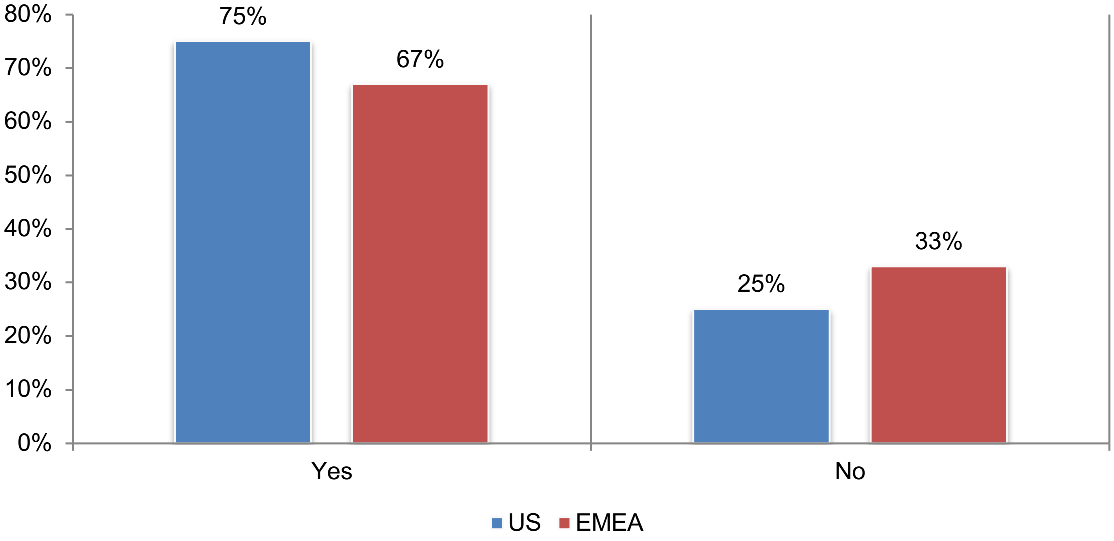
More US organizations have training and awareness programs. Most US and EMEA organizations have privacy and data protection awareness and training programs for those with access to sensitive and confidential personal information. However, as shown in Figure 41, 72 percent of US respondents vs. 65 percent of EMEA respondents have such programs.

Figure 41. 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?



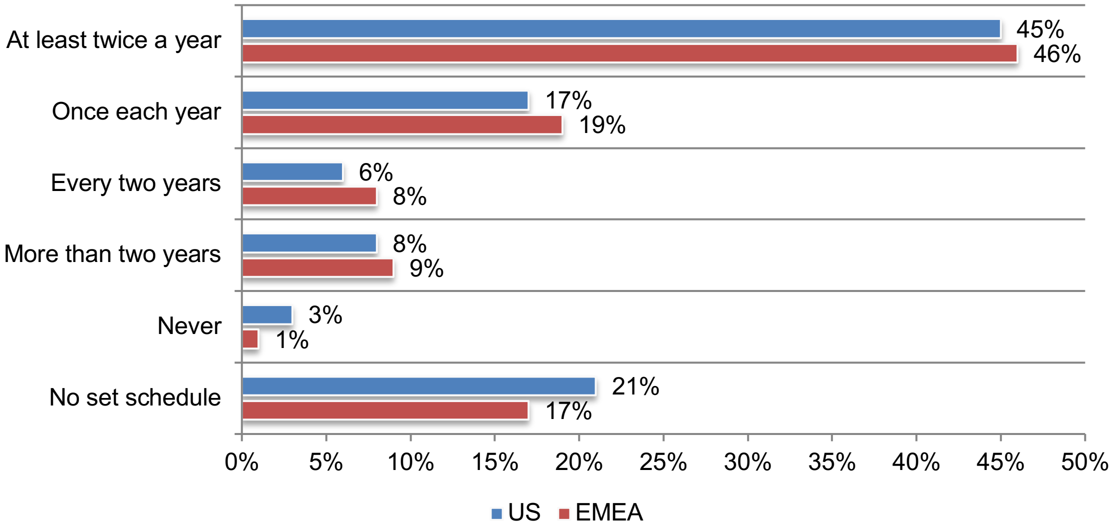
Most organizations, as shown in Figure 42, practice responding to a data breach.

Figure 42. Does your organization practice responding to a data breach?



Both US and EMEA organizations are most likely to conduct data breach response twice a year (45 percent and 46 percent of respondents, respectively).

Figure 43. How often is the response practiced?



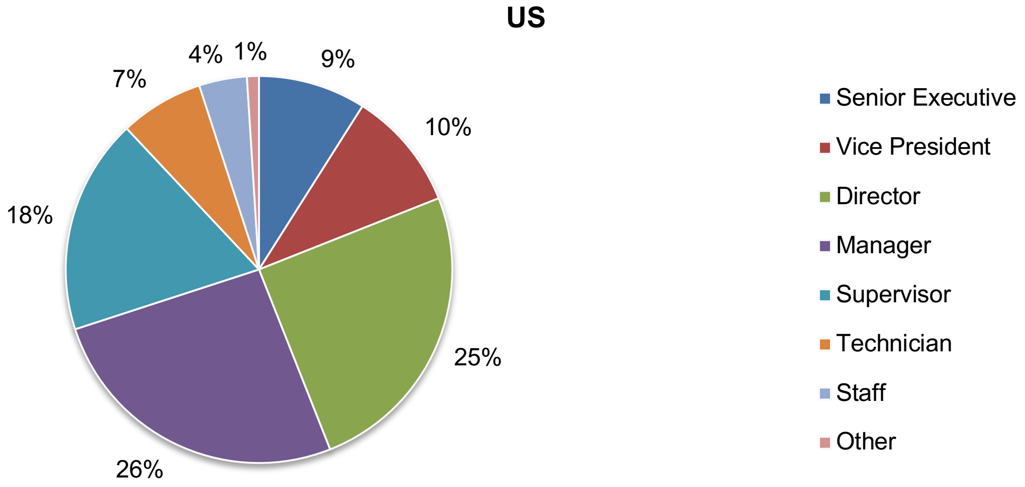
Part 4. Methods

A sampling frame of 15,590 US and 12,881 EMEA IT and IT security, compliance and privacy professionals, who are involved in data breach response plans in their organizations were selected as participants to this survey. Table 1 shows 713 total US survey returns and 513 EMEA survey returns. Screening and reliability checks required the removal of 63 US surveys and 57 EMEA surveys. Our final sample consisted of 650 US surveys (a 4.2 percent response rate) and 456 EMEA surveys (a 3.5 percent response rate).

Table 1. Sample response	US	EMEA	Combined
Sampling frame	15,590	12,881	28,471
Total returns	713	513	1,226
Rejected or screened surveys	63	57	120
Final sample	650	456	1,106
Response rate	4.2%	3.5%	3.9%

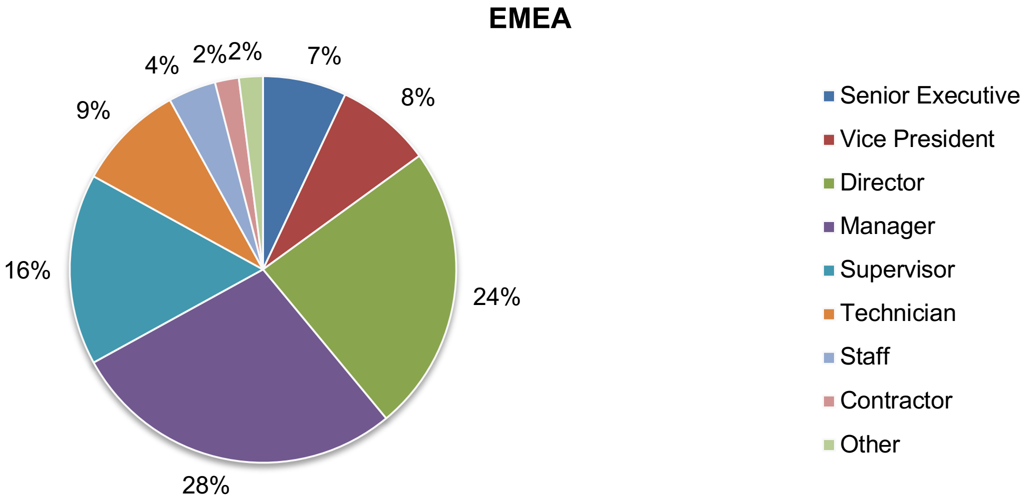
Pie Chart 1 reports the US respondent's organizational level within participating organizations. By design, a majority of respondents (88 percent) are at or above the supervisory levels.

Pie Chart 1. Current position within the organization



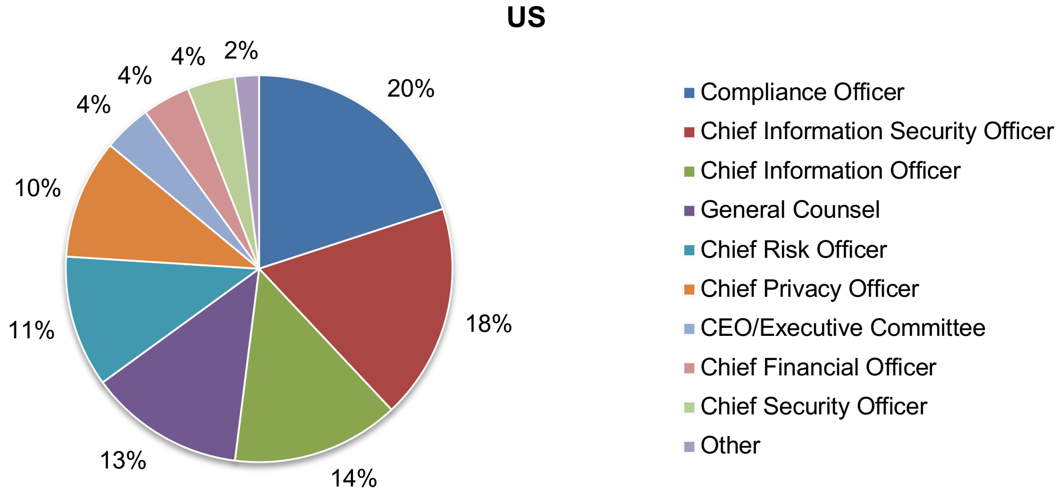
Pie Chart 2 reports the EMEA respondent's organizational level within participating organizations. By design, a majority of respondents (83 percent) are at or above the supervisory levels.

Pie Chart 2. Current position within the organization



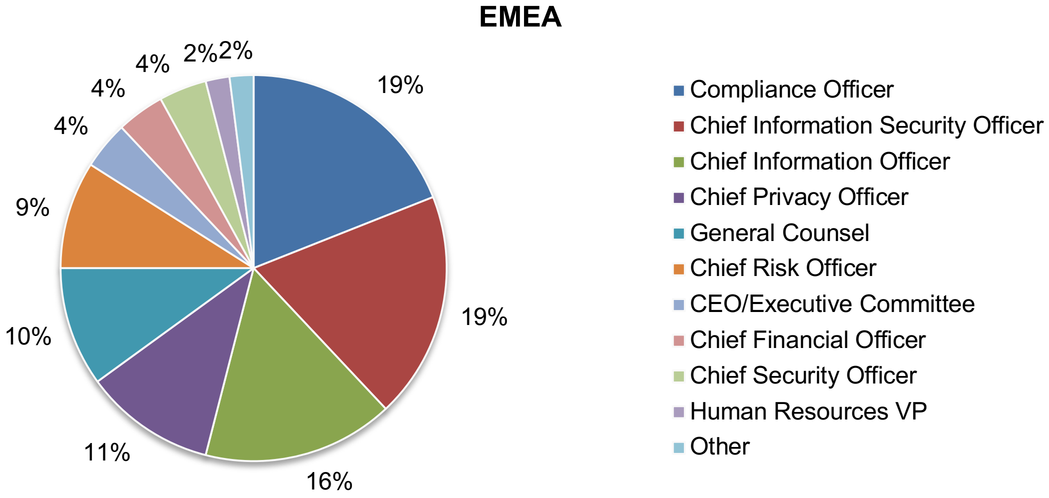
Pie Chart 3 reveals that 20 percent of US respondents report to the compliance officer, 18 percent of respondents report to the chief information security officer, 14 percent of respondents report to the chief information officer, 13 percent of respondents report to the general counsel and 11 percent of respondents report to the chief risk officer.

Pie Chart 3. Primary person respondent reports to within the organization



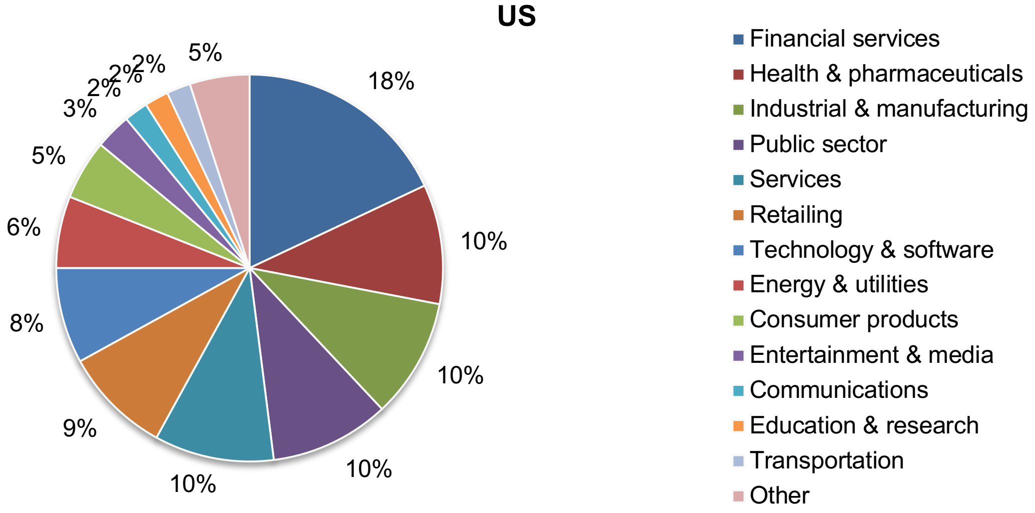
Pie Chart 4 reveals that 19 percent of EMEA respondents report to the compliance officer, 19 percent of respondents report to the chief information security officer, 16 percent of respondents report to the chief information officer, 11 percent of respondents report to the chief privacy officer and 10 percent of respondents report to the general counsel.

Pie Chart 4. Primary person respondent reports to within the organization



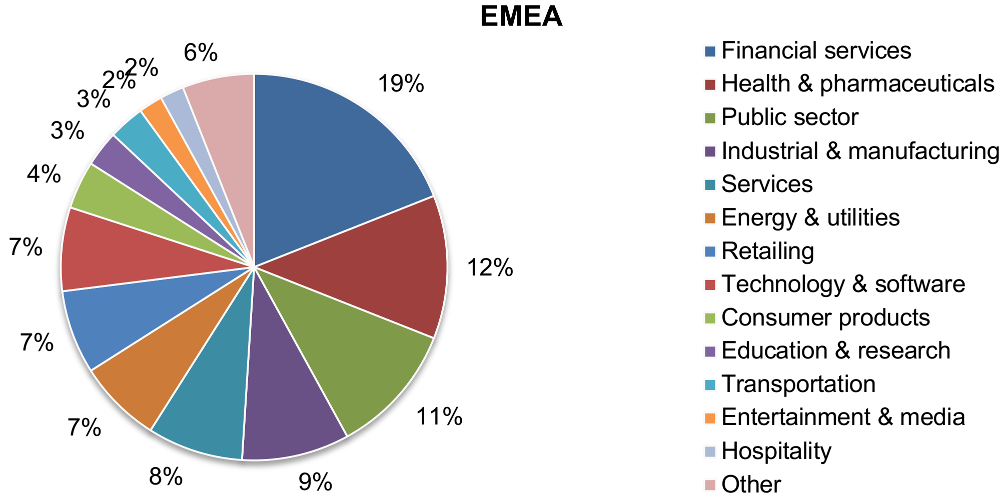
Pie Chart 5 reports the industry classification of US respondents' organizations. The largest industry classification is financial services (18 percent of respondents), which includes banking, investment management, insurance, brokerage, payments and credit cards. This is followed by health and pharmaceutical (10 percent of respondents), industrial/manufacturing (10 percent of respondents), public sector (10 percent of respondents) and services (10 percent of respondents).

Pie Chart 5. Primary industry focus



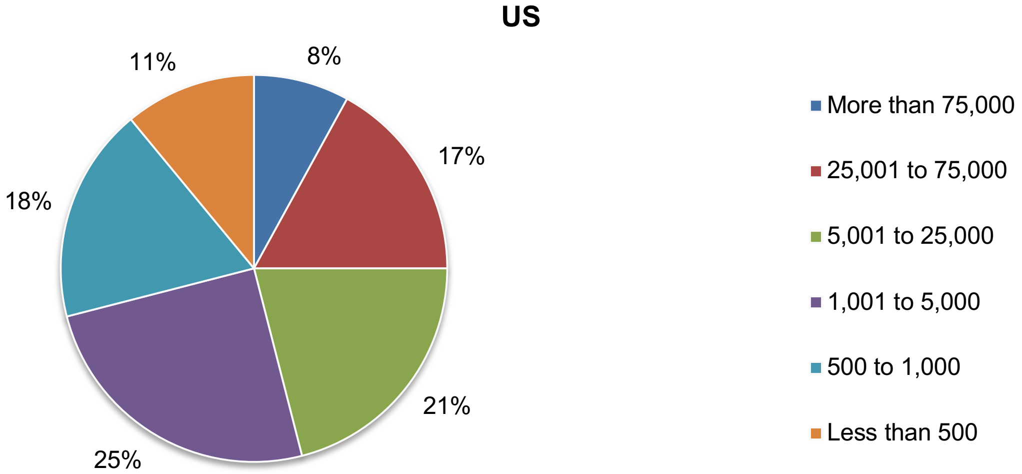
Pie Chart 6 reports the industry classification of EMEA respondents' organizations. The largest industry classification is financial services (19 percent of respondents), which includes banking, investment management, insurance, brokerage, payments and credit cards. This is followed by health and pharmaceutical (12 percent of respondents), public sector (11 percent of respondents) industrial/manufacturing (9 percent of respondents), and services (8 percent of respondents).

Pie Chart 6. Primary industry focus



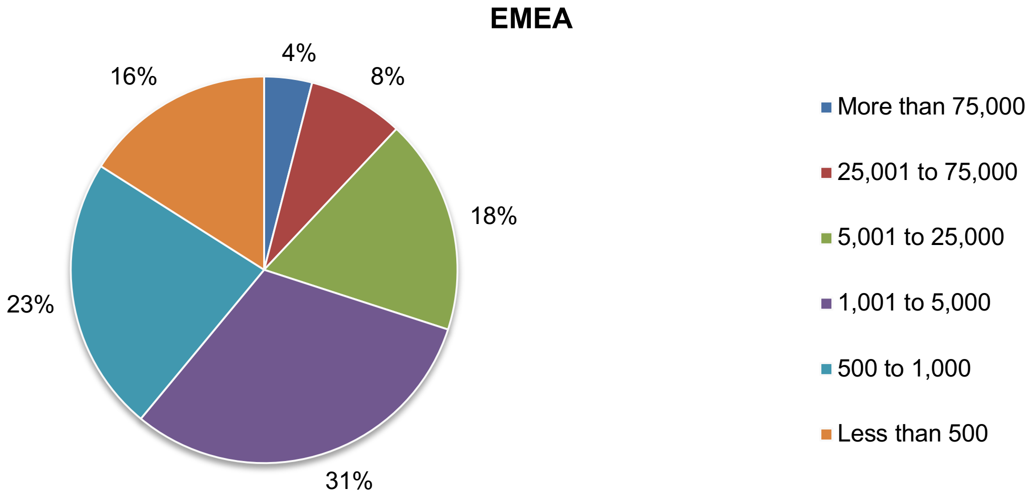
As shown in Pie Chart 7, 71 percent of US respondents are from organizations with a global headcount of more than 1,000 employees.

Pie Chart 7. Global employee headcount



As shown in Pie Chart 7, 61 percent of EMEA respondents are from organizations with a global headcount of more than 1,000 employees.

Pie Chart 7. 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 12 and December 3, 2019.

Survey response	FY2019	FY2018	FY2017
Sampling frame	15,590	15,986	15,402
Total returns	713	702	679
Rejected or screened surveys	63	59	55
Final sample	650	643	624
Response rate	4.2%	4.0%	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?	FY2019	FY2018	FY2017
Yes	63%	59%	56%
No	26%	29%	31%
Unsure	11%	12%	13%
Total	100%	100%	100%

Q1b. If yes, how frequently did these incidents occur during the past 2 years?	FY2019	FY2018	FY2017
Only once	31%	27%	30%
2 to 3 times	33%	35%	37%
4 to 5 times	24%	27%	23%
More than 5 times	12%	11%	10%
Total	100%	100%	100%

Q1c. If yes, were any of these breaches international or global in scope?	FY2019	FY2018	FY2017
Yes	45%	43%	39%
No	49%	50%	53%
Unsure	6%	7%	8%
Total	100%	100%	100%

Attributions. Please rate each statement using the scale provided below each item. Strongly agree and agree response	FY2019	FY2018	FY2017
Q2. My organization is prepared to respond to the theft of sensitive and confidential information that requires notification to victims and regulators.	67%	65%	62%
Q3. My organization is prepared to respond to a data breach involving business confidential information and intellectual property.	44%	36%	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.	38%	39%	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.	44%	41%	36%
Q6. My organization's incident response plan includes breaches involving IoT devices.	40%	35%	29%
Q7. My organization is confident in its ability to minimize the financial and reputational consequences of a material data breach.	23%	21%	25%
Q8. Following a data breach, a credit monitoring and/or identity theft protection product is the best protection for consumers.	62%	59%	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?	FY2019	FY2018	FY2017
Yes	74%	75%	71%
No	26%	25%	29%
Total	100%	100%	100%

Q9b. If yes, how long should identity theft protection be provided?	FY2019	FY2018	FY2017
2 to 3 years	45%	47%	49%
4 to 7 years	39%	35%	30%
8 to 10 years	12%	13%	16%
More than 10 years	4%	5%	5%
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? Please select all that apply.	FY2019	FY2018	FY2017
Free identity theft protection and credit monitoring services	74%	75%	72%
A sincere and personal apology (not a generic notification)	26%	28%	33%
Discounts on products or services	45%	46%	43%
Gift cards	41%	43%	42%
Access to a call center to respond to their concerns and provide information	33%	35%	37%
None of the above would make a difference	24%	25%	25%
Total	243%	252%	252%

Q11. Which of the following issues would have the greatest impact on your organization's reputation? Please select one choice.	FY2019	FY2018	FY2017
Poor customer service	27%	29%	28%
Cybersecurity incident	20%		
Labor or union dispute	2%	2%	3%
Environmental incident	8%	9%	8%
Data breach	22%	27%	25%
Regulatory fines	3%	5%	4%
Publicized lawsuits	6%	9%	10%
Product recall	12%	18%	20%
CEO's salary	0%	1%	2%
Total	100%	100%	100%

* Two responses permitted in FY2015

Part 2. Data breach preparedness

Q12. What best describes the maturity of your organization's privacy and data protection program?	FY2019
Early stage – many privacy and data protection program activities have not as yet been planned or deployed. Response to privacy and data protection issues is reactive and ad hoc. Resources are not sufficient for staffing and administration of the program.	18%
Middle stage – privacy and data protection program activities are planned and defined but only partially deployed. Efforts are being made to establish business processes and workflows.	30%
Late-middle stage – most privacy and data protection program activities are deployed across the enterprise. The program has C-level support and adequate budget.	33%
Mature stage – privacy and data protection program activities are fully deployed and maintained across the enterprise. C-level executives are regularly informed about the effectiveness of the program. Program activities are measured with KPIs.	19%
Total	100%

Q13a. Do you believe your company's C-suite executives are knowledgeable about plans to deal with a possible data breach?	FY2019	FY2018	FY2017
Yes	55%	51%	48%
No	45%	49%	52%
Total	100%	100%	100%

Q13b. If yes, why do you believe your company's C-suite executives are knowledgeable? Please select all that apply.	FY2019	FY2018	FY2017
They regularly participate in detailed reviews of our data breach response plan	26%	22%	19%
They understand the specific security threats facing our organization	40%	37%	36%
They provide detailed feedback about the data breach response plan	25%	24%	25%
They assume responsibility for the successful execution of the incident response plan	24%	23%	25%
They have requested to be notified ASAP if a material data breach occurs	52%	49%	45%
They participate in a high level review of the organization's data protection and privacy practices	15%	13%	15%
Total	182%	168%	165%

Q14a. Do you believe directors on your company's board are knowledgeable about plans to deal with a possible data breach?	FY2019	FY2018	FY2017
Yes	40%	35%	39%
No	60%	65%	61%
Total	100%	100%	100%

Q14b. If yes, why do you believe board members are knowledgeable? Please select all that apply.	FY2019	FY2018	FY2017
They regularly participate in detailed reviews of our data breach response plan	11%	10%	11%
They understand the specific security threats facing our organization	39%	35%	40%
They provide detailed feedback about the data breach response plan	25%	23%	21%
They assume responsibility for the successful execution of the incident response plan	12%	13%	15%
They have requested to be notified ASAP if a material data breach occurs	46%	49%	56%
They participate in a high level review of the organization's data protection and privacy practices	17%	12%	9%
Total	150%	142%	152%

Q15. What types of data loss is your organization most concerned about? Please select the top two.	FY2019	FY2018	FY2017
Loss or theft of customer information	58%	60%	63%
Loss or theft of employee personal data	31%	34%	40%
Loss or theft of medical data	14%	12%	11%
Loss or theft of consumer data*	19%	21%	20%
Loss or theft of intellectual property	67%	60%	54%
Loss or theft of payment card data	11%	13%	12%
Total	200%	200%	200%

*Customer information is included in the consumer data for FY2015 and FY2016

Q16. What are the two biggest barriers to improving the ability of IT security to respond to a data breach? Please select the top three	FY2019	FY2018	FY2017*
Lack of investment in much needed technologies	15%	18%	17%
Lack of expertise	39%	37%	32%
Lack of C-suite support	7%	9%	11%
Lack of security processes for third parties that have access to our data	46%	43%	45%
Lack of visibility into end-user access of sensitive and confidential information	60%	63%	67%
Lack of understanding of unsecured IoT devices	38%	32%	29%
Proliferation of mobile devices	36%	34%	31%
Proliferation of cloud services	56%	60%	68%
None of the above	3%	4%	0%
Total	300%	300%	300%

FY2014 - FY2016 only 2 choices permitted

Q17. 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?	FY2019	FY2018	FY2017
Yes	68%	66%	63%
No	28%	31%	34%
Unsure	4%	3%	3%
Total	100%	100%	100%

Q18. Does your organization train employees to recognize and minimize spear phishing incidents?	FY2019	FY2018	FY2017
Yes	50%	47%	45%
No	50%	53%	55%
Total	100%	100%	100%

Q19. How confident is your organization in its ability to recognize and minimize spear phishing incidents?	FY2019	FY2018	FY2017
Very confident	10%	13%	15%
Confident	13%	12%	16%
Somewhat confident	22%	26%	25%
Not confident	34%	30%	26%
No confidence	21%	19%	18%
Total	100%	100%	100%

Q20a. In the past 12 months, did your organization experience one or more spear phishing attacks?	FY2019
Yes	69%
No	31%
Total	100%

Q20b. How significant were the negative consequences of the spear phishing attacks?	FY2019
Very significant	22%
Significant	45%
Not significant	23%
Minimal	10%
Total	100%

Q21. How confident is your organization in its ability to deal with ransomware?	FY2019	FY2018	FY2017
Very confident	8%	11%	10%
Confident	12%	10%	11%
Somewhat confident	17%	20%	18%
Not confident	36%	34%	36%
No confidence	27%	25%	25%
Total	100%	100%	100%

Q22a. Did your organization **ever** experience a ransomware attack?	FY2019
Yes	36%
No	60%
Unsure	4%
Total	100%

Q22b. If yes, how much was the ransom?	FY2019
Less than $100	6%
$100 to $500	9%
$501 to $1,000	17%
$1,001 to $5,000	24%
$5,001 to $10,000	18%
More than $10,000	26%
Total	100%
Extrapolated value	$ 6,128

Q22c. Did your company pay the ransom?	FY2019
Yes	68%
No	32%
Total	100%

Q23. Have you taken the following steps to prepare for a ransomware incident? Please select all that apply.	FY2019	FY2018	FY2017
Determined under what circumstances payment would be made to resolve the incident	12%	10%	12%
Audited and increased back up of data and systems	63%	59%	55%
Business continuity plan includes a planned system outage in the event of a ransomware incident	49%	46%	42%
Employees are educated about the ransomware risk	34%	35%	36%
Updating software on a regular basis	25%	23%	26%
None of the above	30%	37%	39%
Other	2%	3%	4%
Total	215%	213%	214%

Q24a. 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?	FY2019	FY2018	FY2017
Yes	72%	73%	68%
No	28%	27%	32%
Total	100%	100%	100%

Q24b. If yes, how often is training conducted?	FY2019	FY2018	FY2017
On-boarding new employees	49%	51%	45%
Every six months	2%	2%	3%
Annually	24%	26%	27%
Sporadically	25%	21%	24%
Unsure	0%	0%	1%
Total	100%	100%	100%

Q24c. Are the awareness and training programs regularly reviewed and updated to ensure the content addresses the areas of greatest risk to the organization?	FY2019	FY2018	FY2017
Yes	59%	60%	54%
No	38%	35%	42%
Unsure	3%	5%	4%
Total	100%	100%	100%

Q25. How significant is the influence of employee negligence on your organization's overall security posture?	FY2019	FY2018	FY2017
Very significant	53%	45%	39%
Significant	34%	39%	41%
Not significant	10%	11%	14%
Minimal	3%	5%	6%
Total	100%	100%	100%

Q26a. Does your organization have a data breach or cyber insurance policy?	FY2019	FY2018	FY2017
Yes	49%	47%	45%
No	51%	53%	55%
Total	100%	100%	100%

Q26b. If no, does your organization plan to purchase a data breach or cyber insurance policy?	FY2019	FY2018	FY2017
Yes, within the next six months	25%	24%	21%
Yes, within the next year	25%	23%	24%
Yes, within the next two years	8%	9%	11%
No plans to purchase	39%	42%	40%
Unsure	3%	2%	4%
Total	100%	100%	100%

Q27. What types of incidents does your organization's cyber insurance cover? Please select all that apply.	FY2019	FY2018	FY2017
External attacks by cyber criminals	83%	81%	80%
Malicious or criminal insiders	65%	56%	63%
System or business process failures	31%	33%	35%
Human error, mistakes and negligence	38%	39%	36%
Incidents affecting business partners, vendors or other third parties that have access to your company's information assets	58%	64%	60%
Ransomware attacks	53%	50%	54%
Major security vulnerability in a product, website or service	49%	45%	44%
Other	7%	5%	9%
Unsure	5%	6%	7%
Total	389%	379%	388%

Q28. What coverage does this insurance offer your company? Please select all that apply.	FY2019	FY2018	FY2017
Identity protection services to victims	72%	67%	64%
Call center support	63%	60%	59%
Forensics and investigative costs	64%	62%	63%
Notification costs to data breach victims	69%	70%	69%
Communication costs to regulators	12%	10%	13%
Employee productivity losses	7%	9%	8%
Replacement of lost or damaged equipment	48%	45%	49%
Revenue losses	19%	20%	23%
Legal defense costs	73%	71%	70%
Regulatory penalties and fines	34%	35%	39%
Third-party liability	65%	67%	61%
Brand damages	5%	6%	5%
IoT enabled device protection	16%	13%	9%
Other	6%	6%	7%
Unsure	3%	4%	5%
Total	556%	545%	544%

Q29. 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.	FY2019	FY2018	FY2017
Require they have an incident response plan your organization can review	86%	89%	85%
Require they notify your organization when they have a data breach	89%	95%	90%
Require audits of their security procedures	54%	60%	56%
No steps being taken	5%	3%	5%
Total	234%	247%	236%

Q30a. Does your organization participate in an initiative or program for sharing information with government and industry peers about data breaches and incident response?	FY2019	FY2018	FY2017
Yes, currently participating	34%	30%	26%
Yes, planning to participate	23%	21%	21%
No, does not participate	41%	47%	53%
Unsure	2%	2%	0%
Total	100%	100%	100%

Q30b. 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.	FY2019	FY2018	FY2017
Improves the security posture of my organization	49%	50%	53%
Improves the effectiveness of our incident response plan	18%	19%	24%
Enhances the timeliness of incident response	29%	28%	27%
Reduces the cost of detecting and preventing data breaches	22%	19%	16%
Fosters collaboration among peers and industry groups	78%	81%	77%
Other	4%	3%	3%
Total	200%	200%	200%

Q30c. If no, why does your organization not participate in a threat-sharing program? Please select only two top choices.	FY2019	FY2018	FY2017
Cost	17%	19%	21%
Potential liability of sharing	26%	20%	23%
Anti-competitive concerns	9%	12%	15%
Lack of resources	53%	59%	61%
Lack of incentives	39%	35%	29%
No perceived benefit to my organization	54%	55%	51%
Other	2%	0%	0%
Total	200%	200%	200%

Part 3. Data breach response plan

Q31a. Does your organization have a data breach response plan in place?	FY2019	FY2018	FY2017
Yes (please skip to Q32)	94%	92%	88%
No	6%	8%	12%
Total	100%	100%	100%

Q31b. If no, why not?	FY2019	FY2018	FY2017
No resources or budget	39%	36%	38%
Not important to have data breach response plan in place	10%	11%	13%
Lack of C-level support	20%	23%	20%
Outsourced to consultants	31%	29%	29%
Other	0%	1%	0%
Total	100%	100%	100%

Please skip to 39a

Q32. How often does your company update the data breach response plan?	FY2019	FY2018	FY2017
Each quarter	3%	2%	2%
Twice per year	5%	4%	5%
Once each year	26%	29%	27%
No set time period for reviewing and updating the plan	40%	42%	40%
We have not reviewed or updated since the plan was put in place	26%	23%	26%
Total	100%	100%	100%

Q33. In addition to documenting and practicing your data breach plan, does your organization take any of the following additional steps to prepare? Please select all that apply.	FY2019	FY2018	FY2017
Conduct third-party cyber security assessments	57%	54%	48%
Integrate data breach response into business continuity plans	56%	52%	51%
Create a “standby website” for content that can be made live when an incident occurs	34%	31%	33%
Regularly review physical security and access to confidential information	73%	70%	65%
Meet with law enforcement and/or state regulators in advance of an incident	14%	16%	13%
Subscribe to a dark web monitoring service	26%	19%	21%
Conduct background checks on new full time employees and vendors	69%	65%	62%
Total	329%	307%	293%

Q34. Does your data breach response plan include the following requirements? Please select all that apply.	FY2019	FY2018	FY2017
Required C-level approval of the data breach response plan	75%	79%	75%
Contact information for all members of the data breach response team	93%	95%	94%
Contact information for all members of the data breach backup response team	42%	44%	40%
Procedures for communicating with employees when a data breach occurs	55%	56%	55%
Procedures for responding to a data breach involving overseas locations	48%	46%	41%
Procedures for communicating with state attorneys general and regulators	71%	67%	69%
Procedures for communications with investors	51%	52%	50%
Procedures for communications with business partners and other third parties	54%	50%	46%
Review of a third party or business partner's incident response plan	39%	36%	32%
Procedures for determining and offering identity theft protection services	38%	37%	39%
Procedures for reporting results of the forensics investigation to senior management	36%	33%	28%
Procedures for incorporating findings from the forensics investigations into the security strategy	30%	31%	28%
None of the above	6%	5%	4%
Total	638%	631%	601%

Q35. Does your data breach response plan offer guidance on managing the following security incidents? Please check all that apply.	FY2019	FY2018	FY2017
Loss or theft of payment information, including credit cards	77%	74%	69%
Loss or theft of personally identifiable information	83%	80%	71%
Destructive malware such as ransomware	59%	62%	63%
IoT-based attacks	27%	20%	14%
Hacktivism/activism	36%	39%	40%
Attacks via the Internet or social media	61%	59%	62%
W-2 and other phishing fraud scams	60%	57%	58%
Distributed denial of service attack (DDoS) that causes a system outage	90%	87%	88%
Loss or theft of information about customer affiliations/associations that would result in damage to your organization’s reputation	80%	79%	81%
Loss or theft of intellectual property or confidential business information	78%	73%	69%
Data breach caused by a malicious employee or contractor	59%	61%	62%
Your organization is threatened with extortion as a result of the theft of sensitive and confidential information	62%	55%	60%
Loss or theft of paper documents and tapes containing sensitive and confidential information	37%	34%	36%
None of the above	4%	6%	5%
Total	813%	786%	778%

Q36. 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.	FY2019	FY2018	FY2017
1 to 2	32%	35%	38%
3 to 4	24%	26%	30%
5 to 6	21%	19%	15%
7 to 8	14%	12%	10%
9 to 10	9%	8%	7%
Total	100%	100%	100%
Extrapolated value	4.38	4.14	3.86

Q37. 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.	FY2019	FY2018	FY2017
1 to 2	10%	11%	10%
3 to 4	10%	12%	15%
5 to 6	23%	25%	26%
7 to 8	31%	32%	30%
9 to 10	26%	20%	19%
Total	100%	100%	100%
Extrapolated value	6.56	6.26	6.16

Q38. How could your data breach response plan become more effective? Please select all that apply.	FY2019	FY2018	FY2017
Conduct more fire drills to practice data breach response	78%	80%	85%
Have formal documentation of incident response procedures	59%	65%	62%
Incorporate what was learned from previous data breaches	74%	70%	66%
Ensure seamless coordination among all departments involved in incident response	40%	45%	40%
Increase participation and oversight from senior executives	79%	81%	80%
Assign individuals with a high level of expertise in security to the team	82%	78%	75%
Assign individuals with a high level of expertise in compliance with privacy, data protection laws and regulations to the team	45%	47%	48%
Have a budget dedicated to data breach preparedness	62%	63%	60%
Increase involvement of third-party experts	50%	48%	44%
None of the above	2%	3%	2%
Total	571%	580%	562%

Q39a. Does your organization practice responding to a data breach?	FY2019	FY2018	FY2017
Yes	75%	73%	71%
No	25%	27%	29%
Total	100%	100%	100%

Q39b. If yes, how often is the response practiced?	FY2019	FY2018	FY2017
At least twice a year	45%	50%	44%
Once each year	17%	16%	19%
Every two years	6%	5%	4%
More than two years	8%	7%	9%
Never	3%	0%	0%
No set schedule	21%	22%	24%
Total	100%	100%	100%

Q39c. If yes, what is included in the practice response? Please check all that apply.	FY2019	FY2018	FY2017
Fire drills	63%	67%	65%
Case discussions	51%	49%	46%
Simulations	65%		
Training and awareness about security threats facing the organization	69%	71%	68%
Review of the plan by the person/function most responsible for data breach response	78%	80%	77%
Review of data breach communications plans	54%	50%	52%
Review of what was learned from previous data breaches or other security incidents	67%	79%	75%
None of the above	8%	9%	11%
Other	2%	3%	4%
Total	457%	408%	398%

Q39d. If no, why not? Please check all that apply.	FY2019	FY2018	FY2017
Not enough budget	31%	33%	37%
We are confident in our ability to respond to a data breach	45%	40%	45%
Too difficult to schedule a practice response	76%	78%	73%
Not a priority	60%	57%	61%
Total	212%	208%	216%

Q40a. Does your incident response plan include processes to manage an international data breach?	FY2019	FY2018	FY2017
Yes	64%	59%	54%
No	33%	37%	41%
Unsure	3%	4%	5%
Total	100%	100%	100%

Q40b. If yes, is your organization’s plan specific to each location where it operates?	FY2019	FY2018	FY2017
Yes	57%	51%	50%
No	40%	45%	46%
Unsure	3%	4%	4%
Total	100%	100%	100%

Q41. How confident is your organization in its ability to deal with an international data breach?	FY2019	FY2018	FY2017
Very confident	14%	12%	11%
Confident	20%	17%	17%
Somewhat confident	19%	28%	26%
Not confident	34%	33%	34%
No confidence	13%	10%	12%
Total	100%	100%	100%

Q42. Is your company subject to GDPR?	FY2019	FY2018
Yes	90%	86%
Unsure	7%	8%
No	3%	6%
Total	100%	100%

Q43a. 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	FY2019	FY2018
1 to 2	12%	14%
3 to 4	14%	25%
5 to 6	20%	25%
7 to 8	23%	21%
9 to 10	31%	15%
Total	100%	100%
Extrapolated value	6.44	5.46

Q43b. 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	FY2019	FY2018
1 to 2	12%	20%
3 to 4	17%	33%
5 to 6	21%	24%
7 to 8	29%	14%
9 to 10	21%	9%
Total	100%	100%
Extrapolated value	6.10	4.68

Q43c. If you rated your effectiveness 7 or higher to comply with the GDPR's data breach notification rules, why is your organization effective? Please select all that apply.	FY2019	FY2018
Our organization has the necessary security technologies in place to be able to detect the occurrence of a data breach quickly	56%	54%
Our organization's incident response plan has proven to be effective in providing timely notification	42%	38%
Our organization is able to provide notification to the data protection authority within 72 hours	21%	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"	49%	45%
Other (please specify)	2%	3%
Total	170%	162%

Q44. Since May 25, 2018, how many personal data breaches did your organization have that were required to be reported under GDPR?	FY2019
None	32%
1 to 5	39%
6 to 20	16%
More than 20	13%
Total	100%
Extrapolated value	6.50

Q45. How many of the data breaches did you report to the Regulator?	FY2019
None	45%
1 to 5	34%
6 to 20	11%
More than 20	10%
Total	100%
Extrapolated value	4.95

Q46a. Are you aware of the CCPA?	FY2019
Yes	56%
No (please skip to Part 4)	44%
Total	100%

Q46b. If yes, is your organization subject to the CCPA?	FY2019
Yes	47%
No (please skip to Part 4)	53%
Total	100%

Q47. What are the challenges to achieving and maintaining CCPA compliance? Please select the top two barriers.	FY2019
The lack of privacy or security experts knowledgeable about the CCPA	33%
Insufficient budget to invest in additional staffing	48%
Insufficient budget to invest in appropriate security technologies	29%
The need to make comprehensive changes in business practices	50%
The inability to respond to consumers’ requests to know what personal information is collected about them	38%
Other	2%
Total	200%

Part 4. Organizational characteristics & respondent demographics

D1. What organizational level best describes your current position?	FY2019	FY2018	FY2017
Senior Executive	9%	8%	7%
Vice President	10%	11%	10%
Director	25%	24%	25%
Manager	26%	25%	26%
Supervisor	18%	17%	18%
Technician	7%	8%	7%
Staff	4%	5%	6%
Contractor	0%	1%	1%
Other	1%	1%	0%
Total	100%	100%	100%

D2. Check the **Primary Person** you report to within your organization.	FY2019	FY2018	FY2017
CEO/Executive Committee	4%	5%	5%
Chief Financial Officer	4%	3%	4%
General Counsel	13%	11%	12%
Chief Privacy Officer	10%	9%	10%
Chief Information Officer	14%	15%	15%
Compliance Officer	20%	21%	19%
Human Resources VP	1%	1%	0%
Chief Security Officer	4%	3%	3%
Chief Risk Officer	11%	10%	10%
Other	1%	2%	1%
Chief Information Security Officer	18%	20%	21%
Total	100%	100%	100%

D3. What industry best describes your organization's industry focus?	FY2019	FY2018	FY2017
Communications	2%	2%	2%
Consumer products	5%	6%	5%
Defense & aerospace	1%	1%	0%
Education & research	2%	2%	1%
Energy & utilities	6%	7%	6%
Entertainment & media	3%	2%	3%
Financial services	18%	17%	18%
Health & pharmaceuticals	10%	11%	11%
Hospitality	1%	1%	1%
Industrial & manufacturing	10%	10%	11%
Public sector	10%	11%	10%
Retailing	9%	8%	9%
Services	10%	9%	9%
Technology & software	8%	8%	8%
Transportation	2%	2%	2%
Other	3%	3%	4%
Total	100%	100%	100%

D4. What is the worldwide headcount of your organization?	FY2019	FY2018	FY2017
Less than 500	11%	10%	11%
500 to 1,000	18%	19%	18%
1,001 to 5,000	25%	26%	24%
5,001 to 25,000	21%	20%	22%
25,001 to 75,000	17%	18%	17%
More than 75,000	8%	7%	8%
Total	100%	100%	100%

Survey response	US	EMEA
Sampling frame	15,590	12,881
Total returns	713	513
Rejected or screened surveys	63	57
Final sample	650	456
Response rate	4.2%	3.5%
Sample weights	58.8%	41.2%

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?	US	EMEA
Yes	63%	55%
No	26%	32%
Unsure	11%	13%
Total	100%	100%

Q1b. If yes, how frequently did these incidents occur during the past 2 years?	US	EMEA
Only once	31%	33%
2 to 3 times	33%	35%
4 to 5 times	24%	22%
More than 5 times	12%	10%
Total	100%	100%

Q1c. If yes, were any of these breaches international or global in scope?	US	EMEA
Yes	45%	50%
No	49%	40%
Unsure	6%	10%
Total	100%	100%

Attributions. Please rate each statement using the scale provided below each item. Strongly agree and agree response	US	EMEA
Q2. My organization is prepared to respond to the theft of sensitive and confidential information that requires notification to victims and regulators.	67%	57%
Q3. My organization is prepared to respond to a data breach involving business confidential information and intellectual property.	44%	49%
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.	38%	45%
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.	44%	46%
Q6. My organization's incident response plan includes breaches involving IoT devices.	40%	38%
Q7. My organization is confident in its ability to minimize the financial and reputational consequences of a material data breach.	23%	30%
Q8. Following a data breach, a credit monitoring and/or identity theft protection product is the best protection for consumers.	62%	62%

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?	US	EMEA
Yes	74%	83%
No	26%	17%
Total	100%	100%

Q9b. If yes, how long should identity theft protection be provided?	US	EMEA
2 to 3 years	45%	43%
4 to 7 years	39%	33%
8 to 10 years	12%	18%
More than 10 years	4%	6%
Total	100%	100%

Q10. If your company had a data breach, what do you think would be the best approach to keep your customers and maintain your reputation? Please select all that apply.	US	EMEA
Free identity theft protection and credit monitoring services	74%	66%
A sincere and personal apology (not a generic notification)	26%	34%
Discounts on products or services	45%	51%
Gift cards	41%	49%
Access to a call center to respond to their concerns and provide information	33%	32%
None of the above would make a difference	24%	19%
Total	243%	251%

Q11. Which of the following issues would have the greatest impact on your organization's reputation? Please select one choice.	US	EMEA
Poor customer service	27%	23%
Cybersecurity incident	20%	10%
Labor or union dispute	2%	4%
Environmental incident	8%	15%
Data breach	22%	19%
Regulatory fines	3%	12%
Publicized lawsuits	6%	9%
Product recall	12%	8%
CEO's salary	0%	0%
Total	100%	100%

Part 2. Data breach preparedness

Q12. What best describes the maturity of your organization's privacy and data protection program?	US	EMEA
Early stage – many privacy and data protection program activities have not as yet been planned or deployed. Response to privacy and data protection issues is reactive and ad hoc. Resources are not sufficient for staffing and administration of the program.	18%	23%
Middle stage – privacy and data protection program activities are planned and defined but only partially deployed. Efforts are being made to establish business processes and workflows.	30%	33%
Late-middle stage – most privacy and data protection program activities are deployed across the enterprise. The program has C-level support and adequate budget.	33%	30%
Mature stage – privacy and data protection program activities are fully deployed and maintained across the enterprise. C-level executives are regularly informed about the effectiveness of the program. Program activities are measured with KPIs.	19%	14%
Total	100%	100%

Q13a. Do you believe your company's C-suite executives are knowledgeable about plans to deal with a possible data breach?	US	EMEA
Yes	55%	61%
No	45%	39%
Total	100%	100%

Q13b. If yes, why do you believe your company's C-suite executives are knowledgeable? Please select all that apply.	US	EMEA
They regularly participate in detailed reviews of our data breach response plan	26%	32%
They understand the specific security threats facing our organization	40%	41%
They provide detailed feedback about the data breach response plan	25%	26%
They assume responsibility for the successful execution of the incident response plan	24%	19%
They have requested to be notified ASAP if a material data breach occurs	52%	58%
They participate in a high level review of the organization's data protection and privacy practices	15%	21%
Total	182%	197%

Q14a. Do you believe directors on your company's board are knowledgeable about plans to deal with a possible data breach?	US	EMEA
Yes	40%	35%
No	60%	65%
Total	100%	100%

Q14b. If yes, why do you believe board members are knowledgeable? Please select all that apply.	US	EMEA
They regularly participate in detailed reviews of our data breach response plan	11%	14%
They understand the specific security threats facing our organization	39%	45%
They provide detailed feedback about the data breach response plan	25%	21%
They assume responsibility for the successful execution of the incident response plan	12%	14%
They have requested to be notified ASAP if a material data breach occurs	46%	53%
They participate in a high level review of the organization's data protection and privacy practices	17%	20%
Total	150%	167%

Q15. What types of data loss is your organization most concerned about? Please select the top two.	US	EMEA
Loss or theft of customer information	58%	54%
Loss or theft of employee personal data	31%	32%
Loss or theft of medical data	14%	18%
Loss or theft of consumer data*	19%	18%
Loss or theft of intellectual property	67%	63%
Loss or theft of payment card data	11%	15%
Total	200%	200%

Q16. What are the two biggest barriers to improving the ability of IT security to respond to a data breach? Please select the top three	US	EMEA
Lack of investment in much needed technologies	15%	13%
Lack of expertise	39%	37%
Lack of C-suite support	7%	11%
Lack of security processes for third parties that have access to our data	46%	47%
Lack of visibility into end-user access of sensitive and confidential information	60%	58%
Lack of understanding of unsecured IoT devices	38%	31%
Proliferation of mobile devices	36%	40%
Proliferation of cloud services	56%	55%
None of the above	3%	8%
Total	300%	300%

Q17. 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?	US	EMEA
Yes	68%	63%
No	28%	29%
Unsure	4%	8%
Total	100%	100%

Q18. Does your organization train employees to recognize and minimize spear phishing incidents?	US	EMEA
Yes	50%	56%
No	50%	44%
Total	100%	100%

Q19. How confident is your organization in its ability to recognize and minimize spear phishing incidents?	US	EMEA
Very confident	10%	15%
Confident	13%	20%
Somewhat confident	22%	25%
Not confident	34%	25%
No confidence	21%	15%
Total	100%	100%

Q20a. In the past 12 months, did your organization experience one or more spear phishing attacks?	US	EMEA
Yes	69%	58%
No	31%	42%
Total	100%	100%

Q20b. How significant were the negative consequences of the spear phishing attacks?	US	EMEA
Very significant	22%	26%
Significant	45%	40%
Not significant	23%	25%
Minimal	10%	9%
Total	100%	100%

Q21. How confident is your organization in its ability to deal with ransomware?	US	EMEA
Very confident	8%	14%
Confident	12%	20%
Somewhat confident	17%	17%
Not confident	36%	29%
No confidence	27%	20%
Total	100%	100%

Q22a. Did your organization **ever** experience a ransomware attack?	US	EMEA
Yes	36%	35%
No	60%	58%
Unsure	4%	7%
Total	100%	100%

Q22b. If yes, how much was the ransom?	US	EMEA
Less than $100	6%	12%
$100 to $500	9%	15%
$501 to $1,000	17%	19%
$1,001 to $5,000	24%	26%
$5,001 to $10,000	18%	12%
More than $10,000	26%	16%
Total	100%	100%
Extrapolated value	$ 6,128	$ 4,274

Q22c. Did your company pay the ransom?	US	EMEA
Yes	68%	50%
No	32%	50%
Total	100%	100%

Q23. Have you taken the following steps to prepare for a ransomware incident? Please select all that apply.	US	EMEA
Determined under what circumstances payment would be made to resolve the incident	12%	10%
Audited and increased back up of data and systems	63%	67%
Business continuity plan includes a planned system outage in the event of a ransomware incident	49%	51%
Employees are educated about the ransomware risk	34%	39%
Updating software on a regular basis	25%	26%
None of the above	30%	26%
Other	2%	5%
Total	215%	224%

Q24a. 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?	US	EMEA
Yes	72%	65%
No	28%	35%
Total	100%	100%

Q24b. If yes, how often is training conducted?	US	EMEA
On-boarding new employees	49%	43%
Every six months	2%	1%
Annually	24%	28%
Sporadically	25%	26%
Unsure	0%	2%
Total	100%	100%

Q24c. Are the awareness and training programs regularly reviewed and updated to ensure the content addresses the areas of greatest risk to the organization?	US	EMEA
Yes	59%	60%
No	38%	35%
Unsure	3%	5%
Total	100%	100%

Q25. How significant is the influence of employee negligence on your organization's overall security posture?	US	EMEA
Very significant	53%	45%
Significant	34%	39%
Not significant	10%	11%
Minimal	3%	5%
Total	100%	100%

Q26a. Does your organization have a data breach or cyber insurance policy?	US	EMEA
Yes	49%	46%
No	51%	54%
Total	100%	100%

Q26b. If no, does your organization plan to purchase a data breach or cyber insurance policy?	US	EMEA
Yes, within the next six months	25%	28%
Yes, within the next year	25%	21%
Yes, within the next two years	8%	11%
No plans to purchase	39%	38%
Unsure	3%	2%
Total	100%	100%

Q27. What types of incidents does your organization's cyber insurance cover? Please select all that apply.	US	EMEA
External attacks by cyber criminals	83%	78%
Malicious or criminal insiders	65%	53%
System or business process failures	31%	30%
Human error, mistakes and negligence	38%	42%
Incidents affecting business partners, vendors or other third parties that have access to your company's information assets	58%	61%
Ransomware attacks	53%	54%
Major security vulnerability in a product, website or service	49%	42%
Other	7%	6%
Unsure	5%	7%
Total	389%	373%

Q28. What coverage does this insurance offer your company? Please select all that apply.	US	EMEA
Identity protection services to victims	72%	62%
Call center support	63%	53%
Forensics and investigative costs	64%	59%
Notification costs to data breach victims	69%	71%
Communication costs to regulators	12%	9%
Employee productivity losses	7%	6%
Replacement of lost or damaged equipment	48%	42%
Revenue losses	19%	23%
Legal defense costs	73%	68%
Regulatory penalties and fines	34%	32%
Third-party liability	65%	67%
Brand damages	5%	3%
IoT enabled device protection	16%	12%
Other	6%	9%
Unsure	3%	5%
Total	556%	521%

Q29. 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.	US	EMEA
Require they have an incident response plan your organization can review	86%	79%
Require they notify your organization when they have a data breach	89%	93%
Require audits of their security procedures	54%	55%
No steps being taken	5%	8%
Total	234%	235%

Q30a. Does your organization participate in an initiative or program for sharing information with government and industry peers about data breaches and incident response?	US	EMEA
Yes, currently participating	34%	27%
Yes, planning to participate	23%	25%
No, does not participate	41%	43%
Unsure	2%	5%
Total	100%	100%

Q30b. 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.	US	EMEA
Improves the security posture of my organization	49%	54%
Improves the effectiveness of our incident response plan	18%	23%
Enhances the timeliness of incident response	29%	32%
Reduces the cost of detecting and preventing data breaches	22%	18%
Fosters collaboration among peers and industry groups	78%	67%
Other	4%	6%
Total	200%	200%

Q30c. If no, why does your organization not participate in a threat-sharing program? Please select only two top choices.	US	EMEA
Cost	17%	20%
Potential liability of sharing	26%	27%
Anti-competitive concerns	9%	13%
Lack of resources	53%	61%
Lack of incentives	39%	25%
No perceived benefit to my organization	54%	52%
Other	2%	2%
Total	200%	200%

Part 3. Data breach response plan

Q31a. Does your organization have a data breach response plan in place?	US	EMEA
Yes (please skip to Q32)	94%	88%
No	6%	12%
Total	100%	100%

Q31b. If no, why not?	US	EMEA
No resources or budget	39%	40%
Not important to have data breach response plan in place	10%	12%
Lack of C-level support	20%	14%
Outsourced to consultants	31%	32%
Other	0%	2%
Total	100%	100%

Please skip to 39a

Q32. How often does your company update the data breach response plan?	US	EMEA
Each quarter	3%	5%
Twice per year	5%	5%
Once each year	26%	23%
No set time period for reviewing and updating the plan	40%	42%
We have not reviewed or updated since the plan was put in place	26%	25%
Total	100%	100%

Q33. In addition to documenting and practicing your data breach plan, does your organization take any of the following additional steps to prepare? Please select all that apply.	US	EMEA
Conduct third-party cyber security assessments	57%	60%
Integrate data breach response into business continuity plans	56%	56%
Create a “standby website” for content that can be made live when an incident occurs	34%	35%
Regularly review physical security and access to confidential information	73%	68%
Meet with law enforcement and/or state regulators in advance of an incident	14%	19%
Subscribe to a dark web monitoring service	26%	22%
Conduct background checks on new full time employees and vendors	69%	57%
Total	329%	317%

Q34. Does your data breach response plan include the following requirements? Please select all that apply.	US	EMEA
Required C-level approval of the data breach response plan	75%	67%
Contact information for all members of the data breach response team	93%	90%
Contact information for all members of the data breach backup response team	42%	45%
Procedures for communicating with employees when a data breach occurs	55%	52%
Procedures for responding to a data breach involving overseas locations	48%	43%
Procedures for communicating with state attorneys general and regulators	71%	64%
Procedures for communications with investors	51%	51%
Procedures for communications with business partners and other third parties	54%	45%
Review of a third party or business partner’s incident response plan	39%	34%
Procedures for determining and offering identity theft protection services	38%	37%
Procedures for reporting results of the forensics investigation to senior management	36%	35%
Procedures for incorporating findings from the forensics investigations into the security strategy	30%	33%
None of the above	6%	5%
Total	638%	601%

Q35. Does your data breach response plan offer guidance on managing the following security incidents? Please check all that apply.	US	EMEA
Loss or theft of payment information, including credit cards	77%	74%
Loss or theft of personally identifiable information	83%	80%
Destructive malware such as ransomware	59%	62%
IoT-based attacks	27%	20%
Hacktivism/activism	36%	39%
Attacks via the Internet or social media	61%	55%
W-2 and other phishing fraud scams	60%	57%
Distributed denial of service attack (DDoS) that causes a system outage	90%	78%
Loss or theft of information about customer affiliations/associations that would result in damage to your organization’s reputation	80%	74%
Loss or theft of intellectual property or confidential business information	78%	65%
Data breach caused by a malicious employee or contractor	59%	66%
Your organization is threatened with extortion as a result of the theft of sensitive and confidential information	62%	57%
Loss or theft of paper documents and tapes containing sensitive and confidential information	37%	35%
None of the above	4%	5%
Total	813%	767%

Q36. 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.	US	EMEA
1 to 2	32%	25%
3 to 4	24%	29%
5 to 6	21%	18%
7 to 8	14%	11%
9 to 10	9%	17%
Total	100%	100%
Extrapolated value	4.38	4.82

Q37. 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.	US	EMEA
1 to 2	10%	12%
3 to 4	10%	13%
5 to 6	23%	23%
7 to 8	31%	29%
9 to 10	26%	23%
Total	100%	100%
Extrapolated value	6.56	6.26

Q38. How could your data breach response plan become more effective? Please select all that apply.	US	EMEA
Conduct more fire drills to practice data breach response	78%	68%
Have formal documentation of incident response procedures	59%	57%
Incorporate what was learned from previous data breaches	74%	70%
Ensure seamless coordination among all departments involved in incident response	40%	43%
Increase participation and oversight from senior executives	79%	67%
Assign individuals with a high level of expertise in security to the team	82%	79%
Assign individuals with a high level of expertise in compliance with privacy, data protection laws and regulations to the team	45%	50%
Have a budget dedicated to data breach preparedness	62%	61%
Increase involvement of third-party experts	50%	47%
None of the above	2%	1%
Total	571%	543%

Q39a. Does your organization practice responding to a data breach?	US	EMEA
Yes	75%	67%
No	25%	33%
Total	100%	100%

Q39b. If yes, how often is the response practiced? Please check all that apply.	US	EMEA
At least twice a year	45%	46%
Once each year	17%	19%
Every two years	6%	8%
More than two years	8%	9%
Never	3%	1%
No set schedule	21%	17%
Total	100%	100%

Q39c. If yes, what is included in the practice response? Please check all that apply.	US	EMEA
Fire drills	63%	58%
Case discussions	51%	54%
Simulations	65%	55%
Training and awareness about security threats facing the organization	69%	73%
Review of the plan by the person/function most responsible for data breach response	78%	69%
Review of data breach communications plans	54%	50%
Review of what was learned from previous data breaches or other security incidents	67%	69%
None of the above	8%	10%
Other	2%	4%
Total	457%	442%

Q39d. If no, why not? Please check all that apply.	US	EMEA
Not enough budget	31%	28%
We are confident in our ability to respond to a data breach	45%	49%
Too difficult to schedule a practice response	76%	69%
Not a priority	60%	56%
Total	212%	202%

Q40a. Does your incident response plan include processes to manage an international data breach?	US	EMEA
Yes	64%	61%
No	33%	37%
Unsure	3%	2%
Total	100%	100%

Q40b. If yes, is your organization’s plan specific to each location where it operates?	US	EMEA
Yes	57%	60%
No	40%	38%
Unsure	3%	2%
Total	100%	100%

Q41. How confident is your organization in its ability to deal with an international data breach?	US	EMEA
Very confident	14%	11%
Confident	20%	15%
Somewhat confident	19%	30%
Not confident	34%	29%
No confidence	13%	15%
Total	100%	100%

Q42. Is your company subject to GDPR?	US	EMEA
Yes	90%	84%
Unsure	7%	9%
No	3%	7%
Total	100%	100%

Q43a. 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	US	EMEA
1 to 2	12%	10%
3 to 4	14%	14%
5 to 6	20%	25%
7 to 8	23%	30%
9 to 10	31%	21%
Total	100%	100%
Extrapolated value	6.44	6.26

Q43b. 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	US	EMEA
1 to 2	12%	8%
3 to 4	17%	20%
5 to 6	21%	28%
7 to 8	29%	26%
9 to 10	21%	18%
Total	100%	100%
Extrapolated value	6.10	6.02

Q43c. If you rated your effectiveness 7 or higher to comply with the GDPR's data breach notification rules, why is your organization effective? Please select all that apply.	US	EMEA
Our organization has the necessary security technologies in place to be able to detect the occurrence of a data breach quickly	56%	59%
Our organization's incident response plan has proven to be effective in providing timely notification	42%	41%
Our organization is able to provide notification to the data protection authority within 72 hours	21%	23%
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"	49%	50%
Other (please specify)	2%	0%
Total	170%	173%

Q44. Since May 25, 2018, how many personal data breaches did your organization have that were required to be reported under GDPR?	US	EMEA
None	32%	27%
1 to 5	39%	36%
6 to 20	16%	19%
More than 20	13%	18%
Total	100%	100%
Extrapolated value	6.50	8.05

Q45. How many of the data breaches did you report to the Regulator?	US	EMEA
None	45%	39%
1 to 5	34%	37%
6 to 20	11%	13%
More than 20	10%	11%
Total	100%	100%
Extrapolated value	4.95	5.55

Q46a. Are you aware of the CCPA?	US	EMEA
Yes	56%	48%
No (please skip to Part 4)	44%	52%
Total	100%	100%

Q46b. If yes, is your organization subject to the CCPA?	US	EMEA
Yes	47%	51%
No (please skip to Part 4)	53%	49%
Total	100%	100%

Q47. What are the challenges to achieving and maintaining CCPA compliance? Please select the top two barriers.	US	EMEA
The lack of privacy or security experts knowledgeable about the CCPA	33%	38%
Insufficient budget to invest in additional staffing	48%	44%
Insufficient budget to invest in appropriate security technologies	29%	27%
The need to make comprehensive changes in business practices	50%	45%
The inability to respond to consumers' requests to know what personal information is collected about them	38%	43%
Other	2%	3%
Total	200%	200%

Part 4. Organizational characteristics & respondent demographics

D1. What organizational level best describes your current position?	US	EMEA
Senior Executive	9%	7%
Vice President	10%	8%
Director	25%	24%
Manager	26%	28%
Supervisor	18%	16%
Technician	7%	9%
Staff	4%	4%
Contractor	0%	2%
Other	1%	2%
Total	100%	100%

D2. Check the **Primary Person** you report to within your organization.	US	EMEA
CEO/Executive Committee	4%	4%
Chief Financial Officer	4%	4%
General Counsel	13%	10%
Chief Privacy Officer	10%	11%
Chief Information Officer	14%	16%
Compliance Officer	20%	19%
Human Resources VP	1%	2%
Chief Security Officer	4%	4%
Chief Risk Officer	11%	9%
Other	1%	2%
Chief Information Security Officer	18%	19%
Total	100%	100%

D3. What industry best describes your organization's industry focus?	US	EMEA
Communications	2%	1%
Consumer products	5%	4%
Defense & aerospace	1%	1%
Education & research	2%	3%
Energy & utilities	6%	7%
Entertainment & media	3%	2%
Financial services	18%	19%
Health & pharmaceuticals	10%	12%
Hospitality	1%	2%
Industrial & manufacturing	10%	9%
Public sector	10%	11%
Retailing	9%	7%
Services	10%	8%
Technology & software	8%	7%
Transportation	2%	3%
Other	3%	4%
Total	100%	100%

D4. What is the worldwide headcount of your organization?	US	EMEA
Less than 500	11%	16%
500 to 1,000	18%	23%
1,001 to 5,000	25%	31%
5,001 to 25,000	21%	18%
25,001 to 75,000	17%	8%
More than 75,000	8%	4%
Total	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.

Experian’s Reserved Response Program

Experian’s Reserved Response program is the industry’s first proactive data breach response solution that offers such expertise and dedication to today’s top organizations. The program provides organizations with a dedicated team of breach response experts and guaranteed SLAs in the event of a live breach.