Eighth 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: April 2021

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

Ponemon Institute, April 2021

Part 1. Introduction

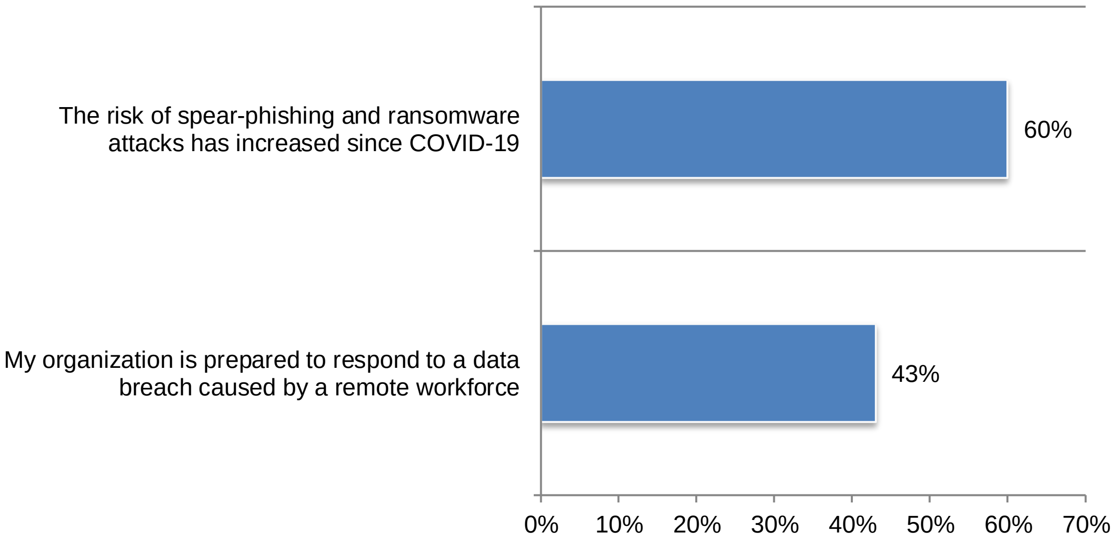
The *Eighth Annual Study: Is Your Company Ready for a Big Data Breach?* sponsored by Experian® Data Breach Resolution and conducted by Ponemon Institute focuses on the state of data breach preparedness and the importance of addressing security risks created by a remote workforce. In this year's study, we surveyed 544 professionals in the United States and 445 in EMEA[1]. A comparison of the US and EMEA findings are presented in 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.

As mentioned above, this year's research features the impact of COVID-19 and the remote workforce on data breach preparedness. We define remote working as the ability for employees and other users to perform work from locations other than the organization's facilities.

The risk of spear-phishing and ransomware attacks has increased since COVID-19. As shown in Figure 1, 60 percent of respondents say the risk of spear-phishing and ransomware attacks has increased since COVID-19. Only 43 percent say their organizations are prepared to respond to a data breach caused by a remote workforce.

Figure 1. The impact of remote working and COVID-19 on data breach preparedness
Strongly agree and Agree responses combined



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

The following research findings illustrate the steps necessary to improve an organization's data breach preparedness.

- **Fifty-six percent of respondents believe remote working will become the new norm.** They also believe it is putting organizations at risk for a data breach. In fact, almost half of data breaches experienced by organizations in this research are believed to have been the result of employees and contractors working remotely.

- **Most data breach plans do not provide guidance on how to respond to a data breach caused by a remote workforce.** Eighty-nine percent of organizations have data breach response plan. However, more than half (52 percent) of respondents say the plan does not include preparedness for a data breach caused by a remote workforce.

- **As a result of the remote workforce, the majority of organizations plan to make changes to their privacy and security practices.** These include hiring more in-house expertise, investing in enabling security technologies, conducting more training and awareness programs to ensure employees and contractors adhere to their organization's security policies while working remotely, conducting risk assessments of vulnerabilities created by a remote workforce and developing and enforcing privacy and security policies for a remote workforce.

- **Boards of directors and the C-Suite need to become more engaged in decisions to secure the remote workforce.** To ensure organizations have the necessary resources and are prepared to deal with a data breach, especially those caused by a remote workforce, the boards of directors and C-suite need to be briefed on the possible security risks. Only 46 percent of respondents say their organizations' leaders are requesting such a briefing.

- **Data breach preparedness would improve if boards of directors and the C-suite are knowledgeable about their organizations plans to deal with a possible data breach**. Less than half (46 percent) of respondents believe their leaders are knowledgeable. Those that are considered knowledgeable only participate in high level reviews of data protection and privacy practices. Instead, boards of directors and the C-suite should participate in detailed reviews of the data breach plan, understand the specific security threats facing the organization, provide feedback about the data breach response plan and assume at least some responsibility for the successful execution of the incident response plan.

- **Data breach response plans need to provide guidance on dealing with an international data breach.** Forty-nine percent of respondents who report their organizations had a data breach say it was international in scope. However, confidence in the ability to deal with an international data breach is low. Less than half of respondents (47 percent) say their data breach response plans have processes to manage such a breach.

- **Practice drills improve the effectiveness of data breach response plans.** When asked how their organization's data breach response plans could be more effective, 81 percent of respondents say it would be to conduct more practice drills. The involvement of in-house security expertise in the response plan (80 percent of respondents) and increased participation and oversight from senior executives also would improve data breach preparedness (74 percent of respondents).

- **In the future, 62 percent of respondents say there will be an increase in security incidents.** Barriers that prevent the IT security team to respond to a data breach are the lack of visibility into end-user access of sensitive and confidential information, proliferation of cloud services and lack of security processes for third parties that have access to their organizations' data, 64 percent, 56 percent and 42 percent of respondents respectively

Part 2. Key findings

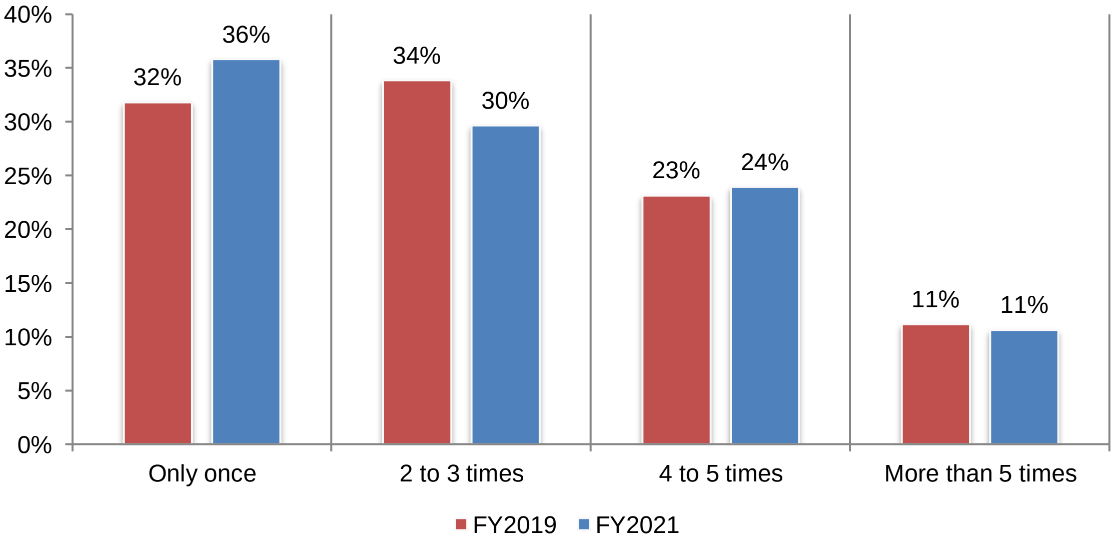
In this section, we provide an analysis of the US and EMEA results over the past one to three years as shown. The complete audited findings are presented in the Appendix of this report. Part 3 of the report presents the differences between the US and EMEA. We have organized this report according to the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

- The state of data breach preparedness
- Ransomware, spear-phishing and COVID-19
- Regulations that affect data breach preparedness
- Perceptions of the future
- US and EMEA differences in responding to a data breach

The state of data breach preparedness

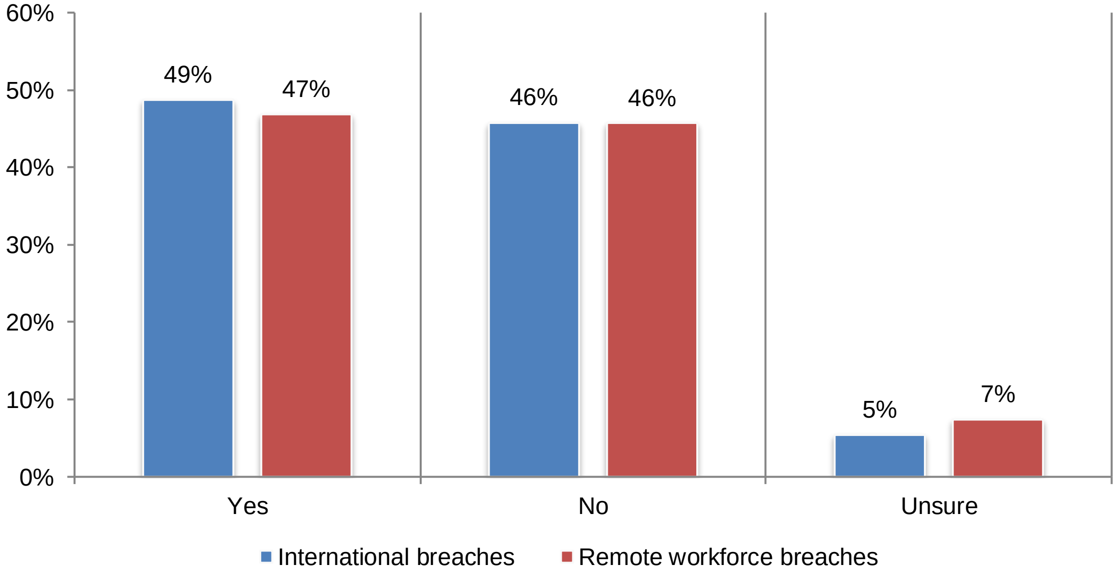
The majority of organizations (59 percent of respondents) have had a data breach involving the loss or theft of more than 1,000 records in the past two years. As shown in Figure 2, 65 percent of respondents say their organizations have had more than one data breach during this period.

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?



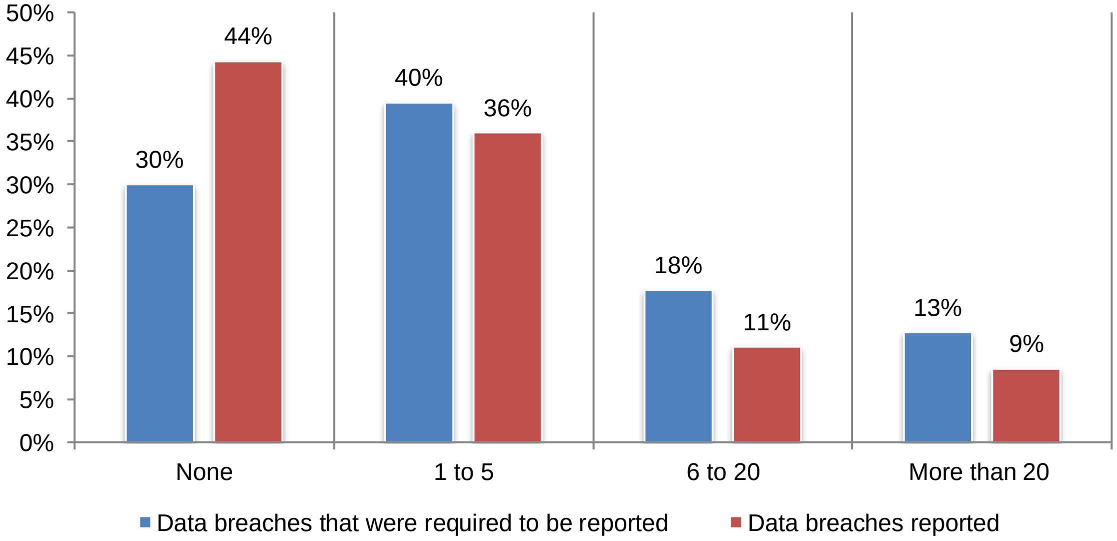
Almost half of data breaches were caused by a remote workforce (47 percent of respondents). However, as discussed previously only 43 percent of respondents say their organizations are prepared to respond to such an incident. Forty-nine percent of respondents say their organizations experienced a data breach that was international in scope, as shown in Figure 3.

Figure 3. Were these breaches international in scope and were they the result of a remote workforce?



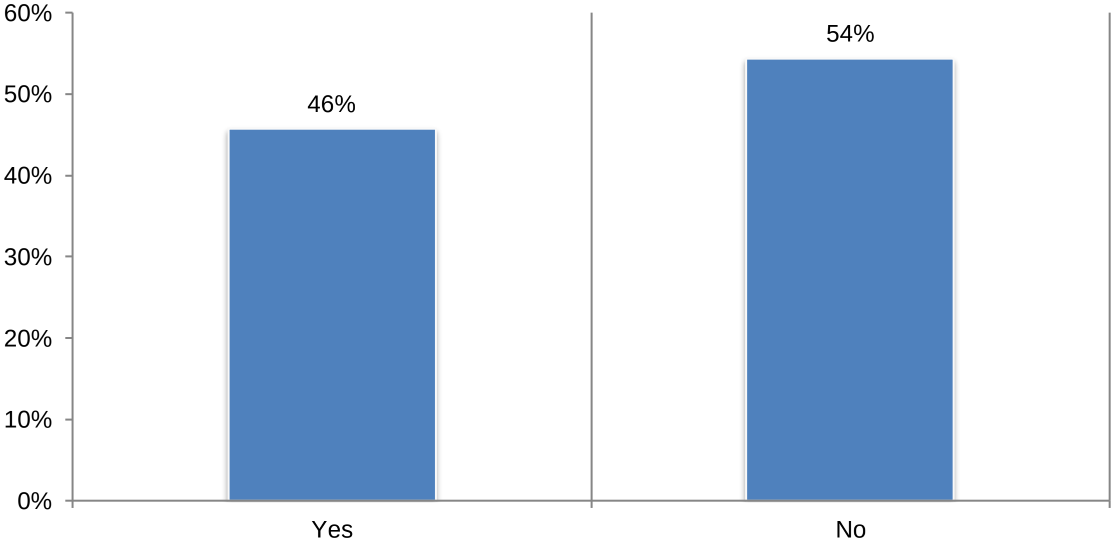
There is a difference between the number of data breaches that require reporting and those that were actually reported. As shown in Figure 4, in the past two years organizations represented in this research had an average of 7 data breaches that were required to be reported. On average, 5 were reported.

Figure 4. In the past two years, on average how many data breaches were required to be reported and how many were reported?
Extrapolated value for the number of data breaches that required reporting = 7
Extrapolated value for the number of data breaches that were reported = 5



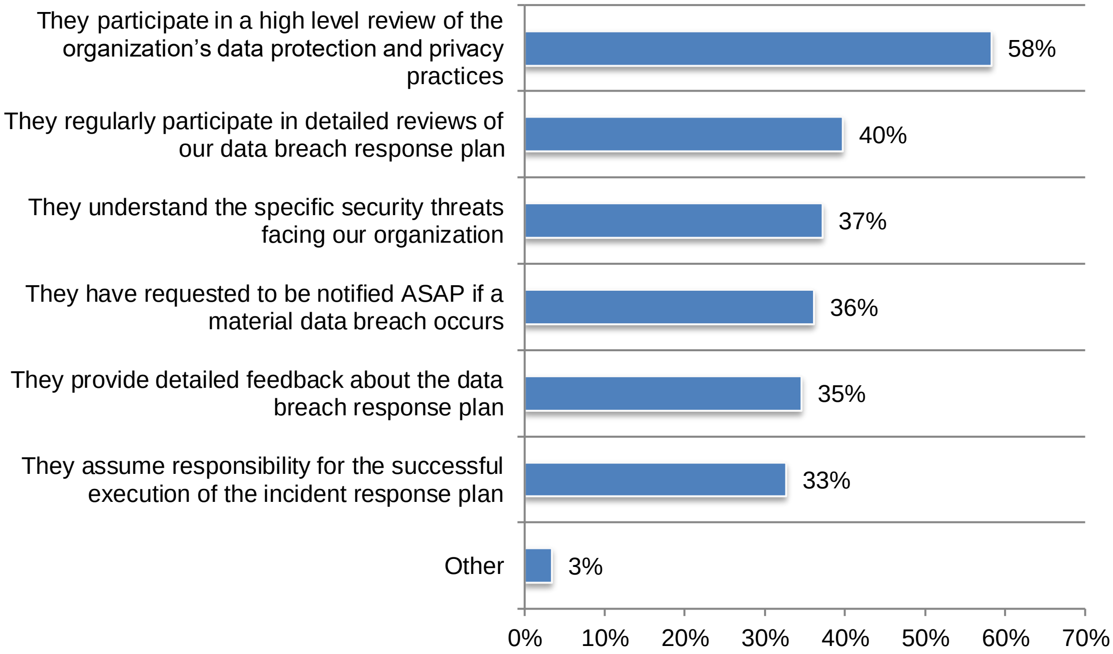
Despite the increase in a remote workforce due to COVID-19, boards of directors and executives are not briefed on the risks. As shown in Figure 5, only 46 percent of respondents say their organizations' leaders are requesting a briefing on the possible security risks to improve their ability to respond to a data breach caused by a remote workforce.

Figure 5. Has the board of directors and C-suite executives requested a briefing on possible security risks caused by a remote workforce?



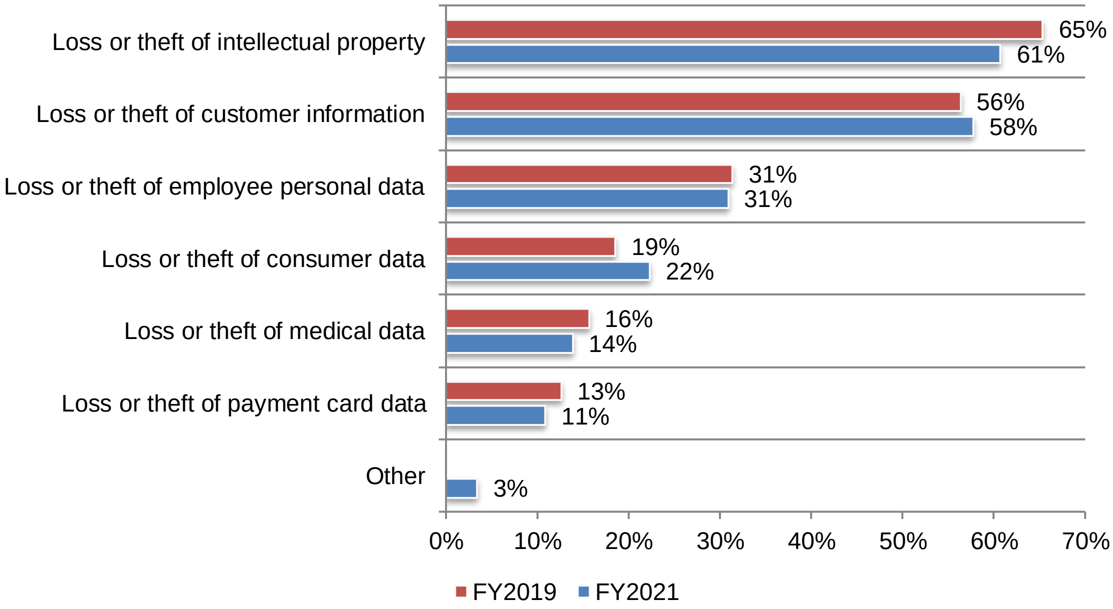
Further, less than half (46 percent) of respondents believe both their company's board of directors and C-suite executives are knowledgeable about plans to deal with a possible data breach. Indications of knowledge are presented in Figure 6. The top two indications are they participate in a high level review of the organization's data protection and privacy practices and they regularly participate in detailed reviews of their data breach response plan. Only one-third of respondents say the board of directors and the C-suite would assume responsibility for the successful execution of the incident response plan.

Figure 6. Why do you believe your company's C-suite and board of directors are knowledgeable?
More than one response permitted



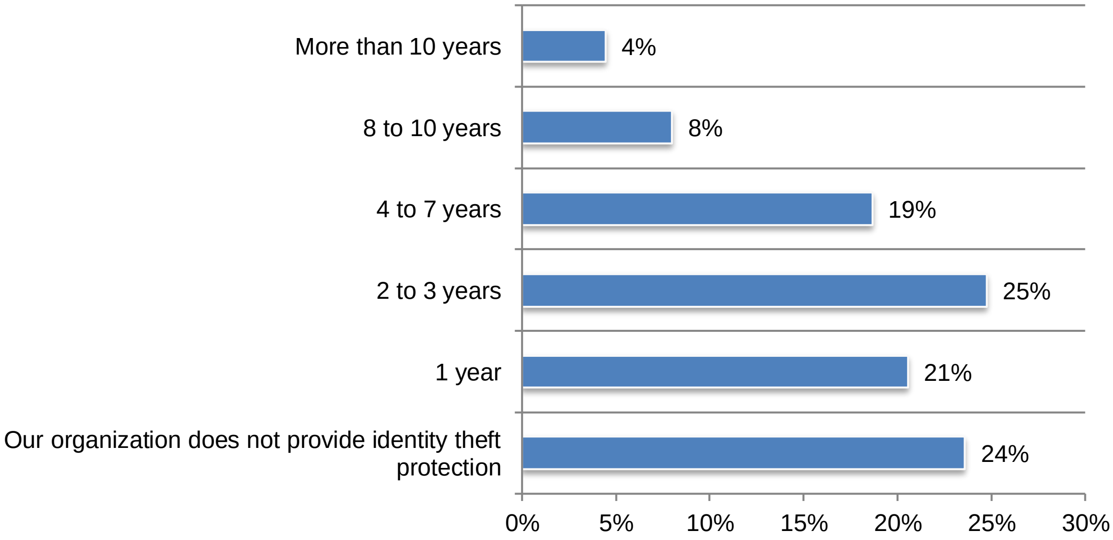
IP and customer information are considered most at risk. As shown in Figure 7, 61 percent of respondents say their organizations worry most about the loss or theft of intellectual property followed by 58 percent of respondents who say they are most concerned about the loss or theft of customer information.

Figure 7. What types of data loss is your organization most concerned about?
Two responses permitted



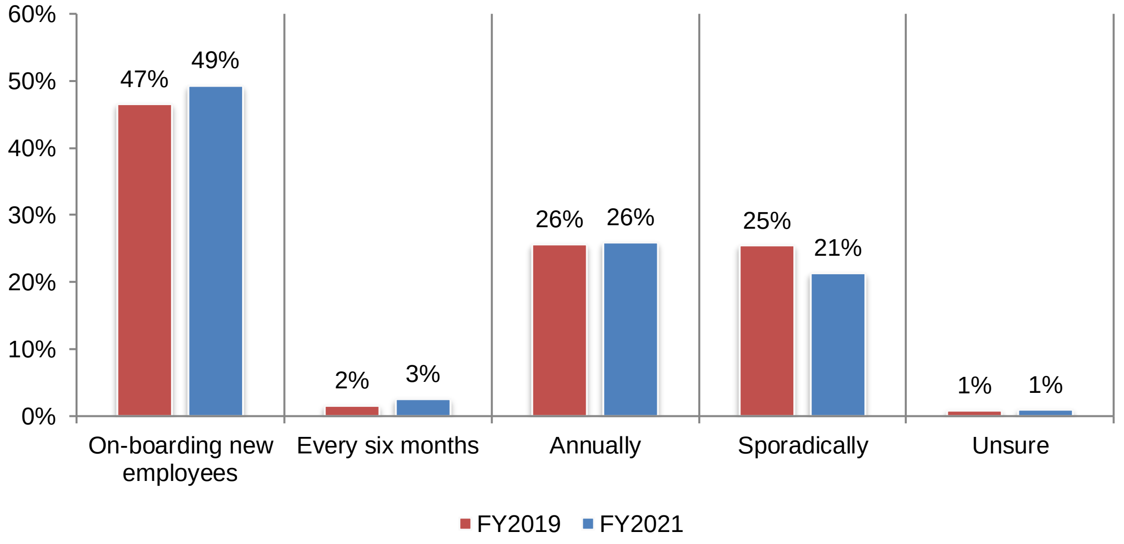
As discussed above, the loss or theft of customer information is a top concern for organizations. As shown in Figure 8, 76 percent of respondents say their organizations offer identity theft protection for at least one year. Thirty-one percent of respondents say such protection is provided for at least four years.

Figure 8. How long should identity theft protection be provided to data breach victims?



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 9, there has been little change since 2019 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.

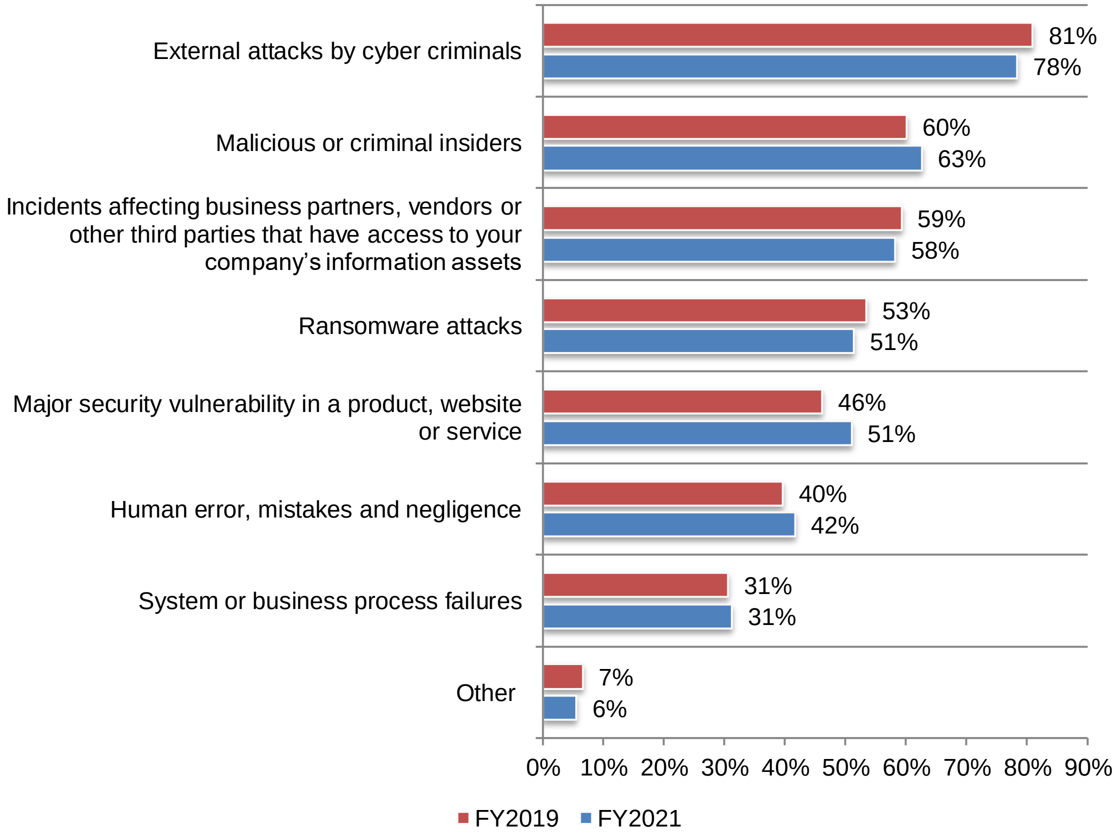
Figure 9. How often are privacy and data protection awareness training programs conducted?



As part of their data breach preparedness, organizations are purchasing cyber insurance. About half (49 percent) of respondents say their organizations have a data breach and cyber insurance policy. Of these respondents, 39 percent of respondents say their organizations have changed and increased the amount of coverage since COVID-19. Of the 51 percent of respondents who currently do not have a cyber insurance policy, 61 percent will purchase one within the next two years.

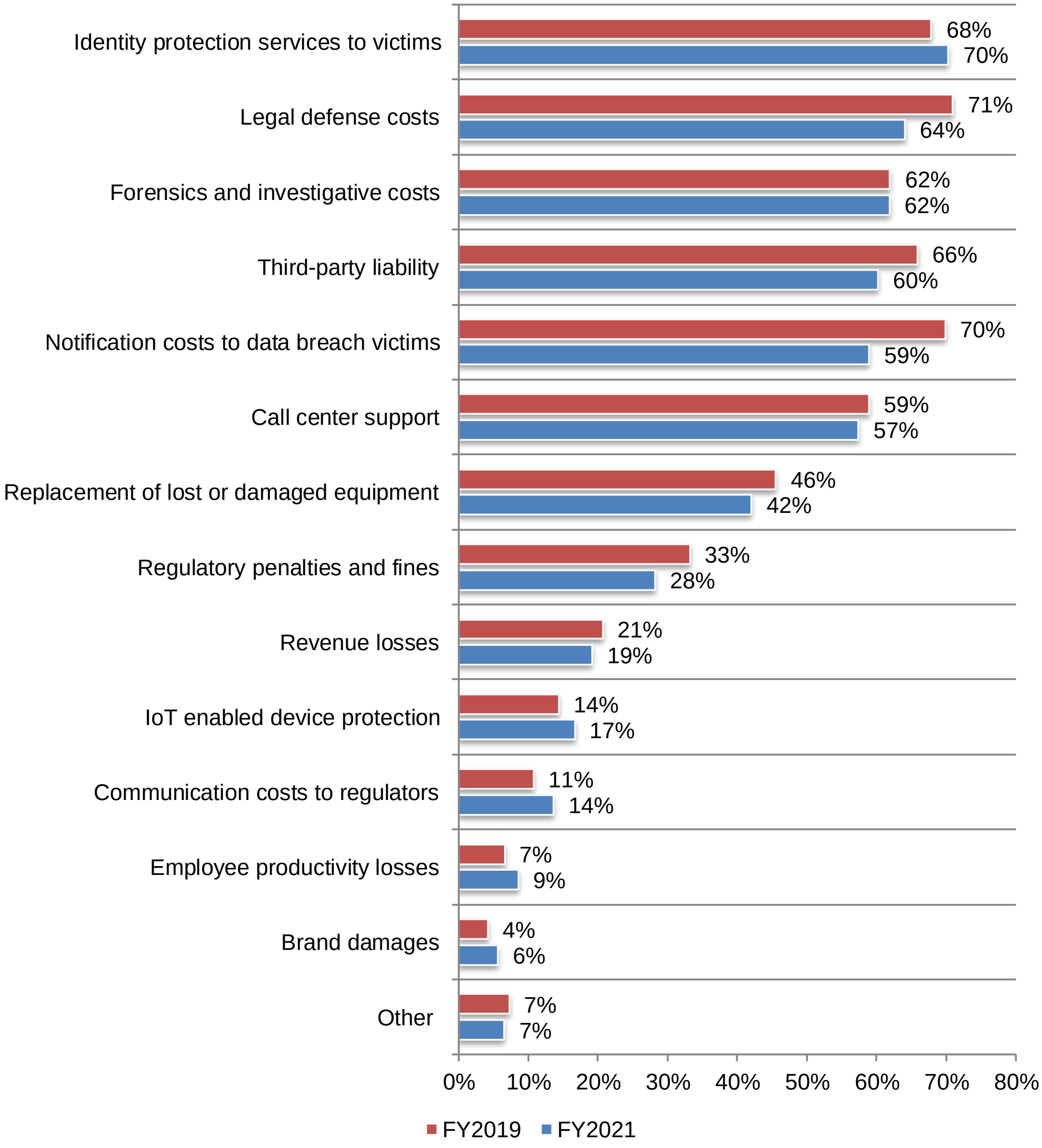
According to Figure 10, 78 percent of respondents say their cyber insurance policy covers incidents caused by cyber criminals and 63 percent of respondents say it covers malicious or criminal insiders. Only 42 percent of respondents say it covers human error, one of the major causes of a data breach.

Figure 10. What types of incidents does your organization's cyber insurance cover?
More than one response permitted



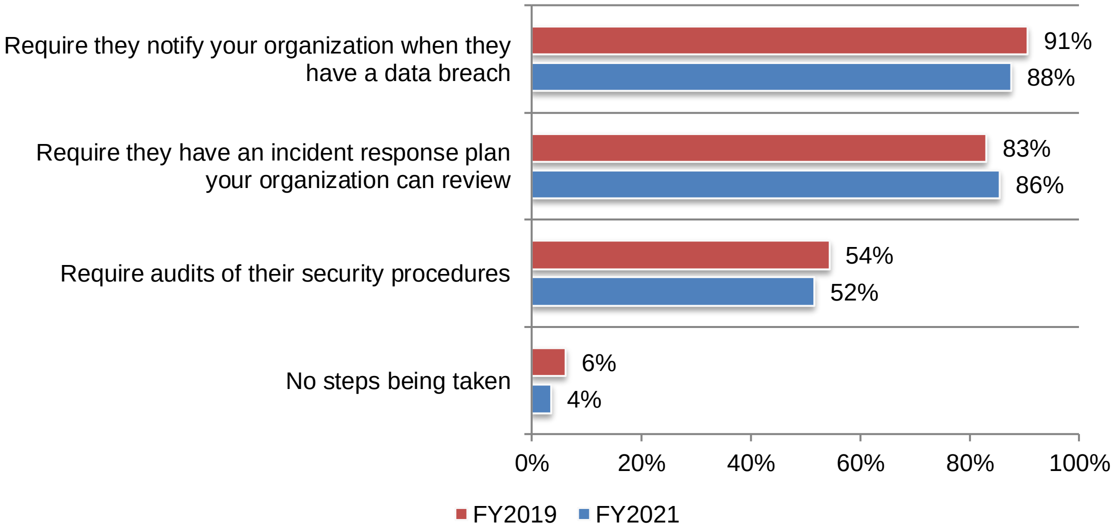
Most cyber insurance policies cover identity theft protection services to victims. Figure 11 presents the coverage provided by the cyber insurance policy. The top areas of coverage are identity protection services to victims, legal defense costs, forensics and investigative costs, and third-party liability.

Figure 11. 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 12, consistent with last year's research, 88 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.

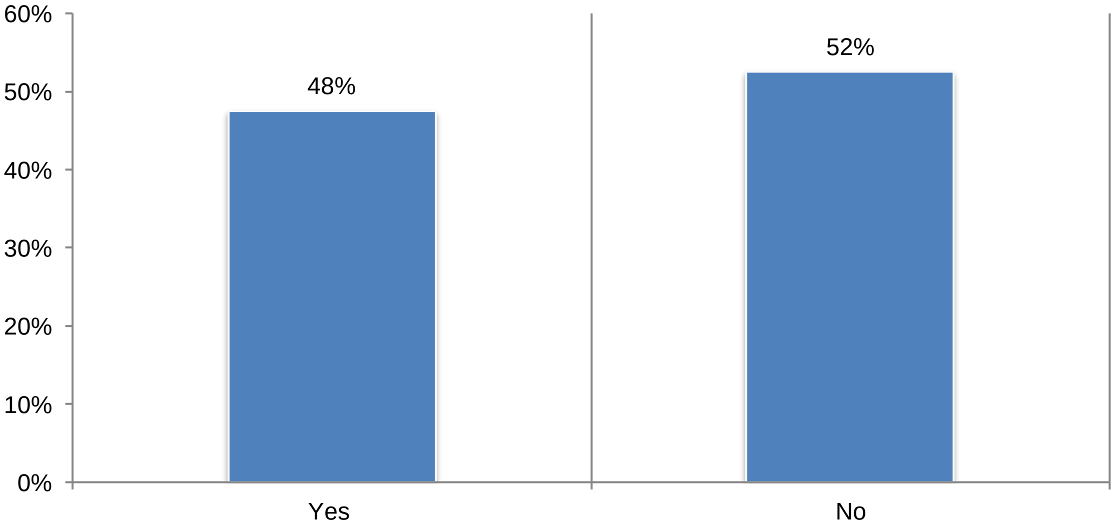
Figure 12. What steps do you take to minimize the consequences of a data breach involving a third party?
More than one response permitted



Data breach response plans

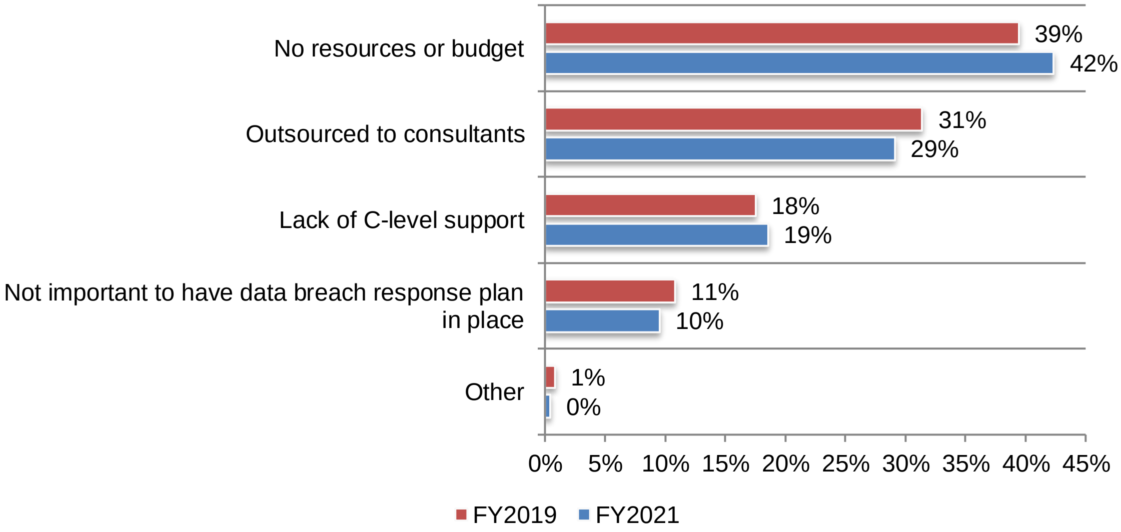
Most data breach response plans do not provide guidance on how to deal with a data breach caused by a remote workforce. Eighty-nine percent of respondents say their organizations have a data breach response plan. However, of these respondents, less than half (48 percent) say their organizations' plans include data breaches caused by a remote workforce, as shown in Figure 13.

Figure 13. Will the data breach response include guidance on how to respond to data breaches created by a remote workforce?



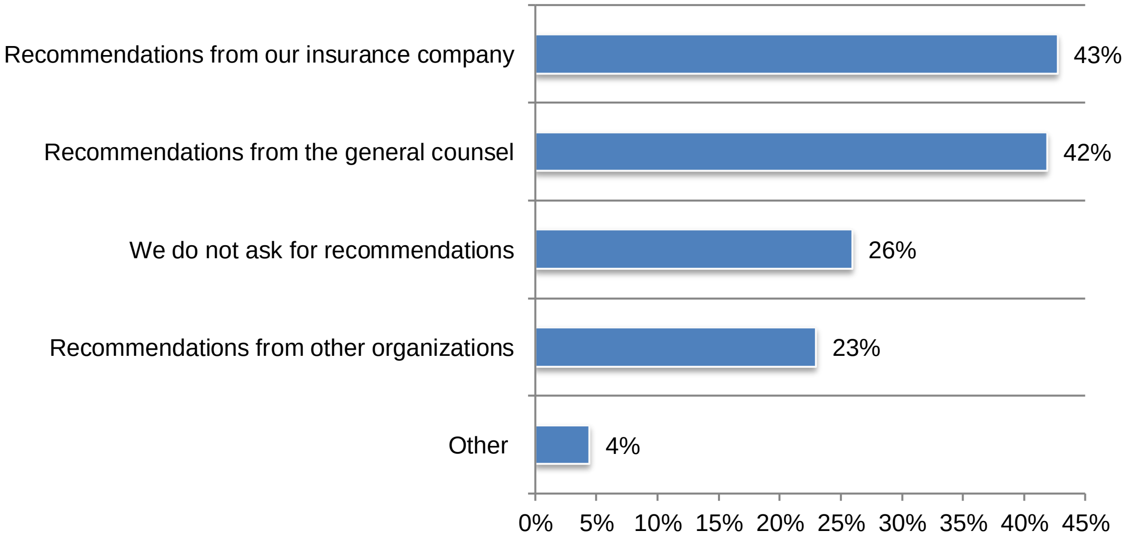
No resources or budget is the main reason the 11 percent of organizations do not have a data breach response plan in place. According to Figure 14, only 10 percent of respondents say it is not important to have data breach response plan in place.

Figure 14. Why doesn't your organization have a data breach response plan in place?



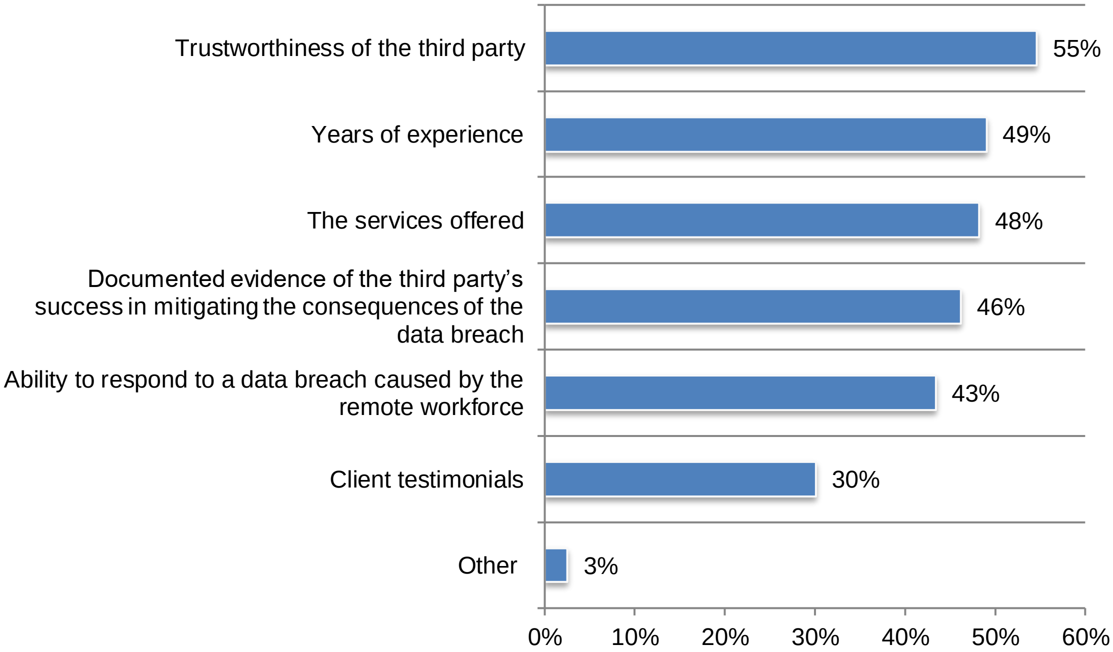
As part of their data breach preparedness, organizations are hiring third parties to manage their data breach response plan. Fifty-four percent of respondents in organizations with a data breach response plan hire a third-party to manage it. Of these respondents, 74 percent of respondents say they ask for recommendations on hiring a third party. Most recommendations are made by insurance companies or the general counsel, as shown in Figure 15.

Figure 15. Does your organization ask for recommendations to make a decision to hire a third party?
More than one response permitted



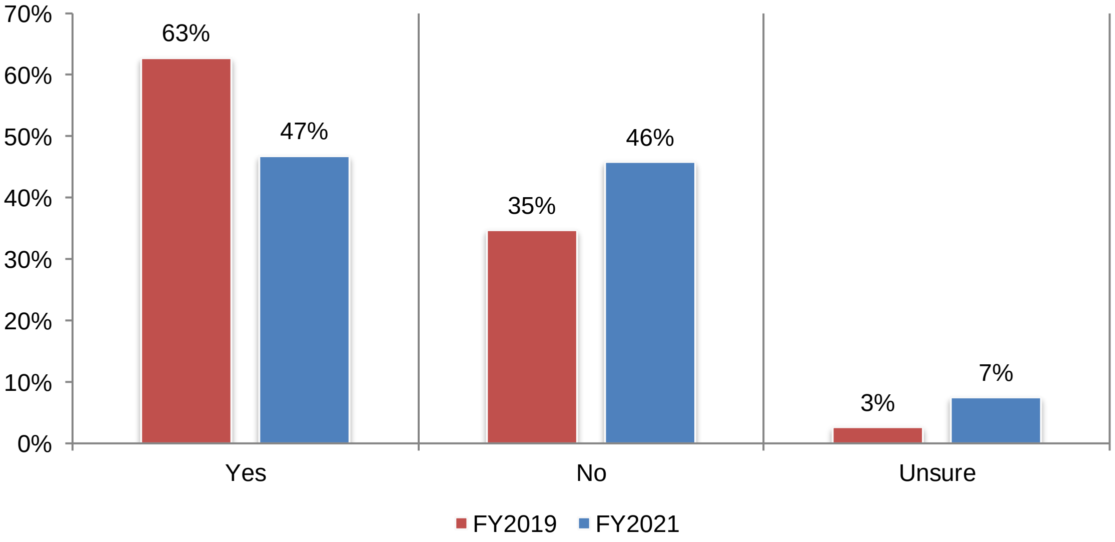
Organizations want to be able to trust the third party managing their incident response plan. According to Figure 16, 55 percent of respondents say trustworthiness is the number one criterion for hiring a third party. Only 43 percent of respondents say it is the ability to respond to a data breach caused by the remote workforce.

Figure 16. What criteria is used to select a third party?
More than one response permitted



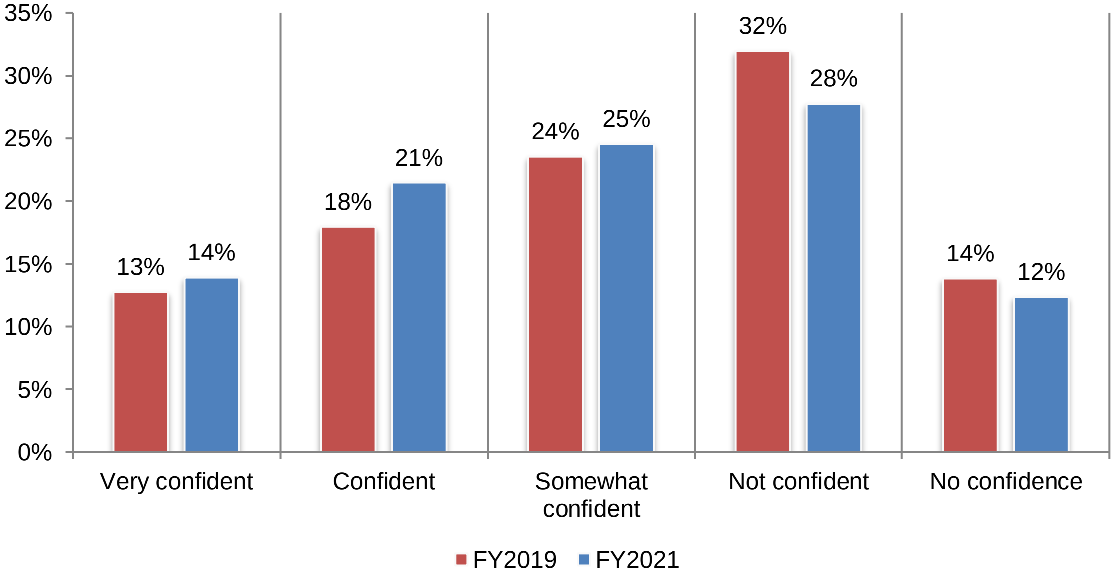
Less than half of respondents have processes in their incident response plans to manage an international data breach. As discussed previously, 59 percent of respondents say their organizations had a data breach in the past two years. Forty-nine percent of respondents say one more of these breaches were global. According to Figure 17, less than half of respondents (47 percent) say their organizations' plans include how to manage an international data breach.

Figure 17. Does your incident response plan include processes to manage an international data breach?



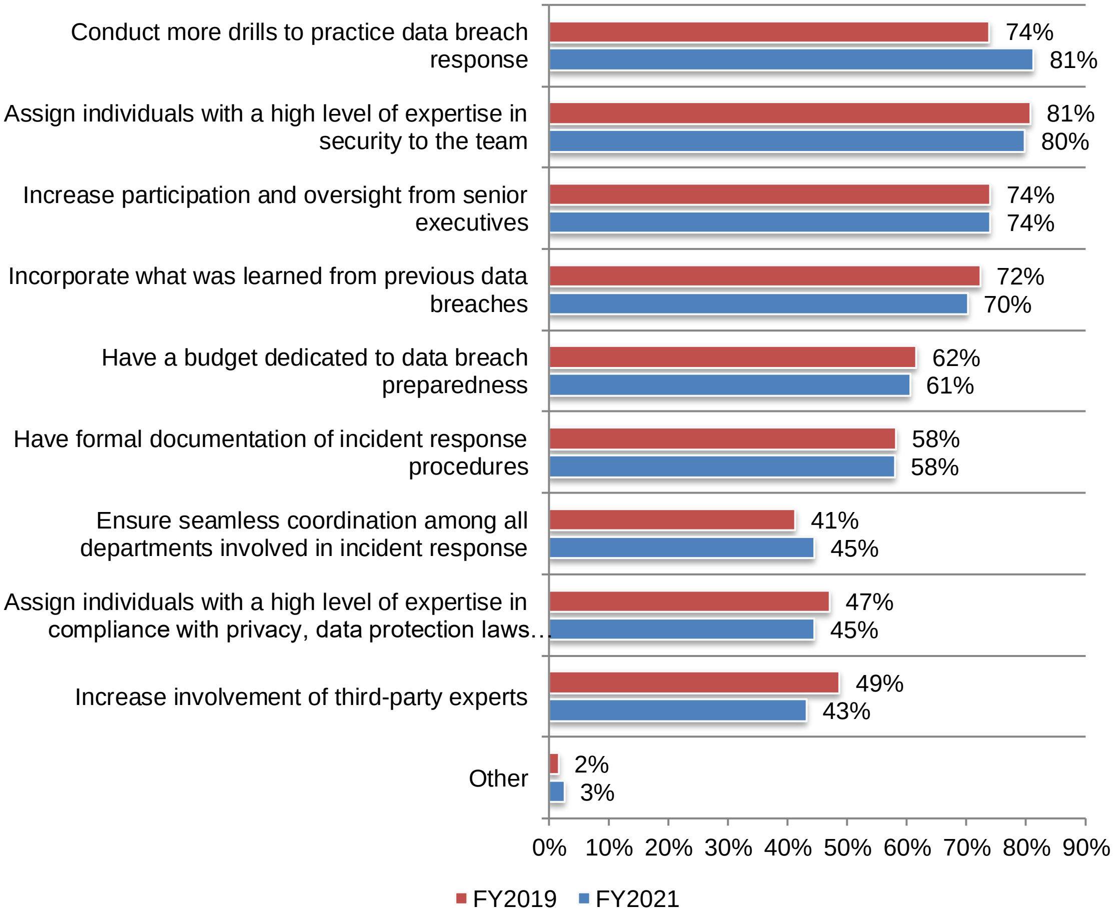
Confidence in the ability to deal with an international data breach is still low, as shown in Figure 18. Only 35 percent of respondents are very confident or confident in their ability to deal with an international data breach. In 2019, only 31 percent of respondents were very confident or confident.

Figure 18. How confident is your organization in its ability to deal with an international data breach?



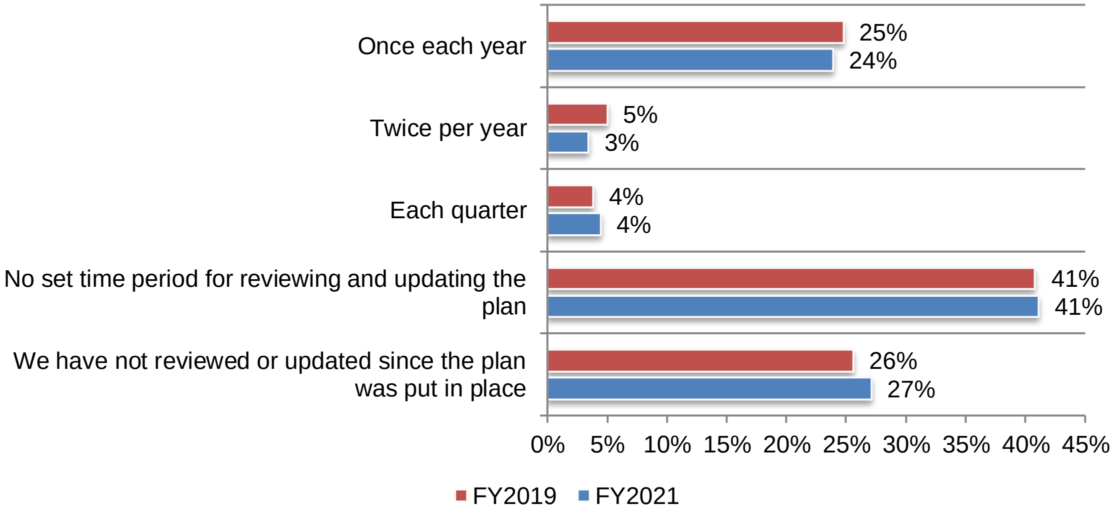
More practice drills and security expertise are believed to improve the effectiveness of data breach response plans. We asked organizations with a data breach response plan how they could become more effective. According to Figure 19, conducting more drills to practice data breach response increased from 74 percent of respondents in 2019 to 81 percent of respondents in this year's research. It is interesting that it is more important to assign individuals with a high level of security expertise (80 percent of respondents) than to assign individuals with expertise in compliance, privacy, data protection laws and regulations to the team.

Figure 19. How could your data breach response plan become more effective?
More than one response permitted



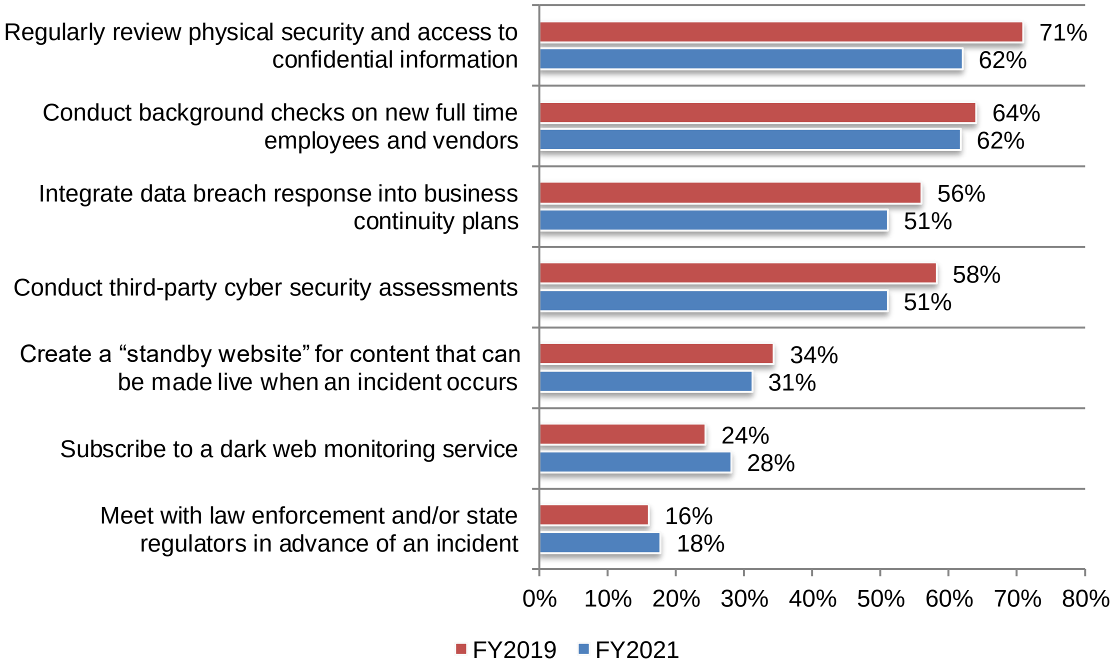
Data breach response plans are not regularly updated. As shown in Figure 20, 68 percent of respondents say their organizations have not reviewed or updated the plan since it was put in place (27 percent) or have not set a specific time to review and update the plan (41 percent). Only 24 percent of respondents say it is reviewed annually.

Figure 20. How often does your company update the data breach response plan?



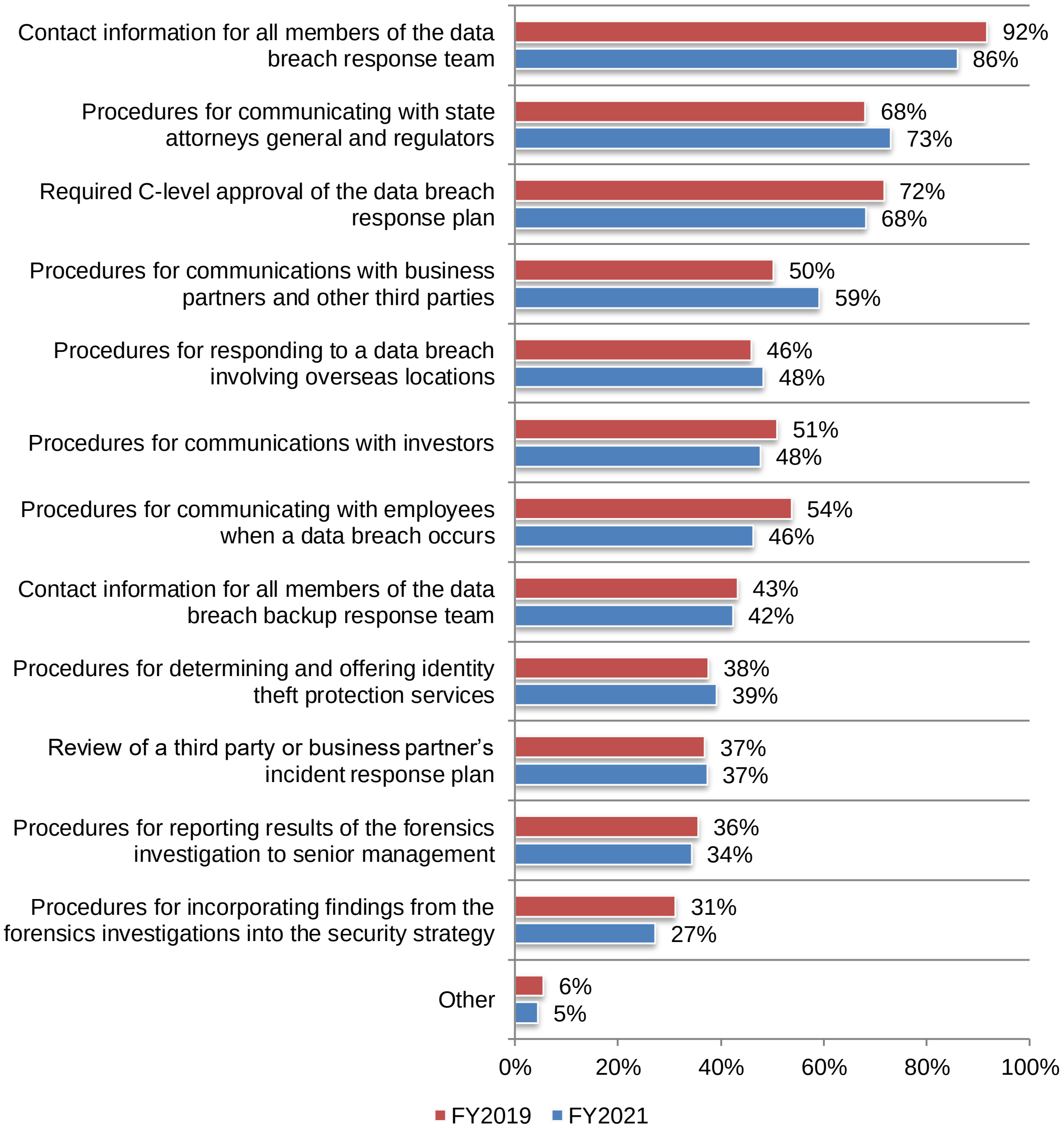
More organizations are regularly reviewing physical security and access to confidential information. According to Figure 21, the primary steps being taken to prepare for a data breach are regular reviews of physical security and access to confidential information (62 percent of respondents) and conducting background checks on new full-time employees and vendors (62 percent of respondents).

Figure 21. Does your organization take any of the following steps to prepare for a data breach?
More than one response permitted



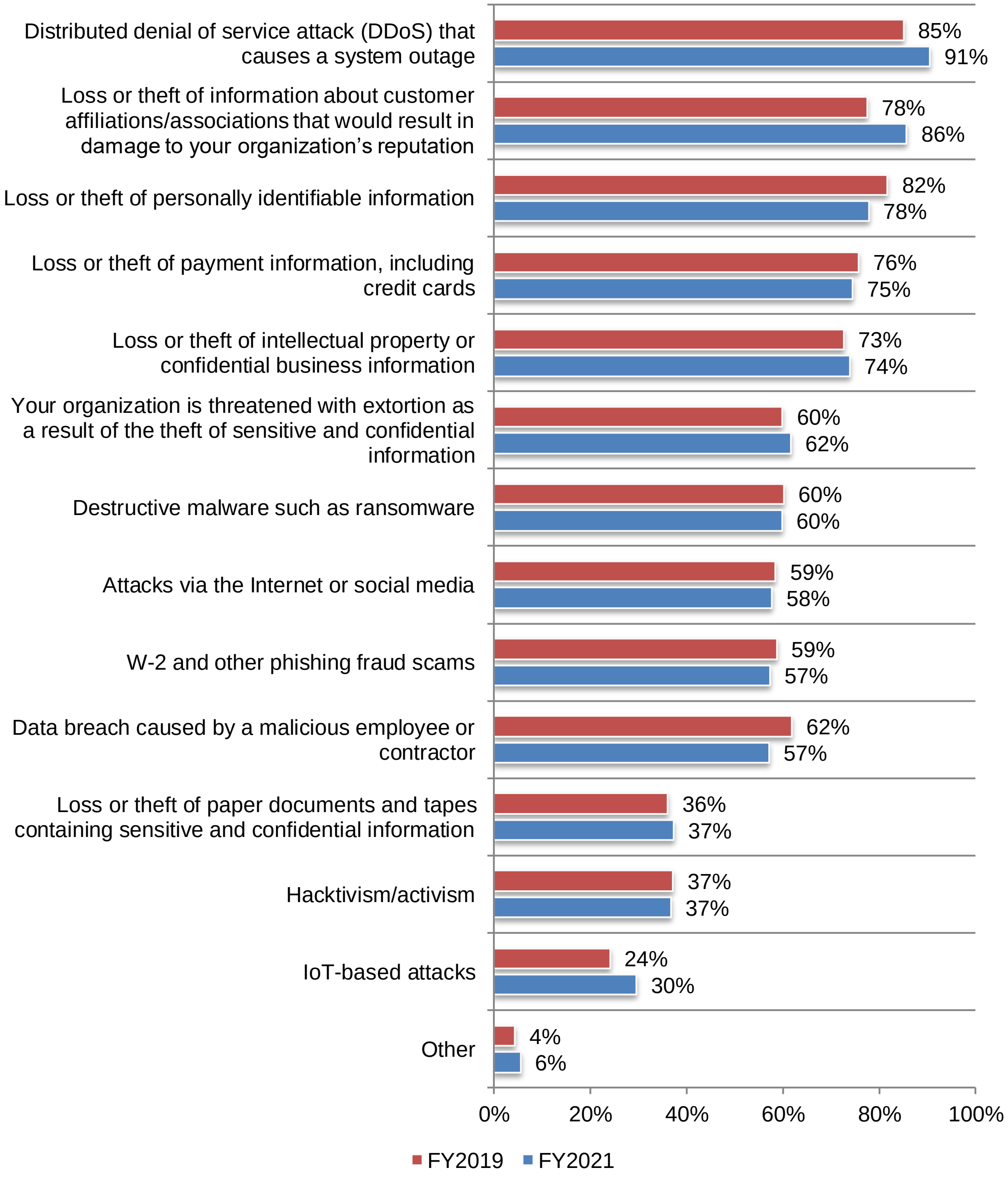
Data breach response plans focus on communication activities. As shown in Figure 22, contact information for all members of the data breach response plan, procedures for communicating with state attorneys general and regulators are the top two steps included in the data breach response plan, 86 percent and 73 percent of respondents respectively. Although organizations are having international data breaches, only 48 percent of respondents say it includes procedures for responding to a data breach in an overseas location.

Figure 22. Does your data breach response plan include the following steps?
More than one response permitted



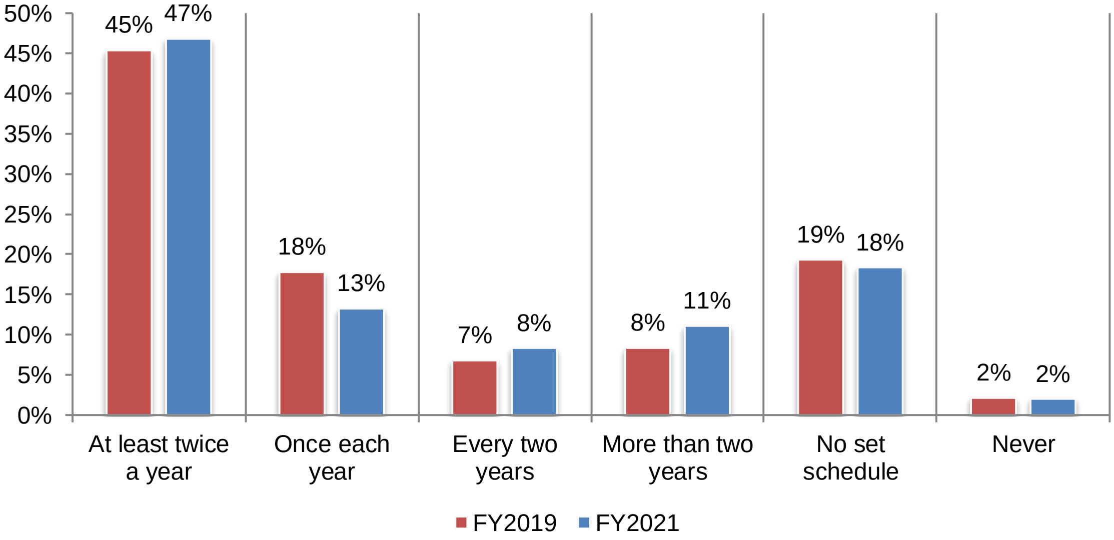
More organizations' data breach response plans offer guidance on the loss or theft of personally identifiable information. According to Figure 23, guidance on managing a distributed denial of service attack (DDoS) that causes a system outage has become more important since 2019, an increase from 85 percent to 91 percent of respondents. Also increasing in importance is the management of loss or theft of information about customer affiliations/associations that would result in damage to the organization's reputation (from 78 percent to 86 percent of respondents).

Figure 23. Does your data breach response plan offer guidance on managing the following security incidents?
More than one response permitted



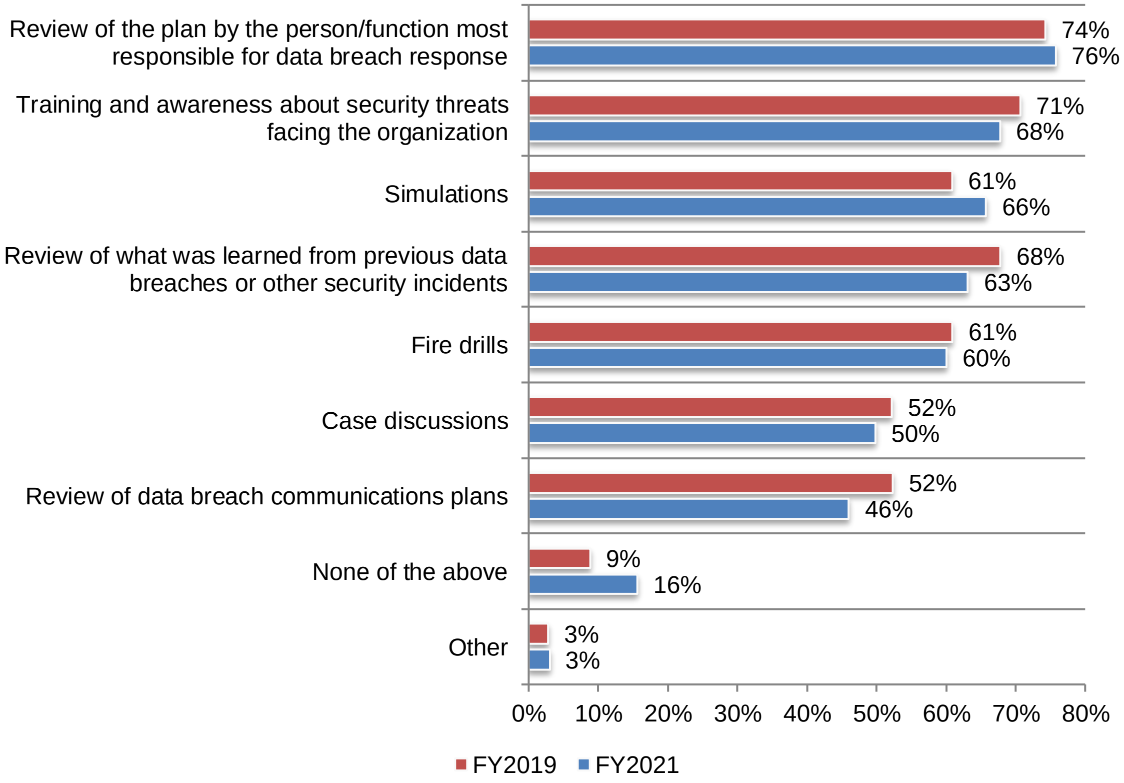
The majority of organizations (80 percent of respondents) practice responding to a data breach. As shown in Figure 24 of these respondents, 47 percent say they practice at least twice a year, a slight change since 2019.

Figure 24. Trends in practicing response plans



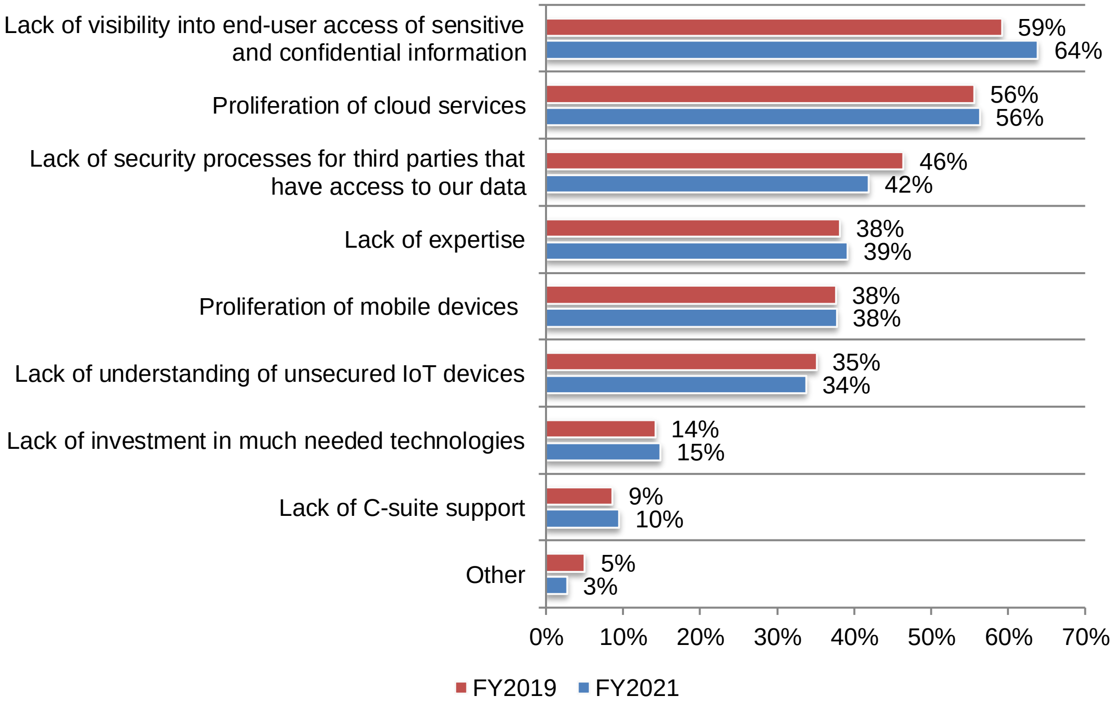
According to Figure 25, the top two steps included in practicing data breach response plans are having the plan reviewed by the person/function most responsible for data breach response (76 percent of respondents) and the training and awareness about security threats facing the organization (68 percent of respondents).

Figure 25. What steps are included in practicing data breach response plans?
More than one response permitted



IT security lacks visibility into end-user access to sensitive and confidential information. As shown in Figure 26, a lack of visibility into end-user access of sensitive and confidential information is the number one barrier to improving data breach response, an increase from 59 percent of respondents in 2019 to 64 percent of respondents in 2021. Proliferation of cloud services is considered by 56 percent of respondents a deterrent to improving data breach response.

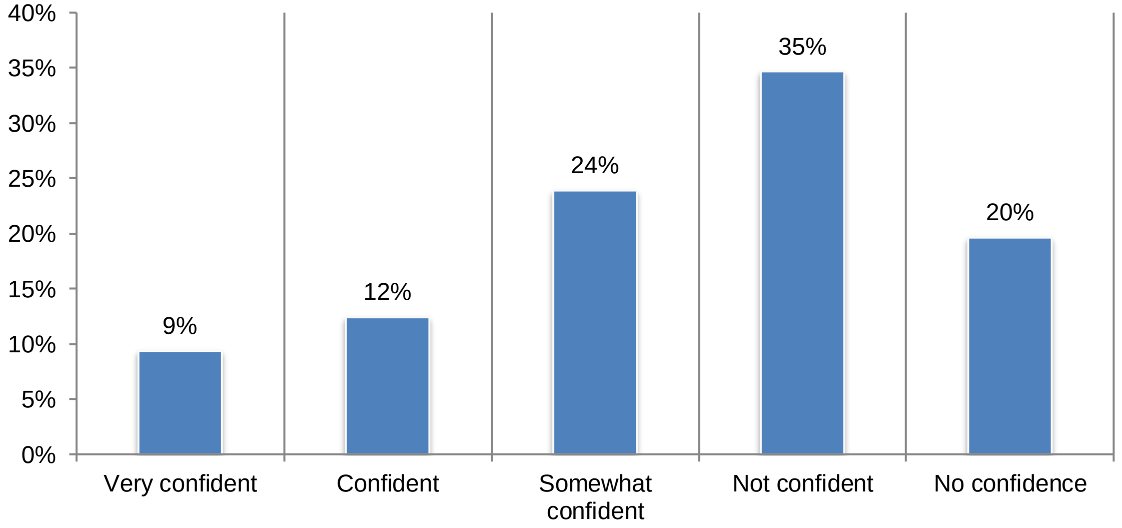
Figure 26. The biggest barriers to improving the ability of IT security to respond to a data breach
Three responses permitted



The impact of ransomware, phishing and COVID-19 on the risk of a data breach

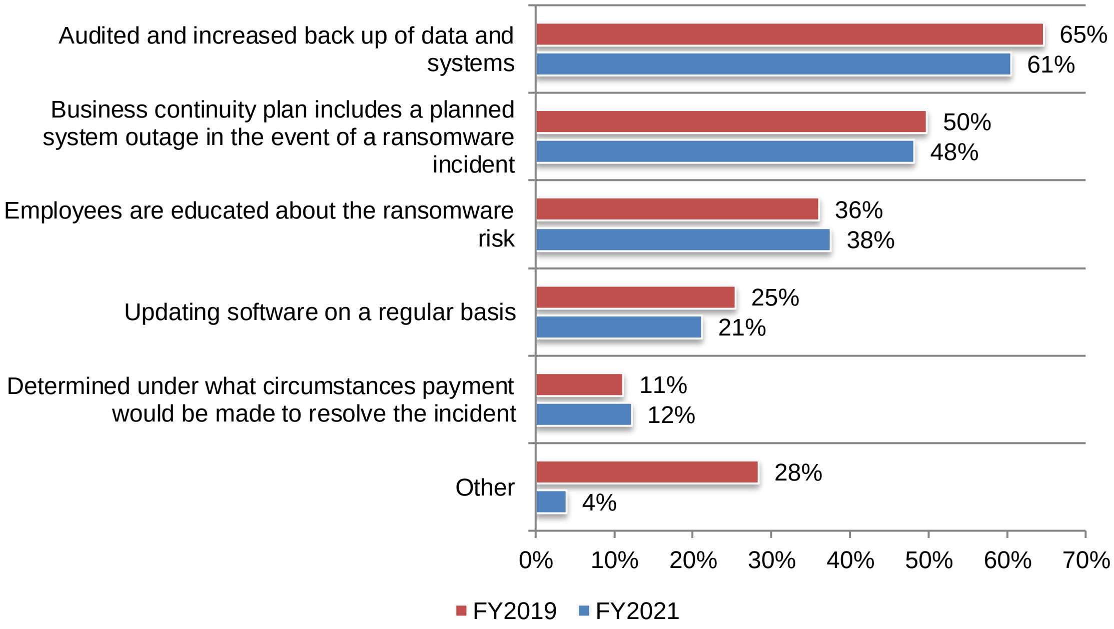
Spear phishing attacks are pervasive, and the consequences are significant. Sixty-nine percent of respondents had one or more spear phishing attacks and 71 percent of these respondents say the negative consequences of these attacks was very significant or significant. As a consequence, as shown in Figure 27, only 21 percent of respondents say their organizations are very confident (9 percent) or confident (12 percent) in their ability to deal with ransomware with a remote workforce.

Figure 27. How confident is your organization in its ability to deal with ransomware with a remote workforce?



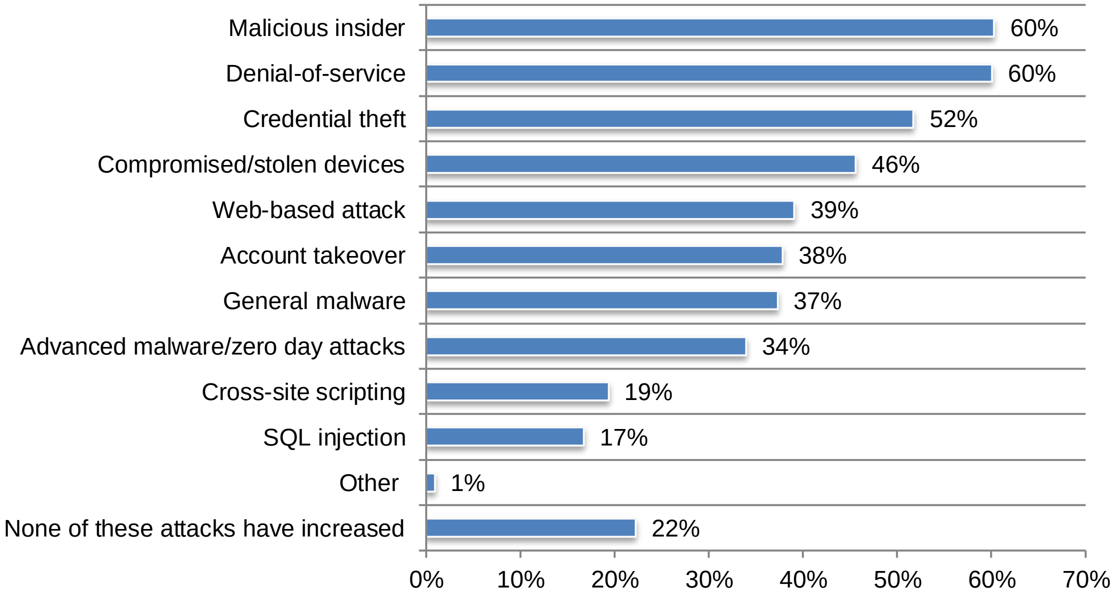
Forty-two percent of respondents say their organizations had a ransomware attack. The average ransom was $5,432 and 62 percent of respondents say it was paid. According to Figure 28, 61 percent of respondents report that their organizations audited, and increased backup of data and systems and their business continuity plan includes a planned system outage in the event of a ransomware incident (48 percent of respondents).

Figure 28. Has your organization taken the following steps to prepare for a ransomware incident?
More than one response permitted



Security attacks are increasing since COVID-19. An average of 37 percent of organizations' workforce are working remotely due to COVI-19. According to Figure 29, the attacks that are increasing are from malicious insiders and denial-of-service attacks (both 60 percent of respondents). Fifty-two percent of respondents say credential theft attacks have increased

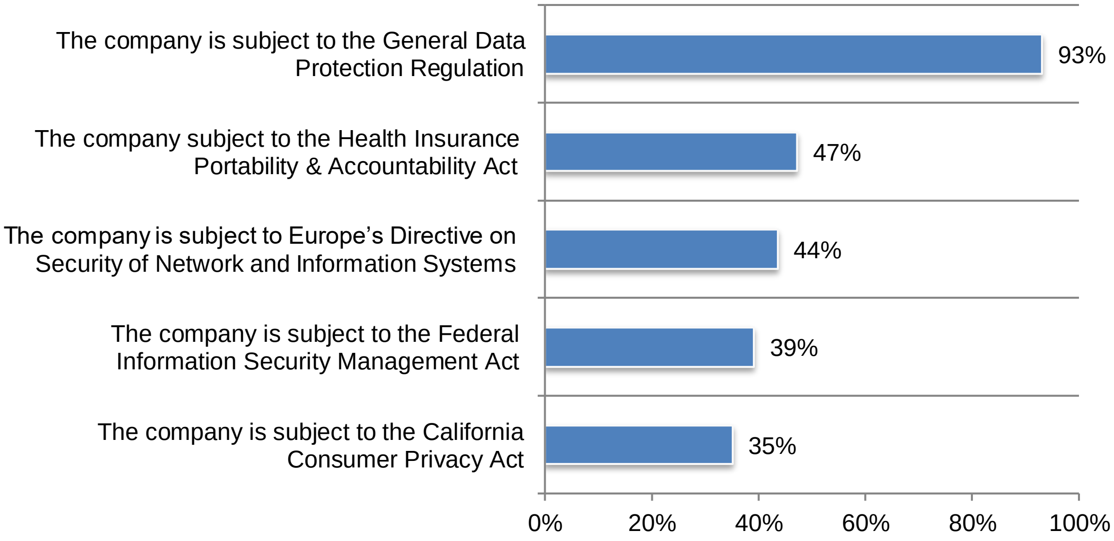
Figure 29. Since COVID-19 have the following attacks increased?
More than one response permitted



Regulations and data breach preparedness

Virtually all organizations represented in this study are subject to GDPR. As shown in Figure 30, 93 percent of respondents say their company is subject to the General Data Protection Regulation (GDPR). However, despite the need to comply with GDPR many organizations are not addressing the steps needed to respond to an international data breach.

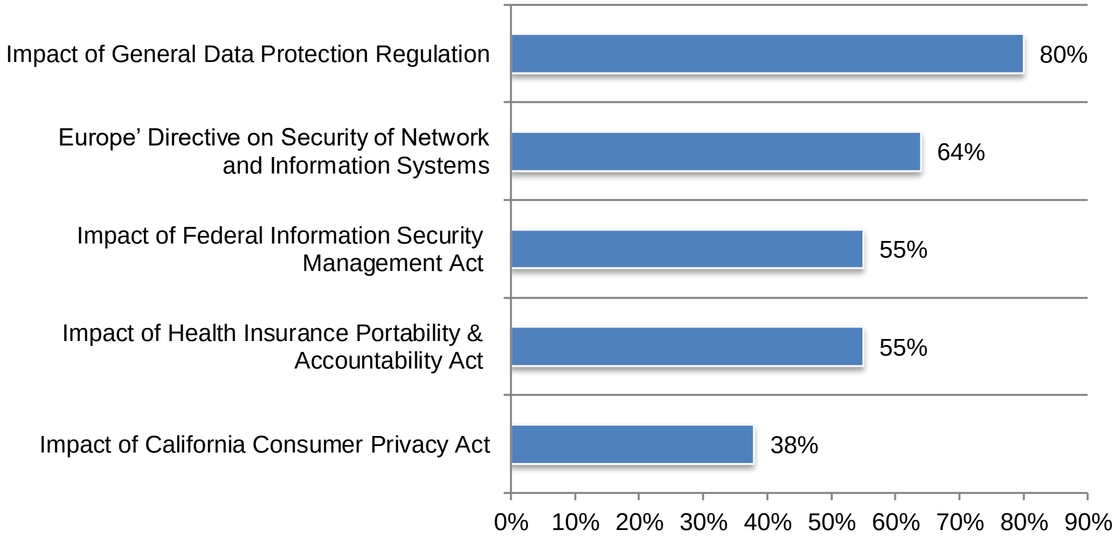
Figure 30. Regulations organizations are subject to and impact data breach preparedness
Yes responses presented



Respondents were asked to rate the impact of these regulations on their organizations' data breach plans on a scale of 1 = no impact to 10 = high impact. Figure 31 shows the high and very high impact (7+ responses).

The GDPR has the greatest impact on data breach response plans. As a result, organizations should increase their focus on ensuring they are improving their ability to respond to a data breach that is international in scope.

Figure 31. The impact of regulations on data breach response plans
On a scale of 1 = No impact to 10 = High impact, 7+ responses presented

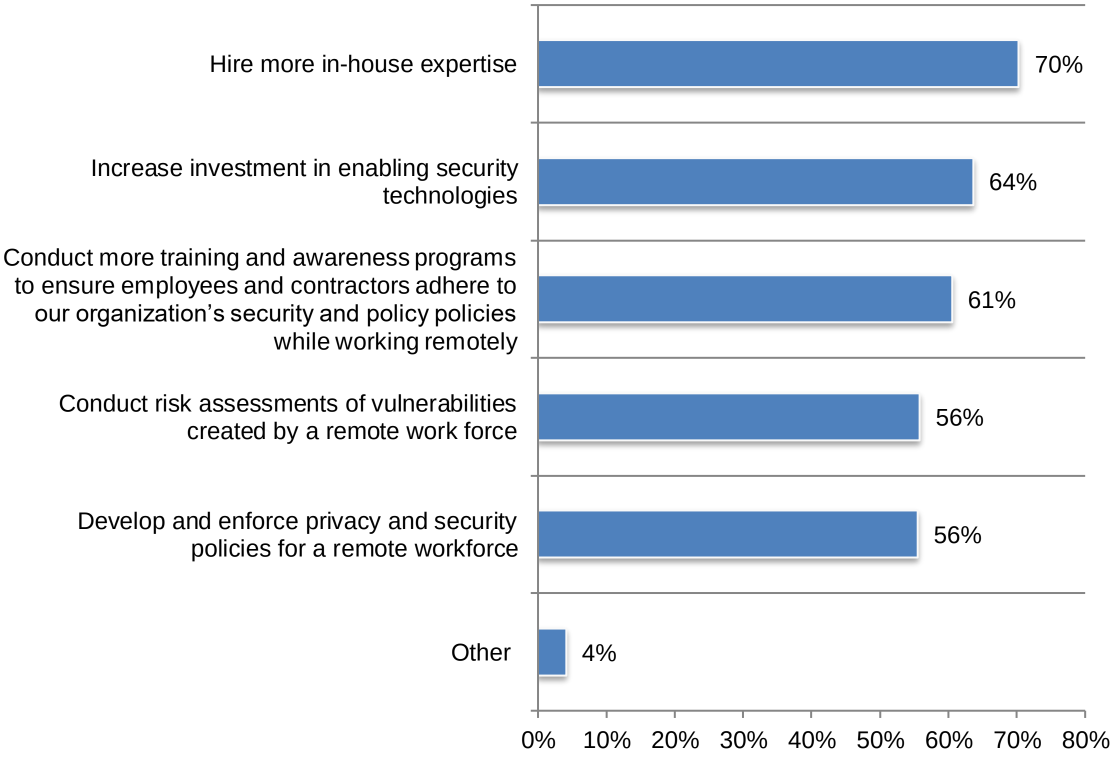


Perceptions about the future

The majority of organizations believe remote working will become the new norm which requires more in-house expertise and investments in security technologies. Fifty-six percent of respondents believe remote working will become the new norm.

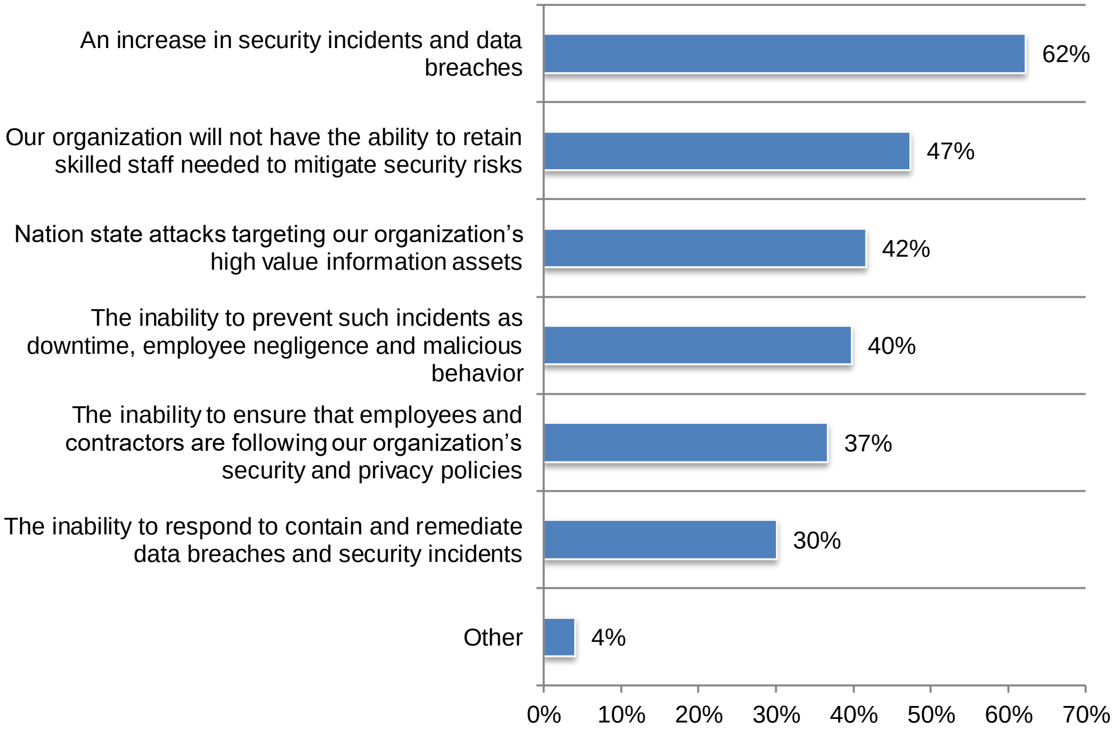
As shown in Figure 32, 70 percent of these respondents say they will hire more in-house expertise and invest in enabling security technologies (64 percent of respondents). Fifty-six percent of respondents say their organizations will conduct risk assessments of vulnerabilities created by a remote workforce and develop and enforce privacy and security policies for a remote workforce.

Figure 32. What changes will your organization make to its privacy and security practices?
More than one response permitted



Security incidents and data breaches are expected to increase. As shown in Figure 33, 62 percent of respondents say their organizations expect more security incidents and data breaches. However, almost half (47 percent) of respondents say their organizations will not have the ability to retain skilled staff needed to mitigate security risks.

Figure 33. What concerns your organization the most?
More than one response permitted

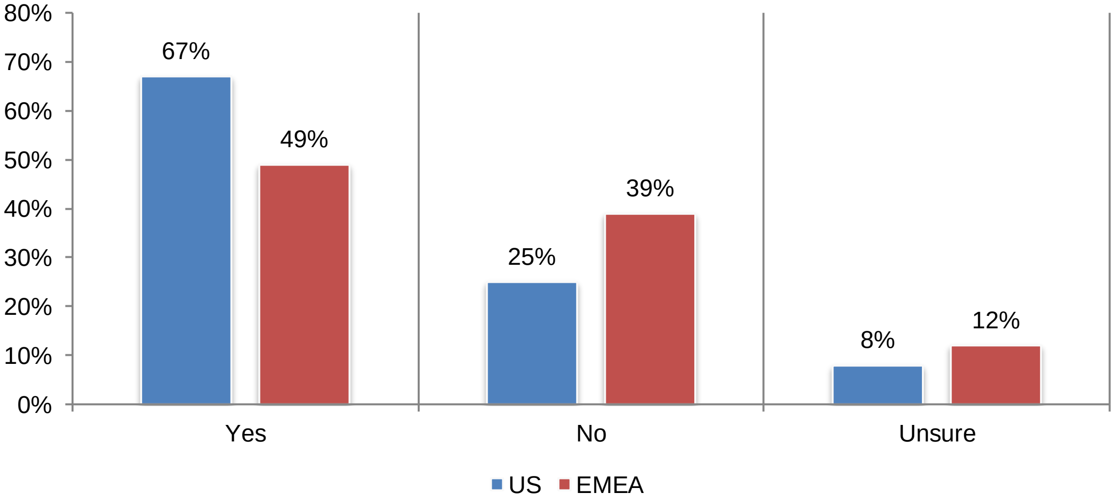


Differences between the US and EMEA

In this section, we highlight the most significant differences in the research between the US (544 respondents) and EMEA (445 respondents).

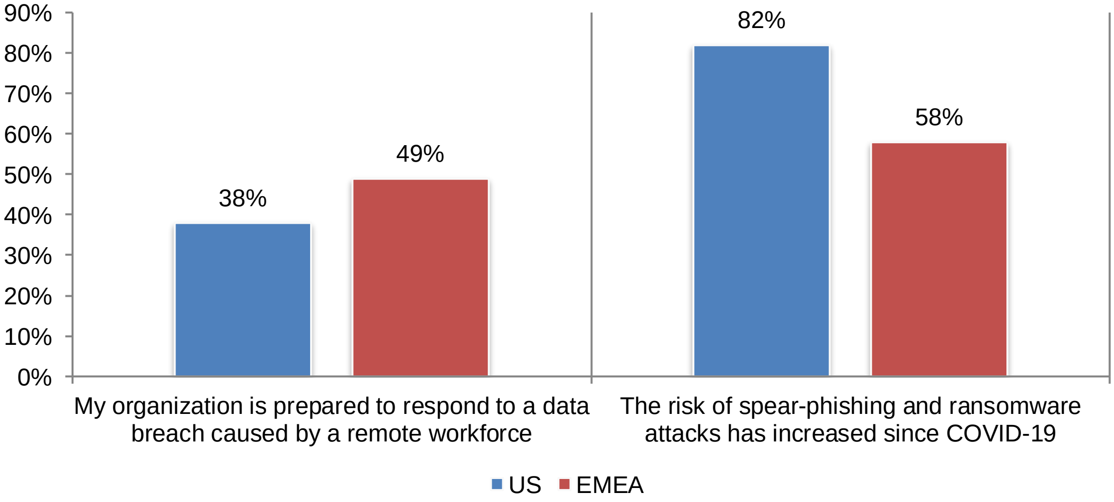
US organizations report having more data breaches than EMEA. According to Figure 34, 67 percent of US respondents and less than half (49 percent) of EMEA respondents say their organizations had a data breach involving the loss or theft of more than 1,000 records containing sensitive or confidential information in the past two years.

Figure 34. 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?



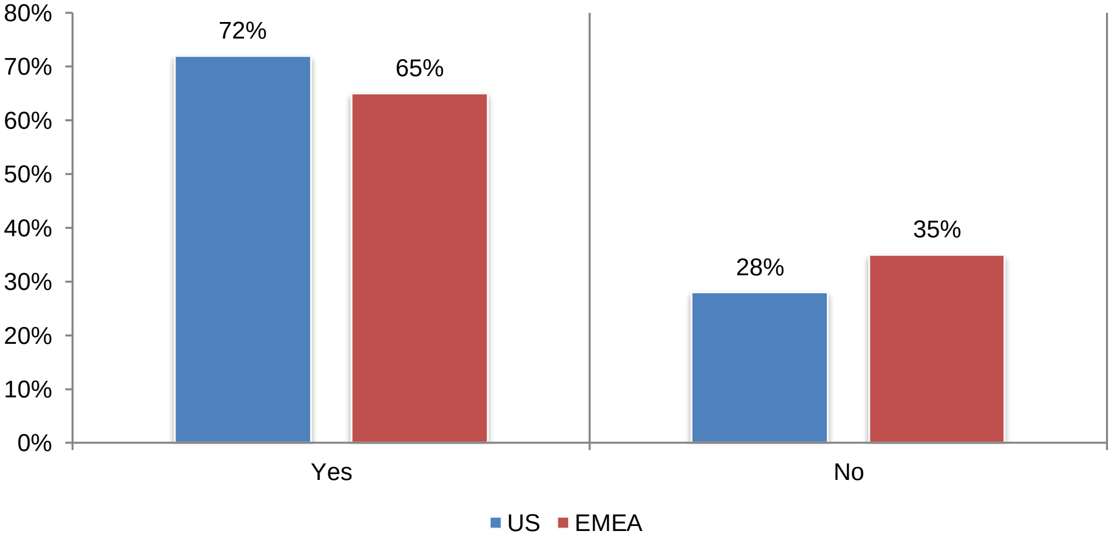
EMEA respondents are more prepared to respond to a data breach caused by a remote workforce. According to Figure 35, almost half (49 percent) of EMEA respondents are prepared to respond to a data breach caused by a remote workforce. In contrast, only 38 percent of US respondents say their organizations are prepared. US respondents are more likely to believe spear-phishing and ransomware attacks have increased since COVID-19 (82 percent vs. 58 percent).

Figure 35. The impact of a remote workforce and COVID-19 on data breach preparedness
Strongly agree and Agree responses combined



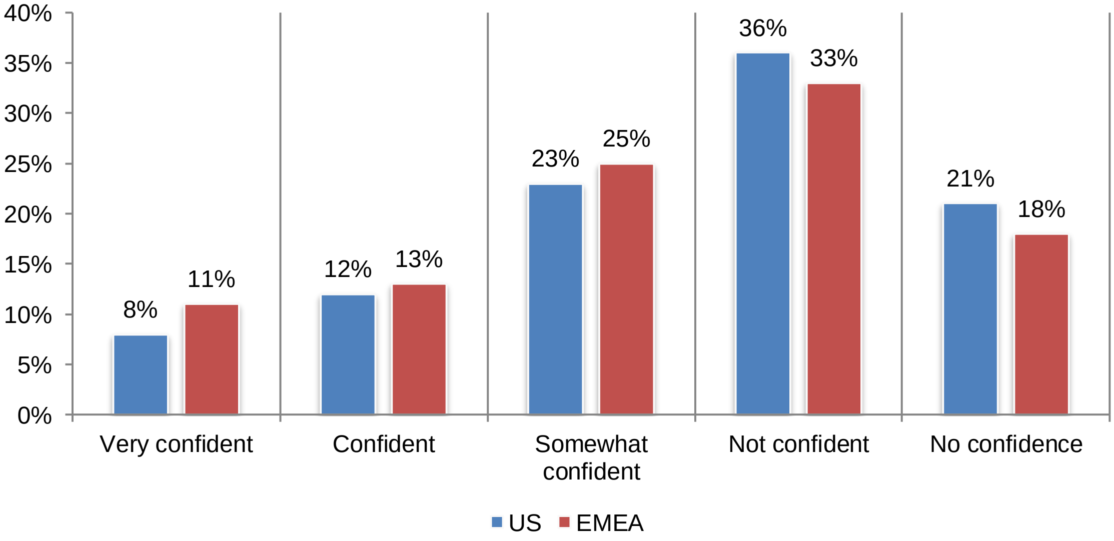
US organizations are more likely to have had one or more spear phishing attacks in the past year. Seventy-two percent of US respondents vs. 65 percent of EMEA respondents report having had a spear phishing attack.

Figure 36. In the past 12 months, did your organization experience one or more spear phishing attacks?



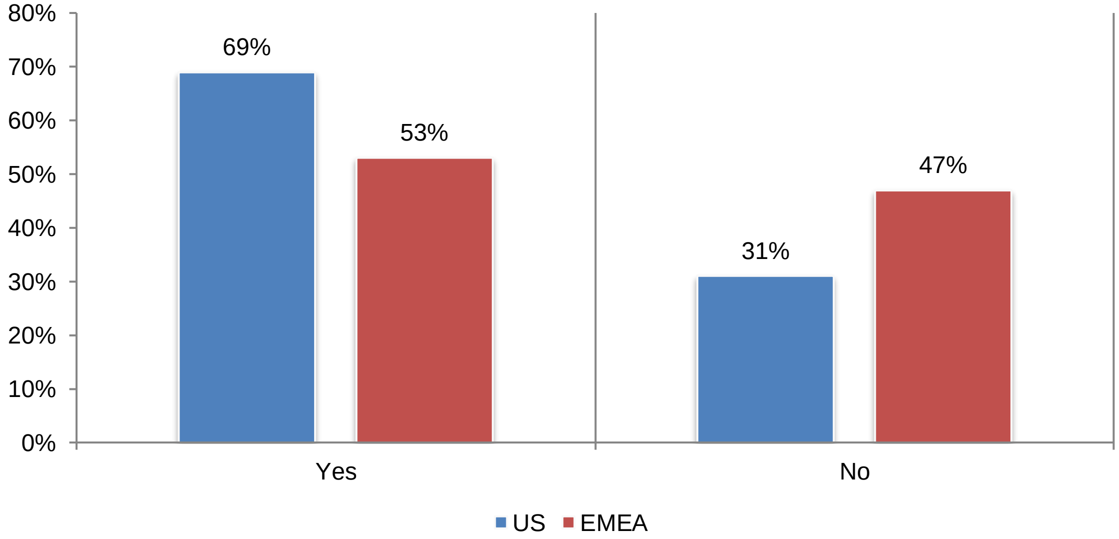
Both US and EMEA are not confident in their organizations' ability to deal with ransomware with a remote workforce. As shown in Figure 37, only 20 percent of US respondents and 24 percent of EMEA respondents are very confident or confident their organizations can deal with a ransomware attack.

Figure 37. How confident is your organization in its ability to deal with ransomware with a remote workforce?



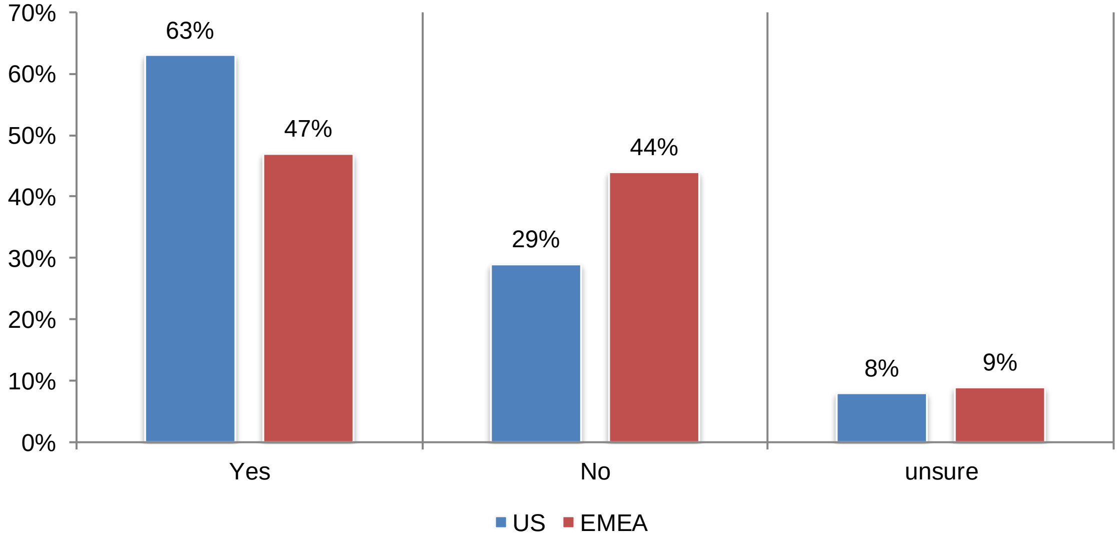
More US organizations that experienced a ransomware attack paid the ransom. Forty-five percent of US respondents and 39 percent of EMEA respondents say they have had a ransomware attack. Of these, 69 percent of US respondents say they paid an average of $5,857 and 53 percent of EMEA respondents paid an average of $4,914 (in US dollars), as shown in Figure 38.

Figure 38. Did your company pay the ransom?



US respondents (63 percent of respondents) are more likely to believe remote working will become the new norm than EMEA (47 percent of respondents).

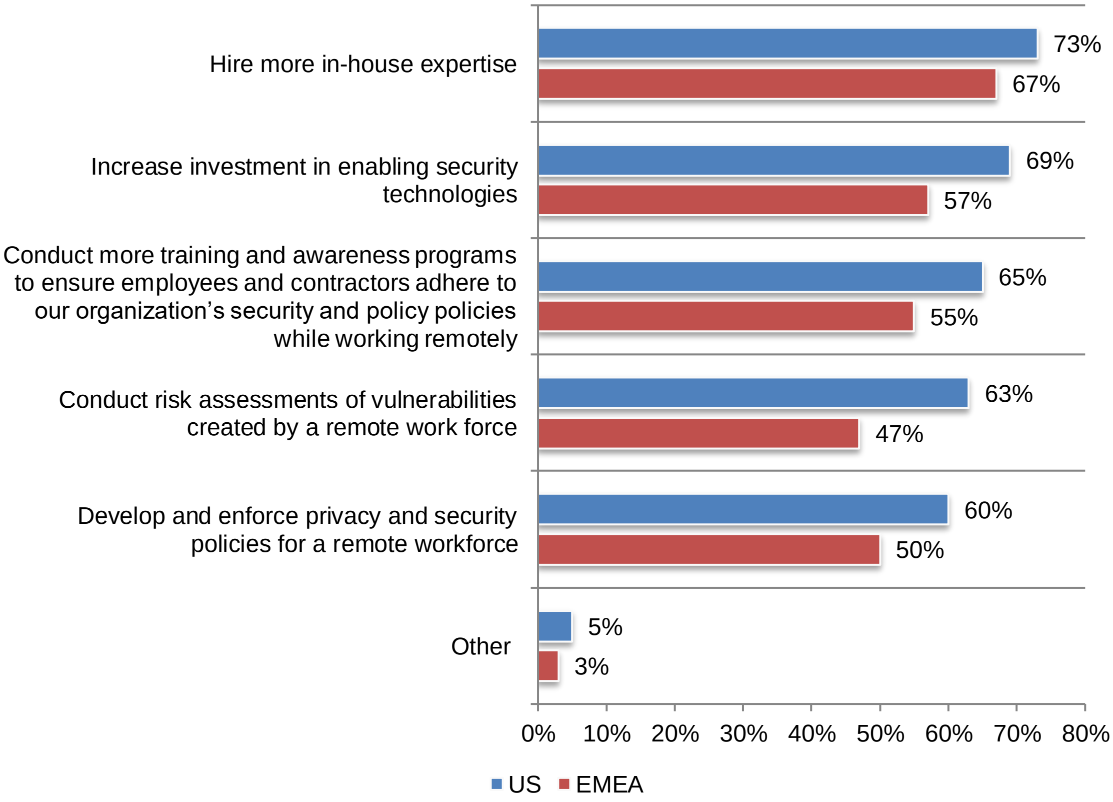
Figure 39. Will remote working become the new norm?



The new norm will require organizations to hire more in-house expertise and increase investments in security technologies. As discussed previously, US respondents are more likely to believe remote working will become the new norm (63 percent vs. 47 percent respondents).

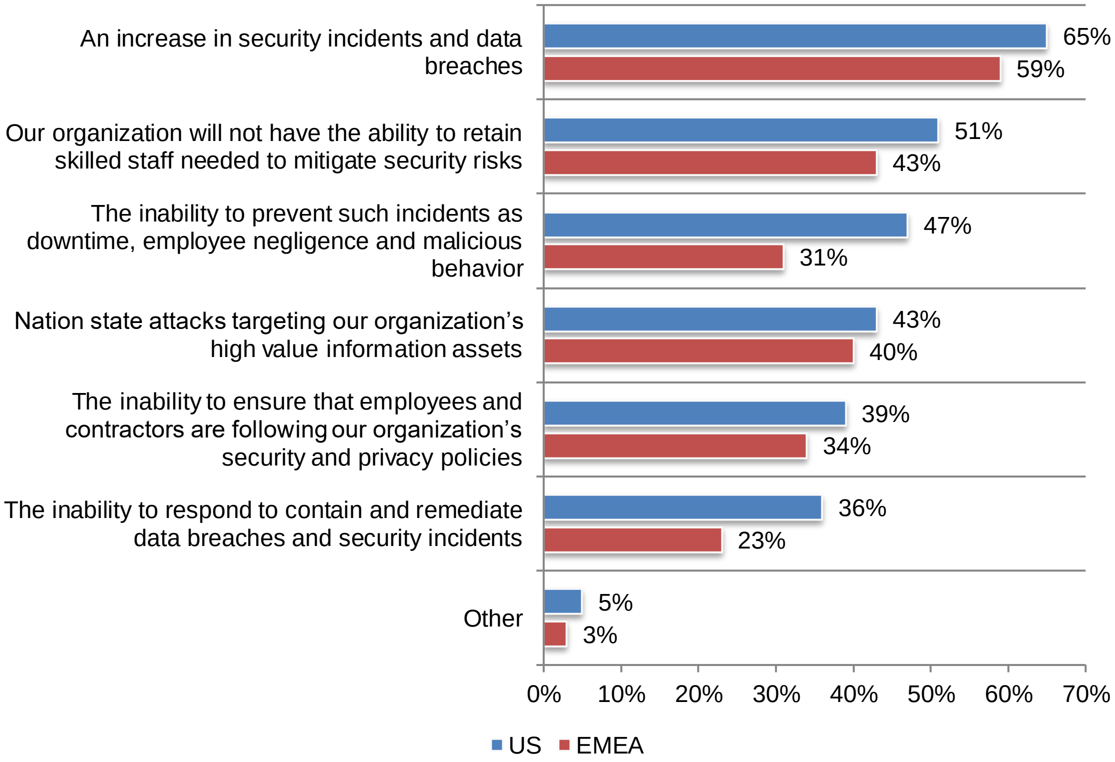
As shown in Figure 40, US respondents are far more likely to make changes to their organizations' privacy and security practices to mitigate risks created by the remote workforce. These include more training and awareness programs (65 percent vs. 55 percent of respondents), risk assessments of vulnerabilities (63 percent vs. 47 percent of respondents) and develop and enforce privacy and security policies for a remote workforce (60 percent vs. 50 percent of respondents).

Figure 40. What changes will be made to the organization's privacy and security practices?
More than one response permitted



US respondents are more concerned about future security incidents. Figure 41 presents a list of security threats to organizations in the next year. As shown, US respondents are more concerned about an increase in security incidents and data breaches (65 percent vs. 59 percent) and the inability to prevent such incidents as downtime, employee negligence and malicious behavior (51 percent vs. 43 percent).

Figure 41. What concerns your organization the most?
More than one response permitted



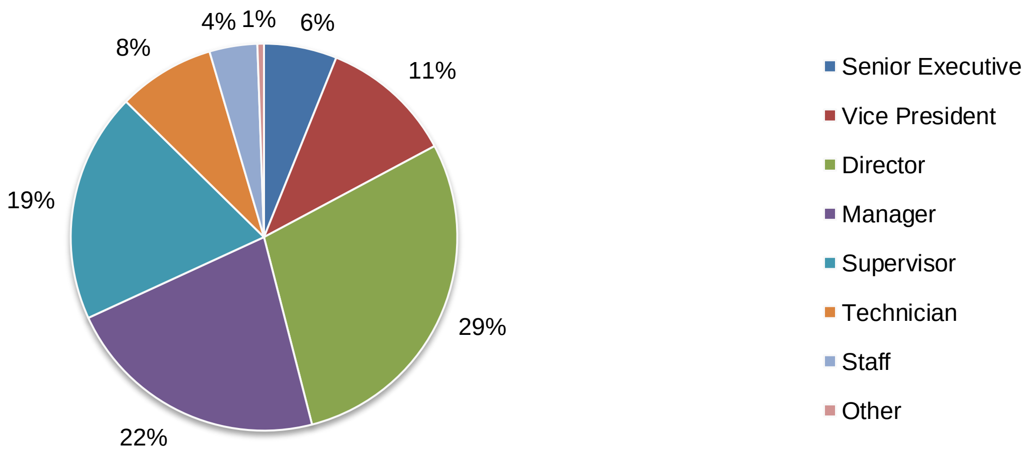
Part 4. Methods

A sampling frame of 14,171 US and 11,900 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 605 total US survey returns and 493 EMEA survey returns. Screening and reliability checks required the removal of 61 US surveys and 48 EMEA surveys. Our final sample consisted of 544 US surveys (a 3.8 percent response rate) and 445 EMEA surveys (a 3.7 percent response rate).

Table 1. Sample response	US	EMEA	Combined
Sampling frame	14,171	11,900	26,071
Total returns	605	493	1,098
Rejected or screened surveys	61	48	109
Final sample	544	445	989
Response rate	3.8%	3.7%	3.8%

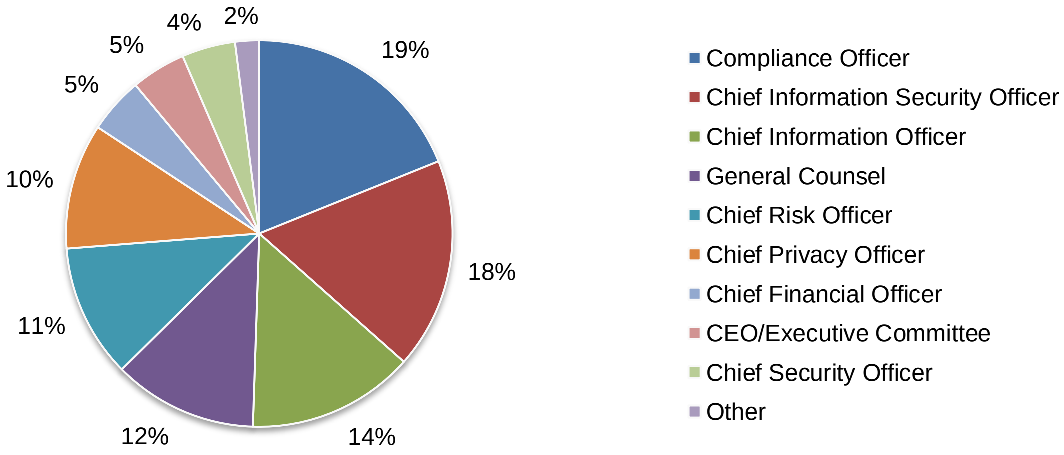
Pie Chart 1 reports the respondent's organizational level within participating organizations. By design, a majority of respondents (88 percent) are at or above the supervisory levels.

Pie Chart 1. Current position within the organization
n=989



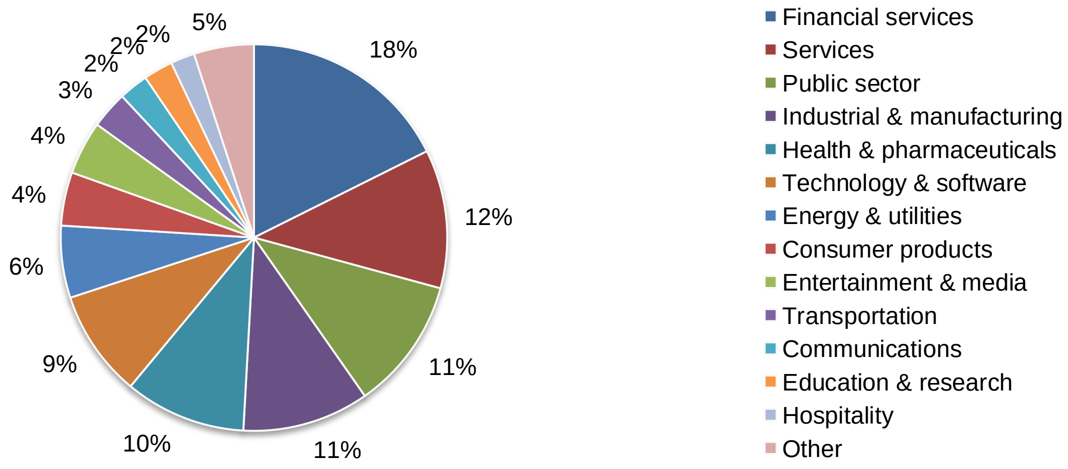
Pie Chart 2 reveals that 19 percent of respondents report to the compliance officer, 18 percent of respondents report to the chief information security officer, 14 percent of respondents report to the chief information officer, 12 percent of respondents report to the general counsel and 11 percent of respondents report to the chief risk officer.

Pie Chart 2. Primary person respondent reports to within the organization
n=989



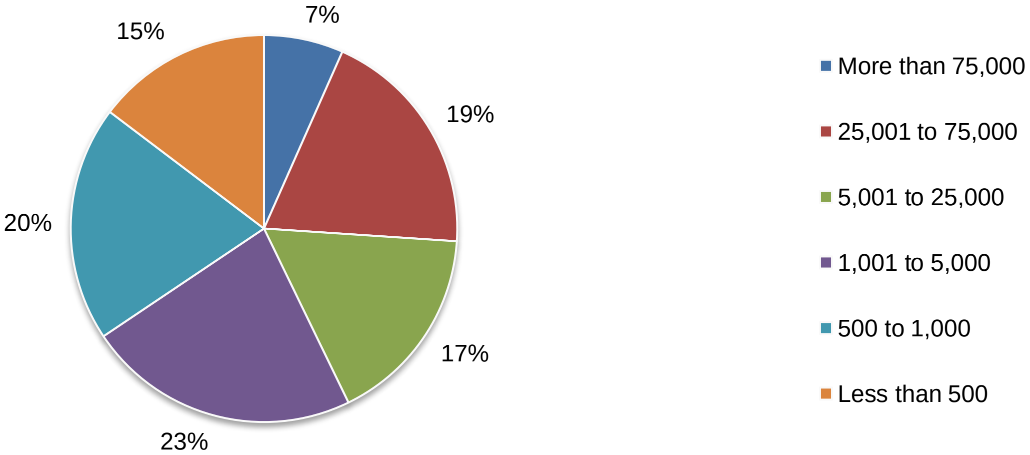
Pie Chart 3 reports the industry classification of respondents' organizations. The largest industry classification is financial services (18 percent of respondents), which includes banking, investment management, insurance, brokerage, payments and credit cards. This is followed by services (12 percent of respondents), public sector (11 percent of respondents), industrial and manufacturing (11 percent of respondents), and health and pharmaceuticals (10 percent of respondents).

Pie Chart 3. Primary industry focus
n=989



As shown in Pie Chart 4, 66 percent of respondents are from organizations with a global headcount of more than 1,000 employees.

Pie Chart 4. Global employee headcount
n=989



Part 4. Caveats to this study

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

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

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

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

Appendix: Detailed Survey Results

The following tables provide the frequency or percentage frequency of responses to all survey questions contained in this study. All survey responses were captured in January 2021.

Survey response	FY2021	US	EMEA
Sampling frame	26,071	14,171	11,900
Total returns	1,098	605	493
Rejected or screened surveys	109	61	48
Final sample	989	544	445
Response rate	3.8%	3.8%	3.7%

Part 1. Background & Attributions

Q1. 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?	FY2021	US	EMEA
Yes	59%	67%	49%
No	31%	25%	39%
Unsure	10%	8%	12%
Total	100%	100%	100%

Q2. How frequently did these incidents occur during the past 2 years?	FY2021	US	EMEA
Only once	36%	34%	38%
2 to 3 times	30%	31%	28%
4 to 5 times	24%	23%	25%
More than 5 times	11%	12%	9%
Total	100%	100%	100%

Q3.Were any of these breaches international or global in scope?	FY2021	US	EMEA
Yes	49%	51%	46%
No	46%	44%	48%
Unsure	5%	5%	6%
Total	100%	100%	100%

Q4. Were any of these breaches the result of a remote workforce?	FY2021	US	EMEA
Yes	47%	50%	43%
No	46%	43%	49%
Unsure	7%	7%	8%
Total	100%	100%	100%

Q5. My organization is prepared to respond to a data breach caused by a remote workforce.	FY2021	US	EMEA
Strongly agree	19%	15%	24%
Agree	24%	23%	25%
Unsure	20%	20%	19%
Disagree	23%	25%	21%
Strongly disagree	14%	17%	11%
Total	100%	100%	100%

Q6. The risk of spear-phishing and ransomware attacks has increased since COVID-19.	FY2021	US	EMEA
Strongly agree	29%	30%	28%
Agree	31%	32%	30%
Unsure	16%	14%	19%
Disagree	13%	14%	12%
Strongly disagree	10%	10%	11%
Total	100%	100%	100%

Q7. 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 and the loss of customers' and business partners' trust and confidence.	FY2021	US	EMEA
Strongly agree	25%	26%	23%
Agree	31%	32%	29%
Unsure	19%	18%	21%
Disagree	15%	14%	16%
Strongly disagree	10%	10%	11%
Total	100%	100%	100%

Q8. Following a data breach involving customers' or employees' sensitive or confidential information, how long should identity theft protection be provided?	FY2021	US	EMEA
1 year	21%	21%	20%
2 to 3 years	25%	27%	22%
4 to 7 years	19%	20%	17%
8 to 10 years	8%	8%	8%
More than 10 years	4%	4%	5%
Our organization does not provide identity theft protection	24%	20%	28%
Total	100%	100%	100%
Extrapolated value	3.14	3.23	3.05

Part 2. Data breach preparedness

Q9. What best describes the maturity of your organization's privacy and data protection program?	FY2021	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.	17%	15%	19%
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.	33%	34%	31%
Late-middle stage – most privacy and data protection program activities are deployed across the enterprise. The program has C-level support and adequate budget.	29%	29%	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.	21%	22%	20%
Total	100%	100%	100%

Q10. Has the board of directors and C-Suite executives requested a briefing on possible security risks caused by a remote workforce?	FY2021	US	EMEA
Yes	46%	43%	49%
No	54%	57%	51%
Total	100%	100%	100%

Q11a. Do you believe your company's board of directors and C-suite executives are knowledgeable about plans to deal with a possible data breach?	FY2021	US	EMEA
Yes	46%	40%	54%
No (proceed to Q12)	54%	60%	46%
Total	100%	100%	100%

Q11b. If yes, why do you believe your company's board of directors and C-suite executives are knowledgeable? Please select all that apply.	FY2021	US	EMEA
They regularly participate in detailed reviews of our data breach response plan	40%	42%	37%
They understand the specific security threats facing our organization	37%	39%	35%
They provide detailed feedback about the data breach response plan	35%	40%	28%
They assume responsibility for the successful execution of the incident response plan	33%	30%	36%
They have requested to be notified ASAP if a material data breach occurs	36%	33%	40%
They participate in a high level review of the organization's data protection and privacy practices	58%	57%	60%
Other	3%	3%	4%
Total	242%	244%	240%

Q12. What types of data loss is your organization most concerned about? Please select the top two.	FY2021	US	EMEA
Loss or theft of customer information	58%	60%	55%
Loss or theft of employee personal data	31%	30%	32%
Loss or theft of medical data	14%	13%	15%
Loss or theft of consumer data	22%	21%	24%
Loss or theft of intellectual property	61%	63%	58%
Loss or theft of payment card data	11%	10%	12%
Other	3%	3%	4%
Total	200%	200%	200%

Q13. What are the two biggest barriers to improving the ability of IT security to respond to a data breach? Please select the top three	FY2021	US	EMEA
Lack of investment in much needed technologies	15%	14%	16%
Lack of expertise	39%	36%	43%
Lack of C-suite support	10%	10%	9%
Lack of security processes for third parties that have access to our data	42%	41%	43%
Lack of visibility into end-user access of sensitive and confidential information	64%	63%	65%
Lack of understanding of unsecured IoT devices	34%	32%	36%
Proliferation of mobile devices	38%	40%	35%
Proliferation of cloud services	56%	59%	53%
Other	2%	5%	0%
Total	300%	300%	300%

Part 3. The impact of COVID-19 on data breach preparedness

Q14. What percentage of your organization's employees are working remotely due to COVID-19?	FY2021	US	EMEA
Less than 10%	25%	21%	30%
10% to 25%	20%	19%	21%
26% to 50%	23%	23%	24%
51% to 75%	17%	19%	14%
76% to 100%	15%	18%	11%
Total	100%	100%	100%
Extrapolated value	37%	41%	33%

Q15. Since COVID-19, have any of the following attacks **increased**? Please select all that apply.	FY2021	US	EMEA
Account takeover	38%	41%	34%
Advanced malware / zero day attacks	34%	38%	29%
Compromised / stolen devices	46%	42%	50%
Credential theft	52%	54%	49%
Cross-site scripting	19%	18%	21%
Denial of service	60%	56%	65%
General malware	37%	40%	34%
Malicious insider	60%	63%	57%
SQL injection	17%	19%	14%
Web-based attack	39%	40%	38%
Other (please specify)	1%	0%	2%
None of these attacks have increased	22%	20%	25%
Total	425%	431%	418%

Q16a. In the past 12 months, did your organization experience one or more spear phishing attacks?	FY2021	US	EMEA
Yes	69%	72%	65%
No	31%	28%	35%
Total	100%	100%	100%

Q16b. How significant were the negative consequences of the spear phishing attacks?	FY2021	US	EMEA
Very significant	26%	27%	24%
Significant	45%	44%	47%
Not significant	19%	18%	20%
Minimal	10%	11%	9%
Total	100%	100%	100%

Q17. How confident is your organization in its ability to deal with ransomware with a remote workforce?	FY2021	US	EMEA
Very confident	9%	8%	11%
Confident	12%	12%	13%
Somewhat confident	24%	23%	25%
Not confident	35%	36%	33%
No confidence	20%	21%	18%
Total	100%	100%	100%

Q18a. Did your organization **ever** experience a ransomware attack?	FY2021	US	EMEA
Yes	42%	45%	39%
No	54%	50%	58%
Unsure	4%	5%	3%
Total	100%	100%	100%

Q18b. If yes, how much was the ransom?	FY2021	US	EMEA
Less than $100	8%	7%	9%
$100 to $500	12%	11%	14%
$501 to $1,000	19%	18%	21%
$1,001 to $5,000	22%	22%	22%
$5,001 to $10,000	16%	17%	14%
More than $10,000	23%	25%	20%
Total	100%	100%	100%
Extrapolated value	5,432	5,857	4,914

Q18c. Did your company pay the ransom?	FY2021	US	EMEA
Yes	62%	69%	53%
No	38%	31%	47%
Total	100%	100%	100%

Q19. Have you taken the following steps to prepare for a ransomware incident? Please select all that apply.	FY2021	US	EMEA
Determined under what circumstances payment would be made to resolve the incident	12%	14%	10%
Audited and increased back up of data and systems	61%	65%	55%
Business continuity plan includes a planned system outage in the event of a ransomware incident	48%	50%	46%
Employees are educated about the ransomware risk	38%	38%	37%
Updating software on a regular basis	21%	23%	19%
Other	4%	3%	5%
Total	184%	193%	172%

Q20a. 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?	FY2021	US	EMEA
Yes	72%	76%	68%
No	28%	24%	32%
Total	100%	100%	100%

Q20b. If yes, how often is training conducted?	FY2021	US	EMEA
On-boarding new employees	49%	52%	46%
Every six months	3%	3%	2%
Annually	26%	25%	27%
Sporadically	21%	20%	23%
Unsure	1%	0%	2%
Total	100%	100%	100%

Part 4. Cyber insurance coverage

Q21a. Does your organization have a data breach or cyber insurance policy?	FY2021	US	EMEA
Yes	49%	54%	42%
No	51%	46%	58%
Total	100%	100%	100%

Q21b. If yes, have you changed the amount of coverage since COVID-19?	FY2021	US	EMEA
Yes	39%	41%	37%
No	61%	59%	63%
Total	100%	100%	100%

Q22. If your organization does not have a cyber insurance policy, does it plan to purchase a data breach or cyber insurance policy?	FY2021	US	EMEA
Yes, within the next six months	24%	29%	18%
Yes, within the next year	30%	27%	33%
Yes, within the next two years	7%	7%	8%
No plans to purchase	38%	35%	41%
Unsure	1%	2%	0%
Total	100%	100%	100%

Q23. What types of incidents does your organization's cyber insurance cover? Please select all that apply.	FY2021	US	EMEA
External attacks by cyber criminals	78%	86%	69%
Malicious or criminal insiders	63%	68%	56%
System or business process failures	31%	29%	34%
Human error, mistakes and negligence	42%	43%	40%
Incidents affecting business partners, vendors or other third parties that have access to your company's information assets	58%	60%	56%
Ransomware attacks	51%	55%	47%
Major security vulnerability in a product, website or service	51%	51%	51%
Other	6%	6%	5%
Total	380%	398%	358%

Q24. What coverage does this insurance offer your company? Please select all that apply.	FY2021	US	EMEA
Identity protection services to victims	70%	73%	67%
Call center support	57%	61%	53%
Forensics and investigative costs	62%	65%	58%
Notification costs to data breach victims	59%	63%	54%
Communication costs to regulators	14%	15%	12%
Employee productivity losses	9%	9%	8%
Replacement of lost or damaged equipment	42%	47%	36%
Revenue losses	19%	21%	17%
Legal defense costs	64%	69%	58%
Regulatory penalties and fines	28%	30%	26%
Third-party liability	60%	62%	58%
Brand damages	6%	7%	4%
IoT enabled device protection	17%	18%	15%
Other	7%	7%	6%
Total	513%	547%	472%

Part 5. Data breach response plan

Q25. 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.	FY2021	US	EMEA
Require they have an incident response plan your organization can review	86%	90%	80%
Require they notify your organization when they have a data breach	88%	88%	87%
Require audits of their security procedures	52%	53%	50%
No steps being taken	4%	4%	3%
Total	228%	235%	220%

Q26a. Does your organization have a data breach response plan in place?	FY2021	US	EMEA
Yes	89%	93%	84%
No	11%	7%	16%
Total	100%	100%	100%

Q26b. If yes, has the data breach response plan added plans to respond to data breaches created by a remote workforce?	FY2021	US	EMEA
Yes	48%	52%	42%
No	52%	48%	58%
Total	100%	100%	100%

Q26c. If your organization does not have a data breach response plan in place, why?	FY2021	US	EMEA
No resources or budget	42%	41%	44%
Not important to have data breach response plan in place	10%	10%	9%
Lack of C-level support	19%	19%	18%
Outsourced to consultants	29%	30%	28%
Other	0%	0%	1%
Total	100%	100%	100%

Q27. How often does your company update the data breach response plan?	FY2021	US	EMEA
Each quarter	4%	4%	5%
Twice per year	3%	3%	4%
Once each year	24%	23%	25%
No set time period for reviewing and updating the plan	41%	42%	40%
We have not reviewed or updated since the plan was put in place	27%	28%	26%
Total	100%	100%	100%

Q28. 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.	FY2021	US	EMEA
Conduct third-party cyber security assessments	51%	56%	45%
Integrate data breach response into business continuity plans	51%	52%	50%
Create a “standby website” for content that can be made live when an incident occurs	31%	33%	29%
Regularly review physical security and access to confidential information	62%	67%	56%
Meet with law enforcement and/or state regulators in advance of an incident	18%	16%	20%
Subscribe to a dark web monitoring service	28%	29%	27%
Conduct background checks on new full time employees and vendors	62%	64%	59%
Other	0%	0%	0%
Total	303%	317%	286%

Q29. Does your data breach response plan include the following requirements? Please select all that apply.	FY2021	US	EMEA
Required C-level approval of the data breach response plan	68%	70%	66%
Contact information for all members of the data breach response team	86%	90%	81%
Contact information for all members of the data breach backup response team	42%	41%	44%
Procedures for communicating with employees when a data breach occurs	46%	49%	43%
Procedures for responding to a data breach involving overseas locations	48%	47%	50%
Procedures for communicating with state attorneys general and regulators	73%	74%	72%
Procedures for communications with investors	48%	50%	45%
Procedures for communications with business partners and other third parties	59%	61%	57%
Review of a third party or business partner’s incident response plan	37%	36%	39%
Procedures for determining and offering identity theft protection services	39%	37%	42%
Procedures for reporting results of the forensics investigation to senior management	34%	33%	36%
Procedures for incorporating findings from the forensics investigations into the security strategy	27%	26%	29%
Other	5%	5%	4%
Total	614%	619%	608%

Q30. Does your data breach response plan offer guidance on managing the following security incidents? Please check all that apply.	FY2021	US	EMEA
Loss or theft of payment information, including credit cards	75%	79%	69%
Loss or theft of personally identifiable information	78%	81%	74%
Destructive malware such as ransomware	60%	58%	62%
IoT-based attacks	30%	31%	28%
Hacktivism/activism	37%	35%	39%
Attacks via the Internet or social media	58%	60%	55%
W-2 and other phishing fraud scams	57%	56%	59%
Distributed denial of service attack (DDoS) that causes a system outage	91%	91%	90%
Loss or theft of information about customer affiliations/associations that would result in damage to your organization's reputation	86%	88%	83%
Loss or theft of intellectual property or confidential business information	74%	73%	75%
Data breach caused by a malicious employee or contractor	57%	54%	61%
Your organization is threatened with extortion as a result of the theft of sensitive and confidential information	62%	63%	60%
Loss or theft of paper documents and tapes containing sensitive and confidential information	37%	36%	39%
Other	6%	6%	5%
Total	806%	811%	799%

Q31. How could your data breach response plan become more effective? Please select the top three choices.	FY2021	US	EMEA
Conduct more drills to practice data breach response	81%	88%	73%
Have formal documentation of incident response procedures	58%	67%	47%
Incorporate what was learned from previous data breaches	70%	72%	68%
Ensure seamless coordination among all departments involved in incident response	45%	45%	44%
Increase participation and oversight from senior executives	74%	79%	68%
Assign individuals with a high level of expertise in security to the team	80%	83%	76%
Assign individuals with a high level of expertise in compliance with privacy, data protection laws and regulations to the team	45%	49%	39%
Have a budget dedicated to data breach preparedness	61%	61%	60%
Increase involvement of third-party experts	43%	45%	41%
Other	3%	3%	2%
Total	559%	592%	518%

Q32a. Does your organization hire a third-party to manage your organization's data breach response plan?	FY2021	US	EMEA
Yes	54%	59%	48%
No	46%	41%	52%
Total	100%	100%	100%

Q32b. If yes, do you ask for recommendations to make a decision to hiring a third-party?	FY2021	US	EMEA
Recommendations from our insurance company	43%	45%	40%
Recommendations from the general counsel	42%	41%	43%
Recommendations from other organizations	23%	23%	23%
Other (please specify)	4%	4%	5%
We do not ask for recommendations	26%	30%	21%
Total	138%	143%	132%

Q32c. If yes, do you use any of the following criteria to select a third party?	FY2021	US	EMEA
Years of experience	49%	54%	43%
Client testimonials	30%	31%	29%
The services offered	48%	50%	46%
Trustworthiness of the third party	55%	56%	53%
Documented evidence of the third party's success in mitigating the consequences of the data breach	46%	48%	44%
Ability to respond to a data breach caused by the remote workforce	43%	47%	39%
Other (please specify)	3%	3%	2%
Total	274%	289%	256%

Q33a. Does your organization practice data breach response?	FY2021	US	EMEA
At least twice a year	47%	50%	43%
Once each year	13%	16%	10%
Every two years	8%	7%	10%
More than two years	11%	8%	15%
Never	2%	2%	2%
No set schedule	18%	17%	20%
Total	100%	100%	100%

Q33b. If your organization practices data breach response, what is included in the practice response? Please check all that apply.	FY2021	US	EMEA
Fire drills	60%	65%	54%
Case discussions	50%	53%	46%
Simulations	66%	68%	63%
Training and awareness about security threats facing the organization	68%	70%	65%
Review of the plan by the person/function most responsible for data breach response	76%	78%	73%
Review of data breach communications plans	46%	51%	40%
Review of what was learned from previous data breaches or other security incidents	63%	60%	67%
None of the above	16%	17%	14%
Other	3%	3%	3%
Total	447%	465%	425%

Q33c. If your organization never practices data breach response, why not?	FY2021	US	EMEA
Not enough budget	29%	29%	30%
We are confident in our ability to respond to a data breach	41%	40%	42%
Too difficult to schedule a practice response	64%	69%	57%
Not a priority	63%	65%	60%
Total	197%	203%	189%

Q34a. Does your incident response plan include processes to manage an international data breach?	FY2021	US	EMEA
Yes	47%	54%	38%
No	46%	39%	54%
Unsure	7%	7%	8%
Total	100%	100%	100%

Q34b. If yes, is your organization’s plan specific to each location where it operates?	FY2021	US	EMEA
Yes	53%	59%	46%
No	44%	38%	51%
Unsure	3%	3%	3%
Total	100%	100%	100%

Q35. How confident is your organization in its ability to deal with an international data breach?	FY2021	US	EMEA
Very confident	14%	13%	15%
Confident	21%	21%	22%
Somewhat confident	25%	25%	24%
Not confident	28%	30%	25%
No confidence	12%	11%	14%
Total	100%	100%	100%

Part 6. Regulations

Q36a. Is your company subject to the General Data Protection Regulation (GDPR)?	FY2021	US	EMEA
Yes	93%	89%	98%
No	7%	11%	2%
Total	100%	100%	100%

Q36b. Using the following 10-point scale, please rate the impact the General Data Protection Regulation (GDPR) has on your organization's data breach response plan. 1 = No impact to 10 = high impact.	FY2021	US	EMEA
1 to 2	1%	0%	2%
3 to 4	9%	9%	8%
5 to 6	11%	12%	9%
7 to 8	40%	39%	42%
9 to 10	40%	40%	39%
Total	100%	100%	100%
Extrapolated value	7.68	7.70	7.66

Q37a. Is your company subject to the California Consumer Privacy Act (CCPA)?	FY2021	US	EMEA
Yes	35%	45%	23%
No	65%	55%	77%
Total	100%	100%	100%

Q37b. Using the following 10-point scale, please rate the impact the CCPA has on your organization's data breach response plan. 1 = No impact to 10 = high impact.	FY2021	US	EMEA
1 to 2	15%	11%	20%
3 to 4	18%	16%	21%
5 to 6	29%	34%	23%
7 to 8	26%	26%	26%
9 to 10	12%	13%	10%
Total	100%	100%	100%
Extrapolated value	5.52	5.78	5.20

Q38a. Is your company subject to Europe's Directive on Security of Network and Information Systems (NIS)?	FY2021	US	EMEA
Yes	44%	26%	65%
No	56%	74%	35%
Total	100%	100%	100%

Q38b. Using the following 10-point scale, please rate the impact the NIS has on your organization's data breach response plan. 1 = No impact to 10 = high impact.	FY2021	US	EMEA
1 to 2	5%	6%	3%
3 to 4	13%	15%	11%
5 to 6	18%	19%	16%
7 to 8	30%	26%	35%
9 to 10	34%	34%	35%
Total	100%	100%	100%
Extrapolated value	7.03	6.84	7.26

Q39a. Is your company subject to the Health Insurance Portability & Accountability Act (HIPAA)?	FY2021	US	EMEA
Yes	47%	67%	23%
No	53%	33%	77%
Total	100%	100%	100%

Q39b. Using the following 10-point scale, please rate the impact HIPAAA has on your organization’s data breach response plan. 1 = No impact to 10 = high impact.	FY2021	US	EMEA
1 to 2	12%	4%	21%
3 to 4	15%	9%	23%
5 to 6	18%	17%	19%
7 to 8	27%	33%	20%
9 to 10	28%	37%	17%
Total	100%	100%	100%
Extrapolated value	6.39	7.30	5.28

Q40a. Is your company subject to the Federal Information Security Management Act (FISMA)	FY2021	US	EMEA
Yes	39%	63%	10%
No	61%	37%	90%
Total	100%	100%	100%

Q40b. Using the following 10-point scale, please rate the impact the FISMA has on your organization’s data breach response plan. 1 = No impact to 10 = high impact.	FY2021	US	EMEA
1 to 2	13%	7%	20%
3 to 4	17%	10%	25%
5 to 6	16%	18%	13%
7 to 8	29%	34%	22%
9 to 10	26%	31%	20%
Total	100%	100%	100%
Extrapolated value	6.27	6.94	5.44

Q41a. In the past two years, how many personal data breaches did your organization have that were required to be reported to regulators?	FY2021	US	EMEA
None	30%	30%	30%
1 to 5	40%	40%	39%
6 to 20	18%	15%	21%
More than 20	13%	15%	10%
Total	100%	100%	100%
Extrapolated value	6.68	6.90	6.40

FY2019 data for GDPR only

Q41b. How many of the data breaches did you report to the Regulator?	FY2021	US	EMEA
None	44%	43%	46%
1 to 5	36%	36%	36%
6 to 20	11%	12%	10%
More than 20	9%	9%	8%
Total	100%	100%	100%
Extrapolated value	4.66	4.89	4.38

Part 7. Perceptions about the future

Q42a. Will remote working become the new norm?	FY2021	US	EMEA
Yes	56%	63%	47%
No	36%	29%	44%
Unsure	8%	8%	9%
Total	100%	100%	100%

Q42b. If yes, what changes will your organization make to its privacy and security practices?	FY2021	US	EMEA
Conduct more training and awareness programs to ensure employees and contractors adhere to our organization's security and policy policies while working remotely	61%	65%	55%
Conduct risk assessments of vulnerabilities created by a remote work force	56%	63%	47%
Develop and enforce privacy and security policies for a remote workforce	56%	60%	50%
Hire more in-house expertise	70%	73%	67%
Increase investment in enabling security technologies	64%	69%	57%
Other	4%	5%	3%
Total	310%	335%	279%

Q43. In the next 12 months, what concerns your organization most?	FY2021	US	EMEA
An increase in security incidents and data breaches	62%	65%	59%
Nation state attacks targeting our organization's high value information assets	42%	43%	40%
Our organization will not have the ability to retain skilled staff needed to mitigate security risks	47%	51%	43%
The inability to ensure that employees and contractors are following our organization's security and privacy policies	37%	39%	34%
The inability to prevent such incidents as downtime, employee negligence and malicious behavior	40%	47%	31%
The inability to respond to contain and remediate data breaches and security incidents	30%	36%	23%
Other	4%	5%	3%
Total	262%	286%	233%

Part 8. Organizational characteristics & respondent demographics

D1. What organizational level best describes your current position?	FY2021	US	EMEA
Senior Executive	6%	7%	5%
Vice President	11%	12%	10%
Director	29%	27%	31%
Manager	22%	19%	26%
Supervisor	19%	21%	17%
Technician	8%	9%	7%
Staff	4%	4%	4%
Contractor	0%	0%	0%
Other	1%	1%	0%
Total	100%	100%	100%

D2. Check the **Primary Person** you report to within your organization.	FY2021	US	EMEA
CEO/Executive Committee	5%	5%	4%
Chief Financial Officer	5%	6%	3%
General Counsel	12%	12%	12%
Chief Privacy Officer	10%	10%	11%
Chief Information Officer	14%	13%	15%
Compliance Officer	19%	17%	21%
Human Resources VP	1%	2%	0%
Chief Security Officer	4%	4%	5%
Chief Risk Officer	11%	12%	10%
Chief Information Security Officer	18%	18%	17%
Other	1%	1%	2%
Total	100%	100%	100%

D3. What industry best describes your organization’s industry focus?	FY2021	US	EMEA
Agriculture & food service	1%	1%	2%
Communications	2%	2%	3%
Consumer products	4%	4%	5%
Defense & aerospace	1%	1%	0%
Education & research	2%	2%	3%
Energy & utilities	6%	6%	6%
Entertainment & media	4%	4%	5%
Financial services	18%	18%	17%
Health & pharmaceuticals	10%	11%	9%
Hospitality	2%	2%	2%
Industrial & manufacturing	11%	11%	10%
Other	3%	3%	4%
Public sector	11%	11%	11%
Services	12%	12%	11%
Technology & software	9%	8%	10%
Transportation	3%	4%	2%
Total	100%	100%	100%

D4. What is the worldwide headcount of your organization?	FY2021	US	EMEA
Less than 500	15%	12%	18%
500 to 1,000	20%	17%	23%
1,001 to 5,000	23%	21%	25%
5,001 to 25,000	17%	19%	14%
25,001 to 75,000	19%	23%	15%
More than 75,000	7%	8%	5%
Total	100%	100%	100%

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

Ponemon Institute

Advancing Responsible Information Management

Ponemon Institute is dedicated to independent research and education that advances responsible information and privacy management practices within business and government. Our mission is to conduct high quality, empirical studies on critical issues affecting the management and security of sensitive information about people and organizations.

We uphold strict data confidentiality, privacy and ethical research standards. We do not collect any personally identifiable information from individuals (or company identifiable information in our business research). Furthermore, we have strict confidentiality standards to ensure that subjects are not asked extraneous, irrelevant or improper questions.

Experian® Data Breach Resolution

Experian® Data Breach Resolution, powered by the nation's largest credit bureau, is a leader in helping businesses prepare for a data breach via the proprietary Experian Reserved Response™ program and in mitigating consumer risk following breach incidents. With almost two decades of experience, Experian has successfully serviced some of the largest and highest-profile data breaches in history. Our experience managing tens of thousands of client incidents, for organizations of all sizes and virtually in every industry, puts Experian in a unique position to meet your needs. We specialize in swift and effective incident management, notification, call center support and fraud resolution services while serving millions of affected consumers with proven credit and identity protection products. For more information, visit www.experian.com/databreach