Ninth 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 2022

Ponemon INSTITUTE

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

Ponemon Institute, February 2022

Table of Contents	From Page	To Page
Part 1. Introduction	**2**	**3**
Part 2. Key findings	**4**	**30**
The state of data breach preparedness	**4**	**11**
Data breach response plans	**12**	**23**
Rising threats against organizations	**24**	**25**
Regulations that affect data breach preparedness	**26**	**26**
Perceptions about the future	**27**	**27**
Differences between the United States and EMEA	**28**	**30**
Part 3. Methods	**31**	**33**
Part 4. Caveats	**33**	**33**
Appendix: Detailed survey results	**34**	**51**

Part 1. Introduction

The *Ninth Annual Study: Is Your Company Ready for a Big Data Breach?* sponsored by Experian® Data Breach Resolution and conducted by Ponemon Institute tracks the state of data breach preparedness on an annual basis. In this year's research, we explore the value of Business Continuity Management (BCM) and crisis management plans to minimizing the consequences of a data breach.

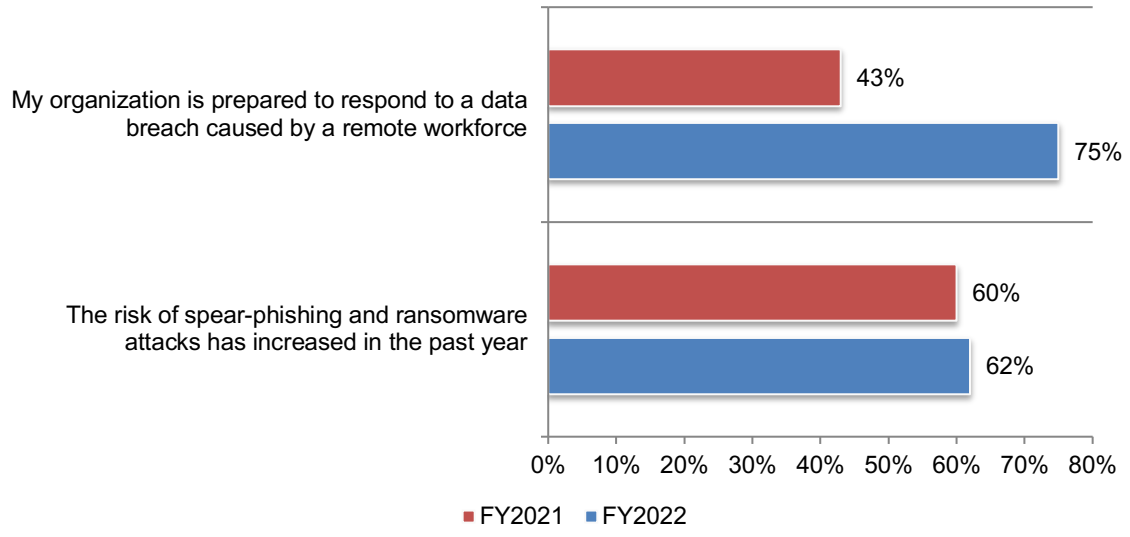
BCM plans involve systems to prevent and respond to a data breach. In addition to prevention and response, the goal is to enable ongoing operations before and during the resolution of the data breach. The purpose of a crisis management plan is to provide guidance on how organizations should respond in a crisis such as a data breach and how to reduce the long-term damage. The number one crisis covered is a cyberattack (46 percent of respondents) followed by data breaches (44 percent of respondents).

Ponemon Institute surveyed 605 professionals in the United States and 465 in EMEA[1]. A comparison of the US and EMEA findings is presented in this report. All respondents work in IT and IT security, compliance and privacy, and are involved in data breach preparedness 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 because of malicious attacks, hactivism or criminal attacks that seek to obtain valuable data, disrupt business operation or tarnish reputation.

While spear-phishing and ransomware attacks continue to increase, it is noteworthy that the ability to respond to a data breach caused by a remote workforce has improved significantly. As shown in Figure 1, in last year's study only 43 percent of respondents said their organization had confidence in their response capabilities. This year, 75 percent of respondents say their organizations are prepared for a data breach caused by a remote workforce. Sixty-two percent of respondents say spear-phishing and ransomware attacks continue to increase.

Figure 1. The continuing risk of spear-phishing, ransomware and remote workers
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.

Organizations need to be prepared for a data breach global in scope or caused by a third party in their supply chain. Forty-nine percent of respondents have faced the challenge of responding to international data breaches. Fifty percent of respondents say third parties in their supply chain caused the data breach.

Boards of directors and C-suite executives need to be more engaged in data breach preparedness. Fifty-seven 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. However, participation in data breach preparedness only involves a high-level review of the organization's data protection and privacy practices. Further, only 43 percent of respondents say they understand the specific threats facing the organization and only 42 percent of respondents say they have requested to be notified ASAP if a material data breach occurs.

The maturity of privacy and data protection programs have increased since last year. More organizations in this year's research have achieved the late-middle stage (31 percent of respondents) and mature stage (25 percent of respondents) with their privacy and data protection program. The benefits are the more extensive deployment of privacy and data protection program activities. C-level executives are regularly informed about the effectiveness of the program and support an adequate budget.

Organizations are still struggling to improve IT security's ability to respond to a data breach. A lack of visibility into end-user access of sensitive and confidential information is the number one barrier to improving IT security's data breach response. Proliferation of cloud services is considered by 58 percent of respondents a deterrent to improving data breach response as well as the lack of in-house expertise (40 percent of respondents).

Organizations need to be prepared for a third-party data breach that has their sensitive information. Fifty percent of respondents say that one or more data breaches their organization experienced was the result of an incident involving a third party in its supply chain. Virtually all (91 percent) respondents say their organizations have a data breach response plan in place. Despite the risk, only about half (56 percent) of respondents are requiring an audit of third-parties' security procedures. Consistent with last year's research, 86 percent of respondents say their organizations require notification when they have a data breach and 81 percent of respondents say they require an incident response plan they can review.

Most data breach response plans are stale and may not reflect the potential threats facing their organizations. Sixty-four percent of respondents say there is no set time for reviewing and updating the data breach plan (35 percent) or it has not been reviewed or updated since the plan was put in place (29 percent).

With the increase in global data breaches, more response plans are addressing procedures to mitigate the consequences of these type of incidents. Fifty-six percent of respondents say their organizations' plan includes how to manage an international data breach, an increase from 47 percent. Fifty-six percent of respondents say the plans are country specific. Despite having this information, only 31 percent of respondents are very confident (10 percent) or confident (21 percent) in their ability to deal with an international data breach.

Part 2. Key findings

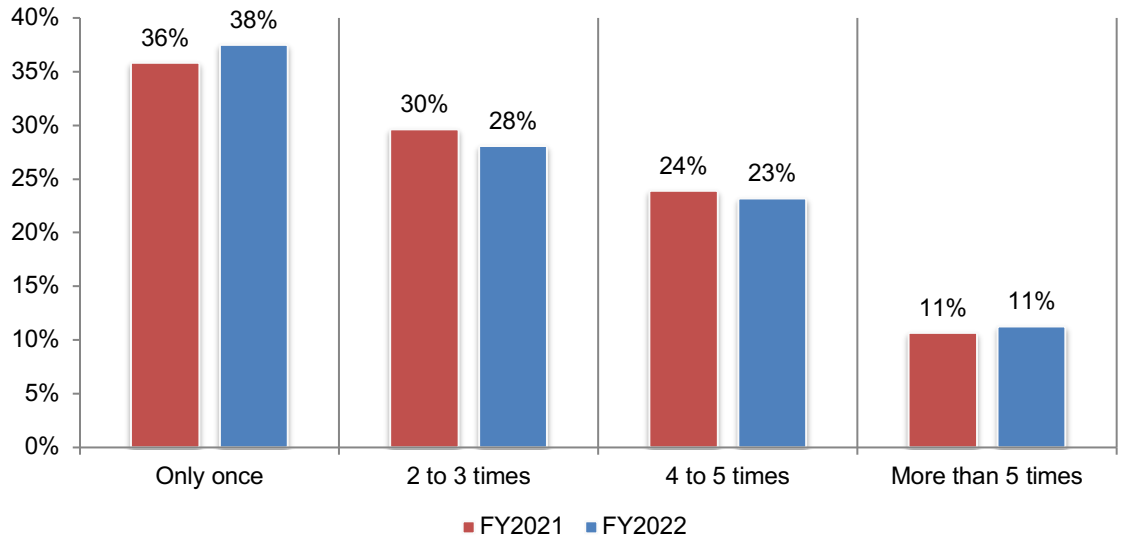
In this section, we provide an analysis of the US and EMEA results over the past one to two years as shown. The complete audited findings are presented in the Appendix of this report. We have organized this report according to the following topics:

- The state of data breach preparedness
- Trends in data breach response plans
- Rising threats against organizations
- 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

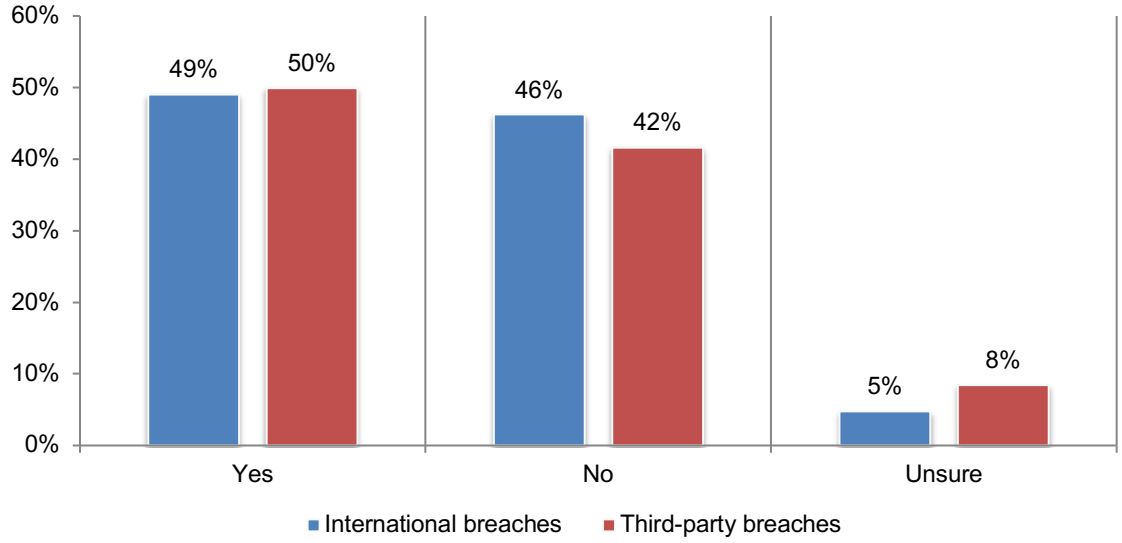
Organizations that have had a data breach involving the loss or theft of more than 1,000 records in the past two years has increased from 59 percent in 2021 to 63 percent in this year's study. As shown in Figure 2, 62 percent of respondents say their organizations have had more than one data breach during 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?



Organizations need to be prepared for a data breach global in scope or caused by a third party in their supply chain. Forty-nine percent of respondents have faced the challenge of responding to international data breaches as shown in Figure 3. Fifty percent of respondents say third parties in their supply chain caused the data breach.

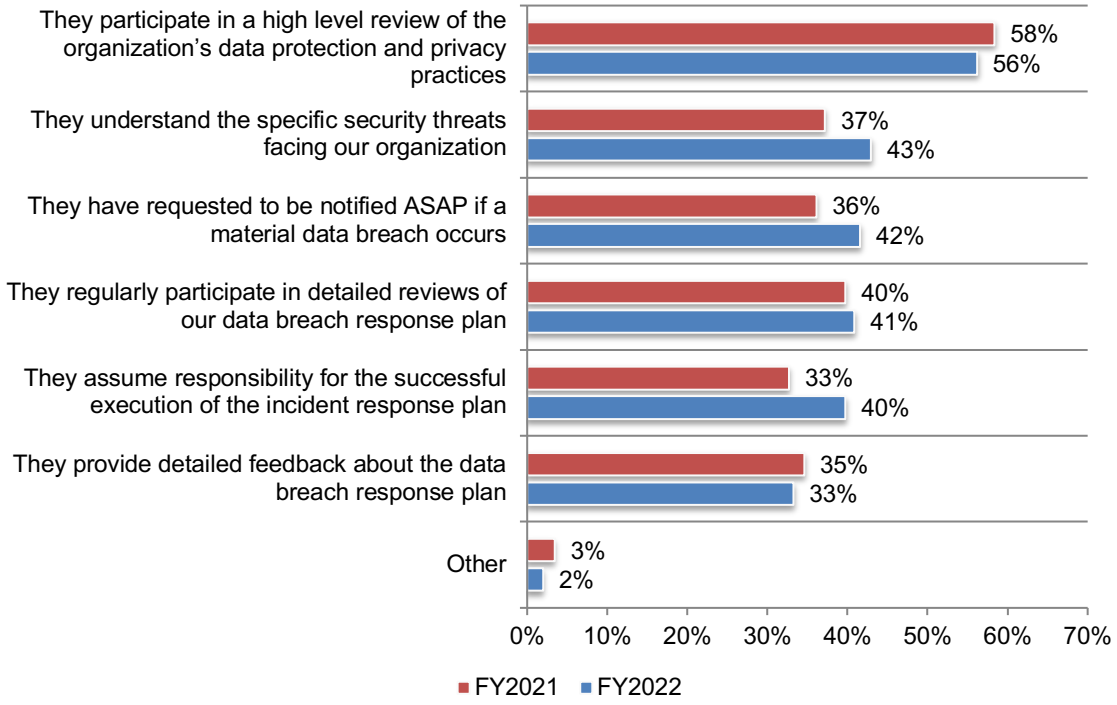
Figure 3. Were these breaches international in scope and were they the result of a third party in your organization's supply chain?



Boards of directors and C-suite executives are considered knowledgeable but not engaged in plans to deal with a possible data breach. Fifty-seven 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.

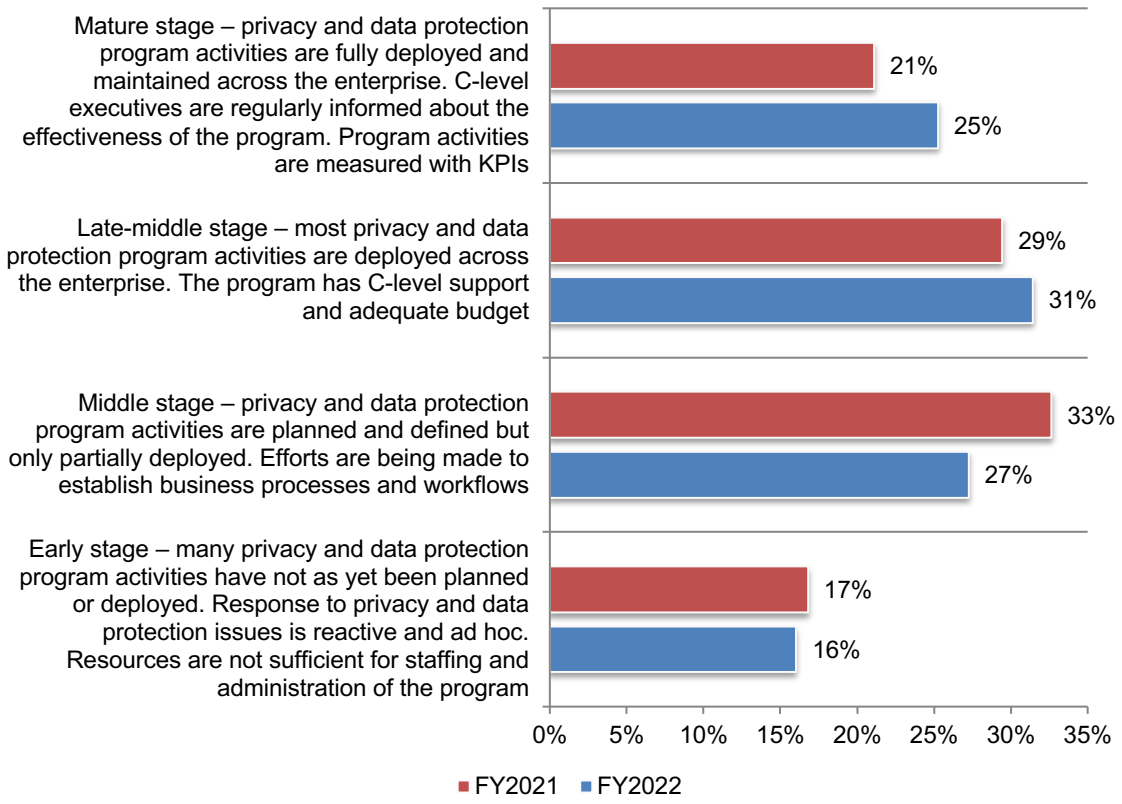
However, indications of their lack of engagement are presented in Figure 4. The top indicator is that they participate only in a high-level review of the organization's data protection and privacy practices. Further, only 43 percent of respondents say they understand the specific threats facing the organization and only 42 percent of respondents say they have requested to be notified ASAP if a material data breach occurs.

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



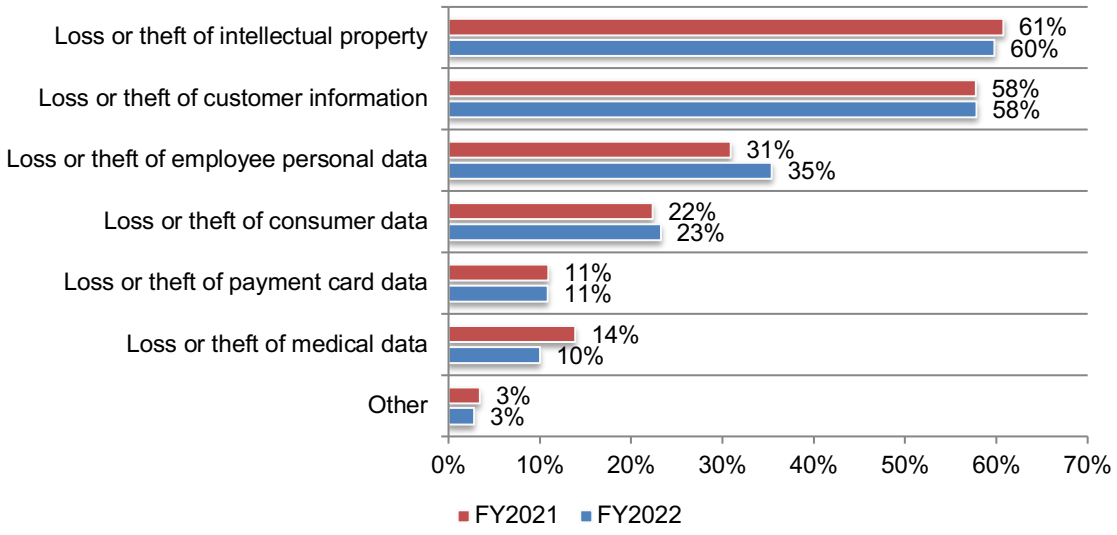
The maturity of privacy and data protection programs increased since last year. As shown in Figure 5, more organizations in this year's research have achieved the late-middle stage (31 percent of respondents) and mature stage (25 percent of respondents) with their privacy and data protection program. The benefits are the more extensive deployment of privacy and data protection program activities. C-level executives are regularly informed about the effectiveness of the program and support an adequate budget.

Figure 5. What best describes the maturity of your organization's privacy and data protection program?



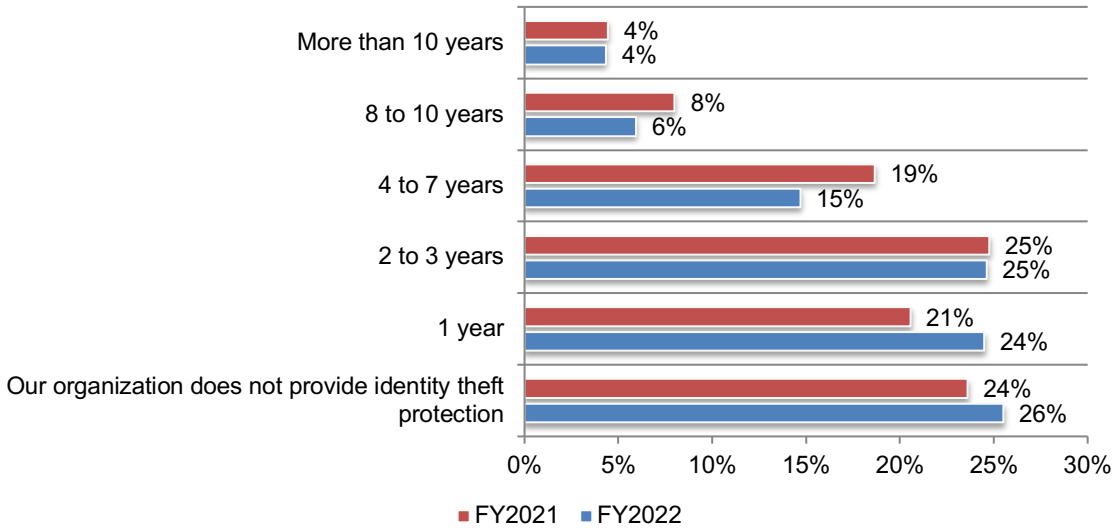
IP and customer information are still considered the data types most at risk. As shown in Figure 6, 60 percent of respondents say their organizations worry most about the loss or theft of intellectual property followed by 58 percent of respondents who say they are most concerned about the loss or theft of customer information.

Figure 6. 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 7, 74 percent of respondents say their organizations offer identity theft protection for at least one year. Twenty-five percent of respondents say such protection is provided for at least four years, a slight decrease from 31 percent of respondents in 2021.

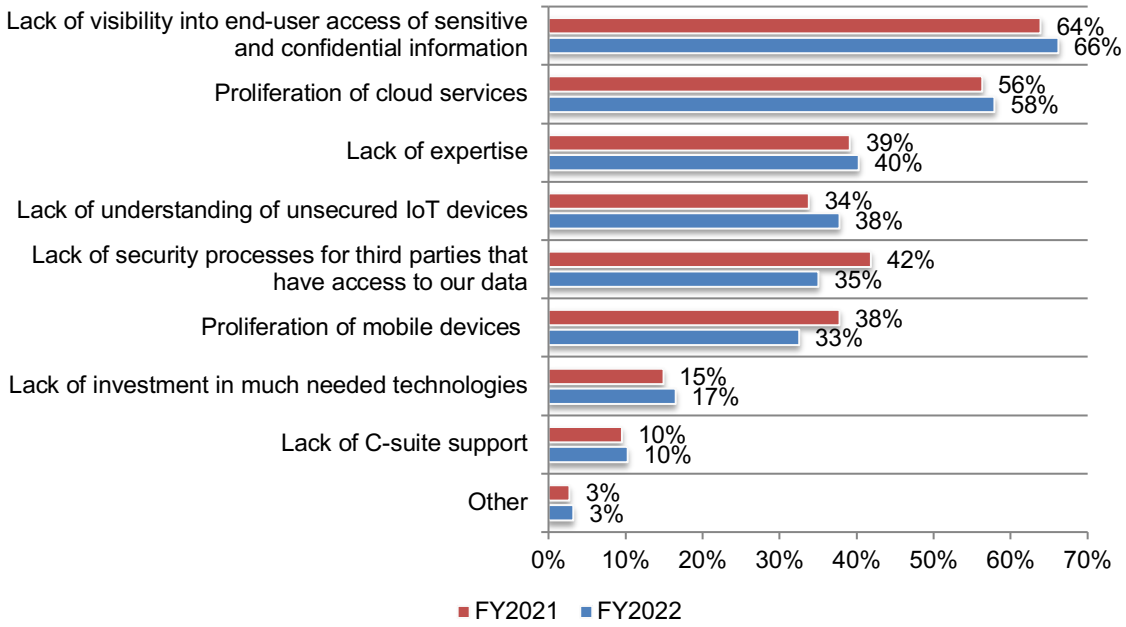
Figure 7. How long should identity theft protection be provided to data breach victims?



Organizations are still struggling to improve IT security's ability to respond to a data breach. As shown in Figure 8, a lack of visibility into end-user access of sensitive and confidential information is the number one barrier to improving IT security's data breach response, an increase from 64 percent of respondents in 2021 to 66 percent of respondents in 2022. Proliferation of cloud services is considered by 58 percent of respondents a deterrent to improving data breach response as well as the lack of in-house expertise (40 percent of respondents).

Figure 8. The biggest barriers to improving the ability of IT security to respond to a data breach

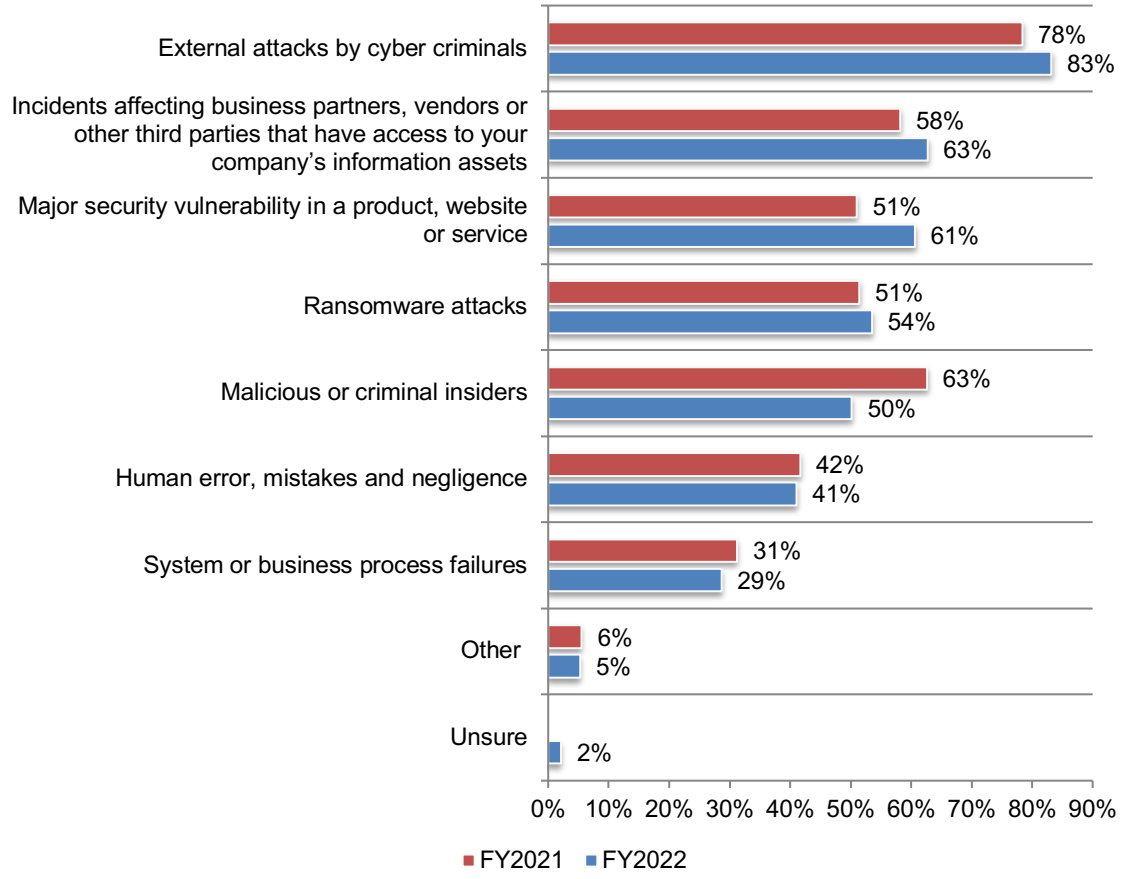
Three responses permitted



Purchases of cyber insurance increased. In last year's research, about half (49 percent) of respondents said their organizations purchased a data breach and cyber insurance policy. This year it has increased to 53 percent of respondents. Of the 47 percent of respondents who currently do not have a cyber insurance policy, 71 percent will purchase it within the next two years, an increase from 61 percent of respondents last year.

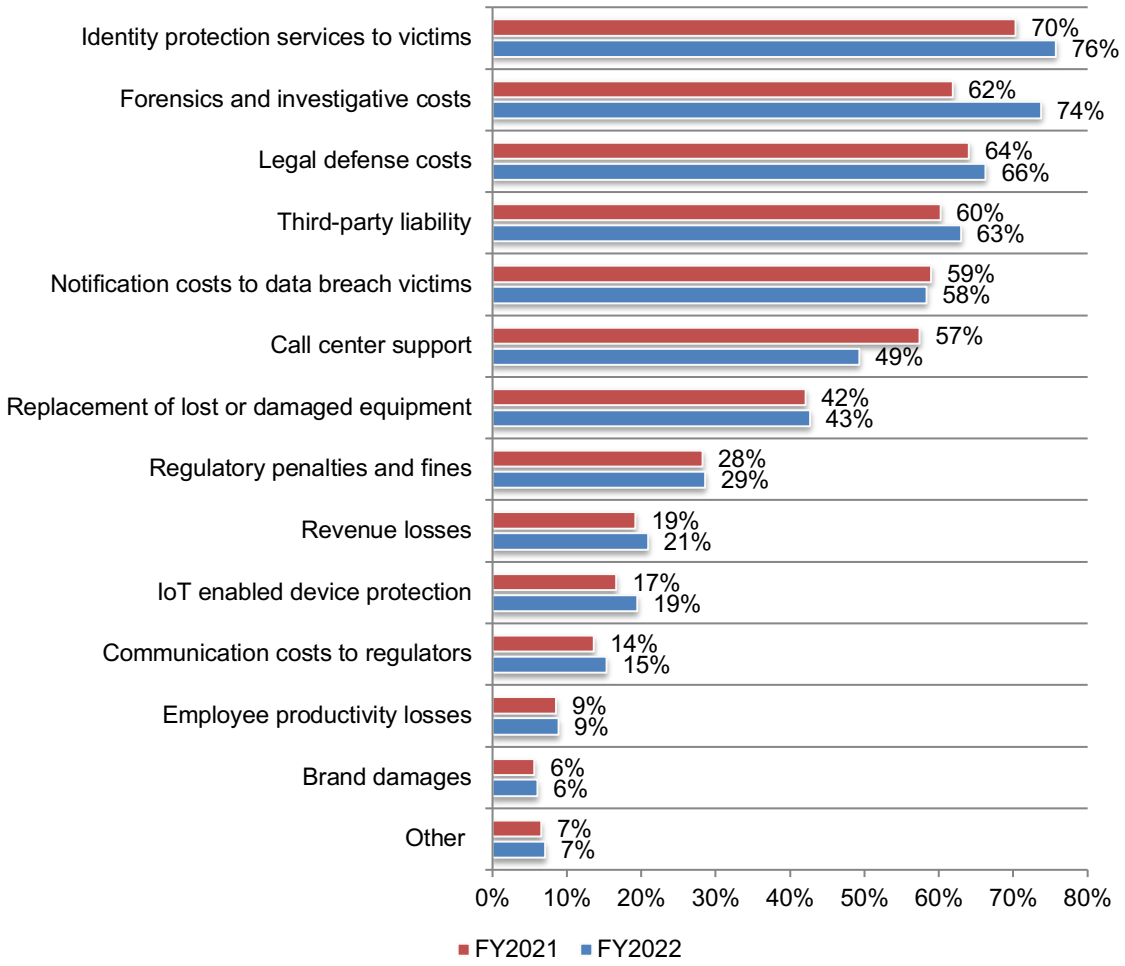
According to Figure 9, 83 percent of respondents say their cyber insurance policy covers incidents caused by cyber criminals an increase from 78 percent last year and 63 percent of respondents say it covers data breaches caused by third parties. The coverage of malicious or criminal insiders decreased from 63 percent of respondents to 50 percent of respondents. Only 41 percent of respondents say it covers human error, one of the major causes of a data breach.

Figure 9. What types of incidents does your organization's cyber insurance cover?
More than one response permitted



More policies cover forensics and investigative costs. Figure 10 presents the various types of coverage provided by the cyber insurance policy. As shown, 74 percent of respondents, an increase from 62 percent of respondents in 2021, say the policy covers forensics and investigative costs. Coverage of identity protection services to victims remains the number one coverage and has also increased significantly from 70 percent of respondents to 76 percent of respondents in this year's research.

Figure 10. What coverage does this insurance offer your company?
More than one response permitted

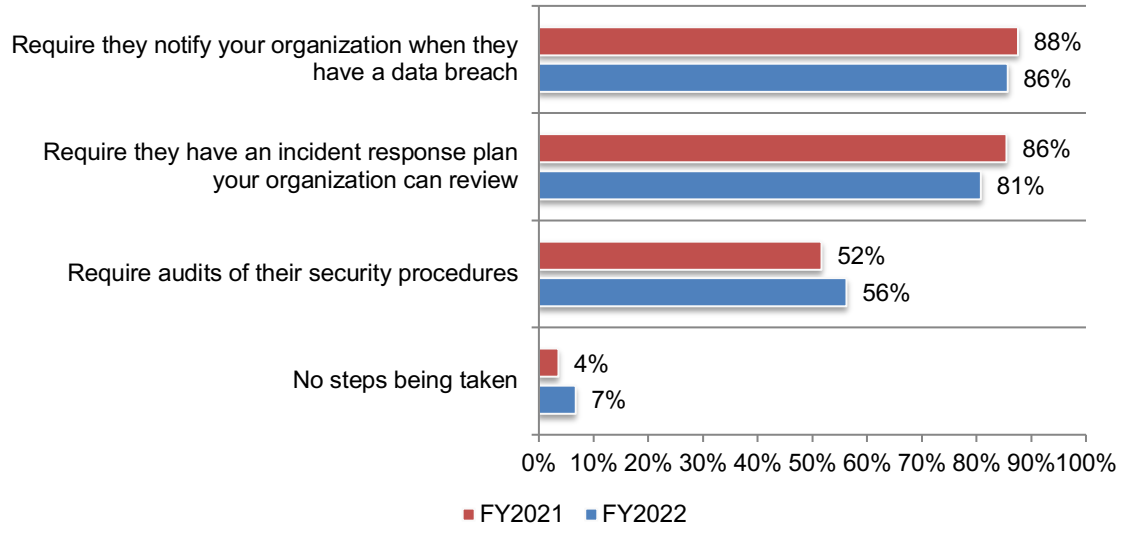


Data breach response plans

Organizations need to be prepared for a third-party data breach that has their sensitive information. Fifty percent of respondents say the one or more data breaches their organization experienced was the result of an incident involving a third party in its supply chain.

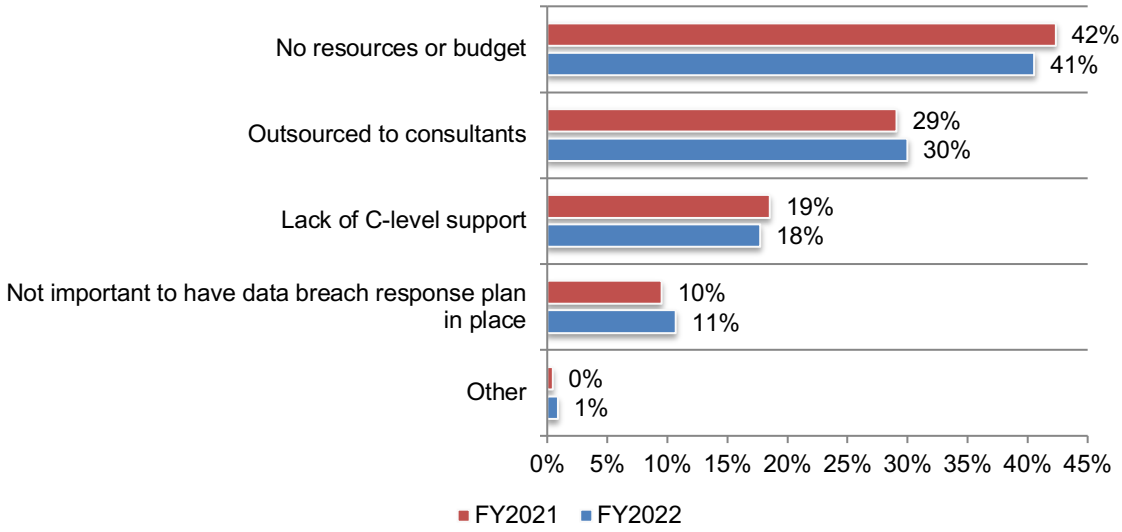
Virtually all (91 percent) respondents say their organizations have a data breach response plan in place. According to Figure 11, despite the risk only about half (56 percent) of respondents are requiring an audit of third-parties' security procedures as part of the plan. Consistent with last year's research, 86 percent of respondents say their organizations require notification when they have a data breach and 81 percent of respondents say they require an incident response plan they can review.

Figure 11. What steps do you take to minimize the consequences of a data breach involving a third party?
More than one response permitted



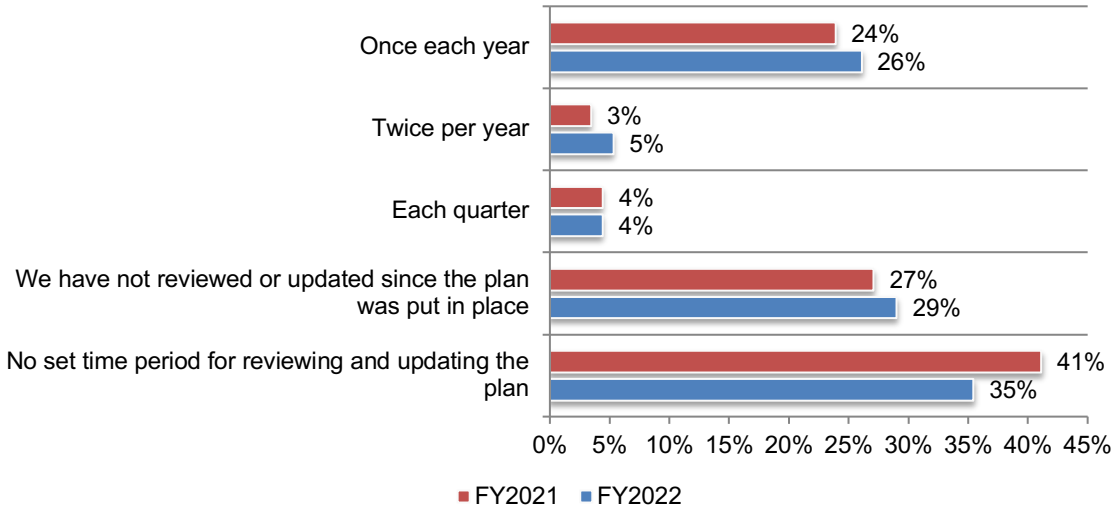
Despite the reputational and financial consequences of a data breach, it is surprising that even a few (9 percent) organizations do not have a data breach response plan. According to Figure 12, 11 percent of these respondents say such a plan is not important. Forty-one percent of these respondents say it is because of a lack of resources or budget.

Figure 12. Why doesn't your organization have a data breach response plan?



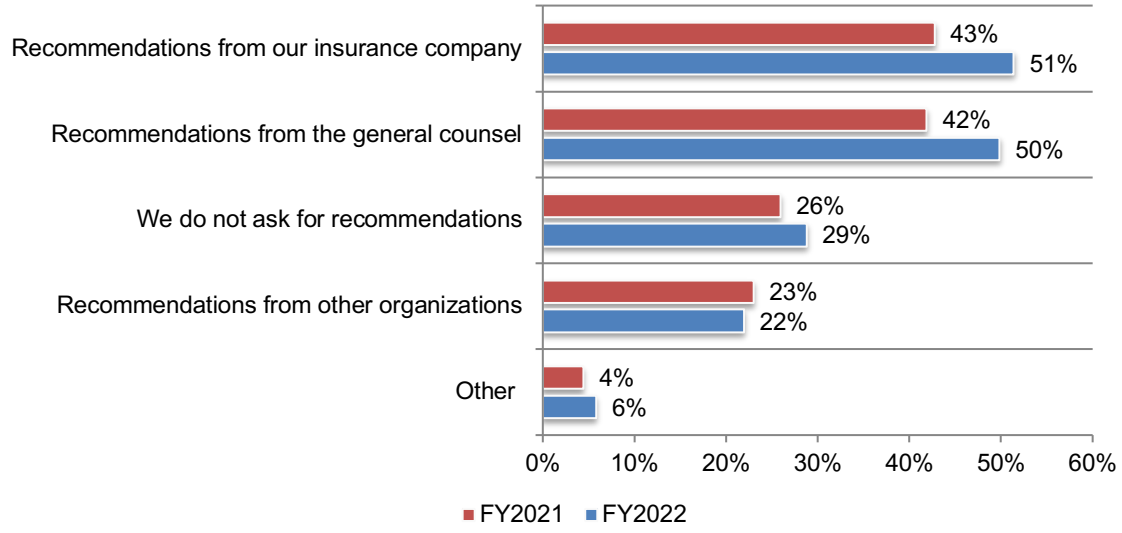
Most data breach response plans are stale and may not reflect the potential threats facing their organizations. As shown in Figure 13, 64 percent of respondents say there is no set time for reviewing and updating the plan (35 percent) or they have not reviewed or updated it since the plan was put in place (29 percent).

Figure 13. How often does your company update the data breach response plan?



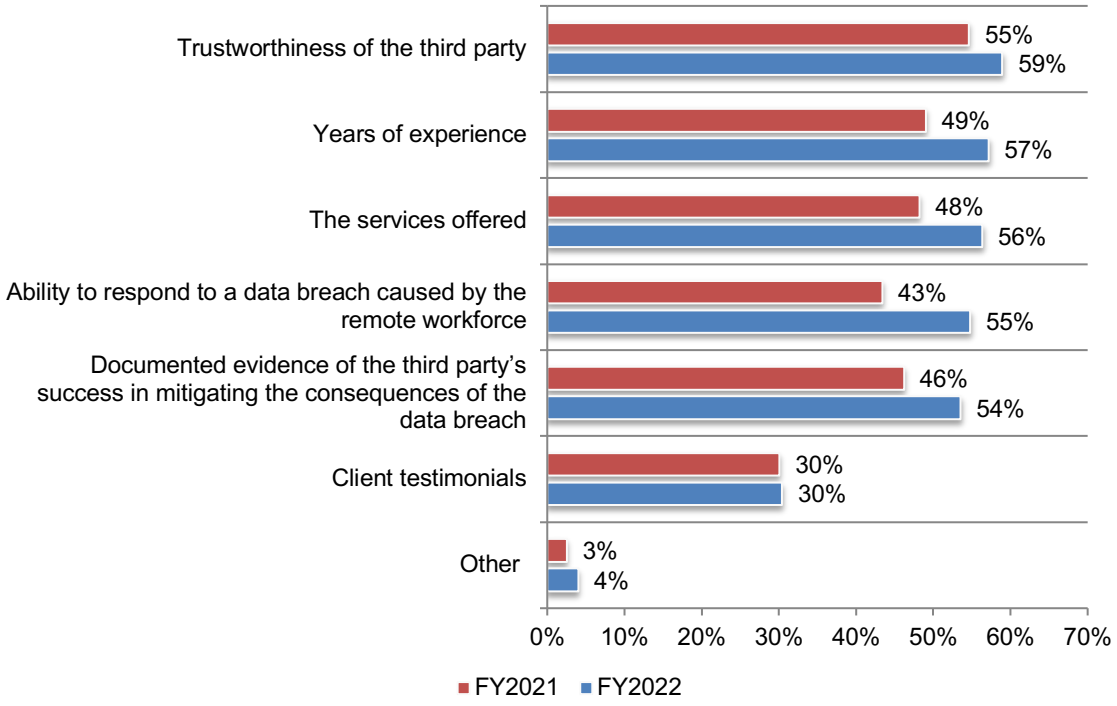
Organizations are relying more upon third parties to manage their data breach response plan. Sixty-one percent of respondents, an increase from 54 percent of respondents in last year's research, plan to hire a third-party to manage the plan. Of these respondents, 71 percent say they ask for recommendations on hiring a third party. Most recommendations are made by insurance companies or the general counsel, as shown in Figure 14.

Figure 14. Does your organization ask for recommendations before hiring a third party?
More than one response permitted



There is a significant shift in criteria used to select a third party. According to Figure 15, the importance of the third party's ability to respond to a data breach caused by a remote workforce has increased from 43 percent of respondents to 55 percent of respondents. Documented evidence of the third party's success in mitigating the consequences of the data breach has increased from 46 percent of respondents to 54 percent of respondents and the services offered grew from 48 percent of respondents to 56 percent of respondents. Trust, however, is still the number one criterion.

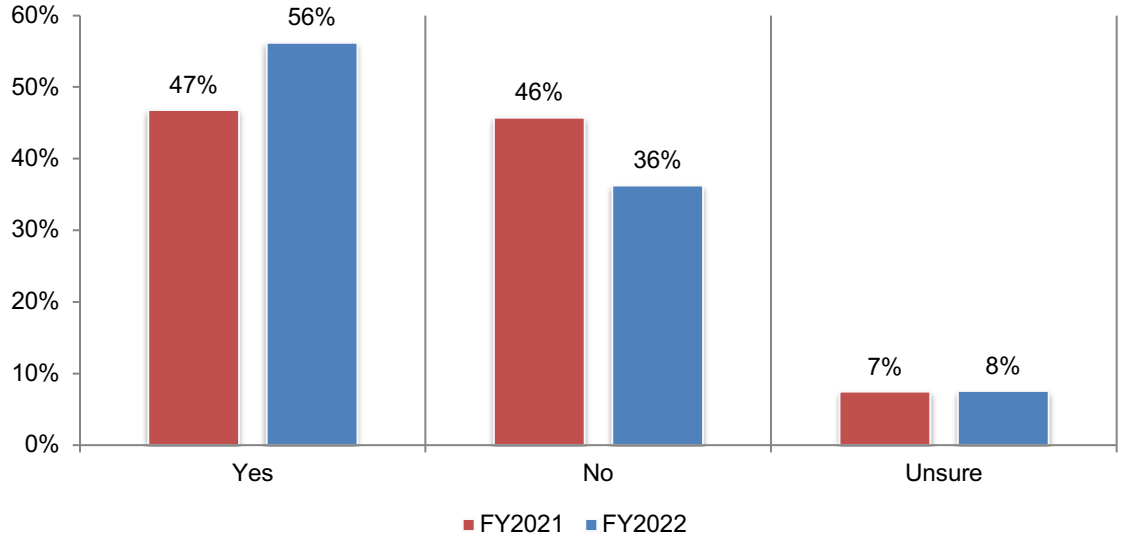
Figure 15. What criteria is used to select a third party?
More than one response permitted



With the increase in global data breaches, more response plans are addressing procedures to mitigate the consequences of these type of incidents. As discussed previously, 62 percent of respondents say their organizations had one or more data breaches in the past two years. Of these respondents, 49 percent of respondents say one more of these breaches were global.

According to Figure 16, 56 percent of respondents say their organizations' plan includes how to manage an international data breach, an increase from 47 percent. Fifty-six percent of respondents say the plans are country specific. Despite having this information, only 31 percent of respondents are very confident (10 percent) or confident (21 percent) in their ability to deal with an international data breach.

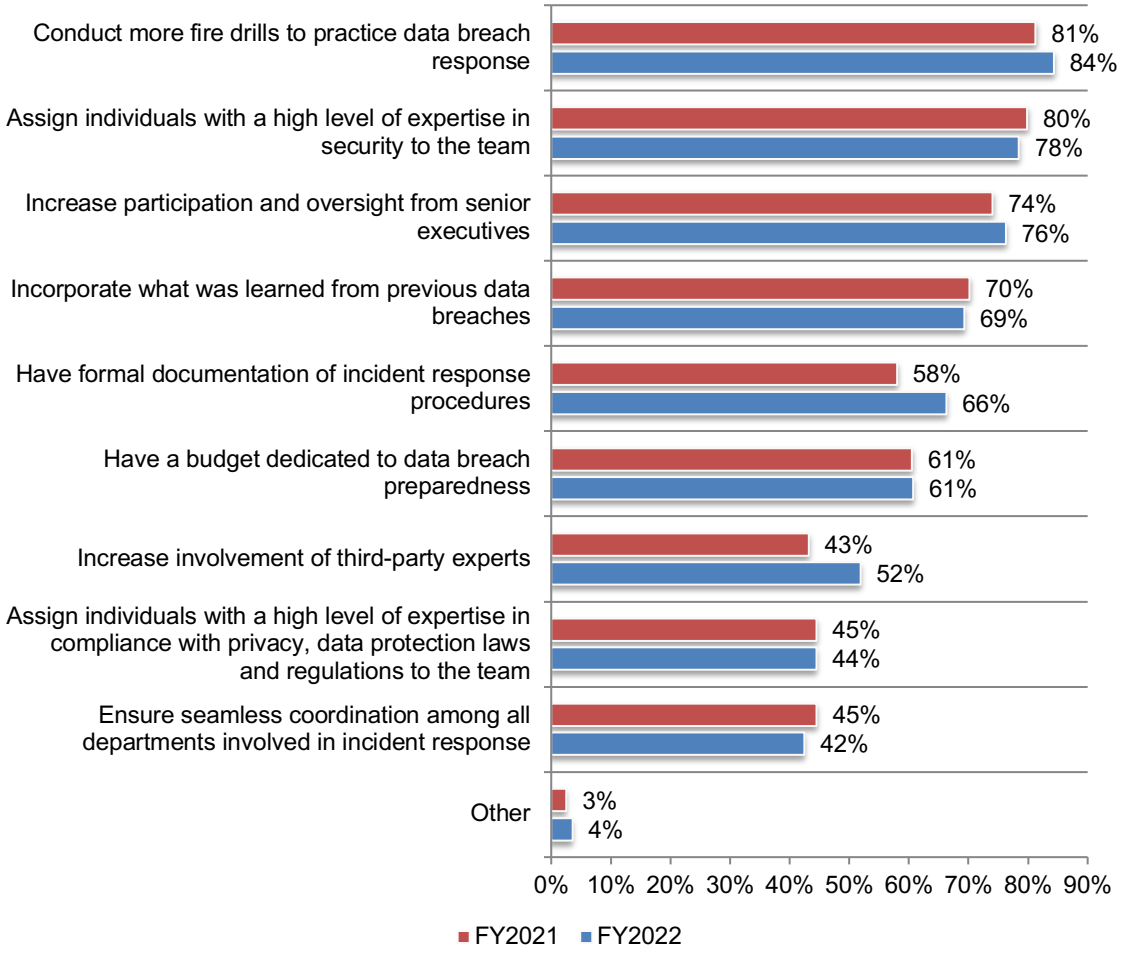
Figure 16. Does your data breach response plan include how to manage an international incident?



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 17, conducting more drills to practice data breach response increased from 81 percent of respondents in 2021 to 84 percent of respondents in this year's research.

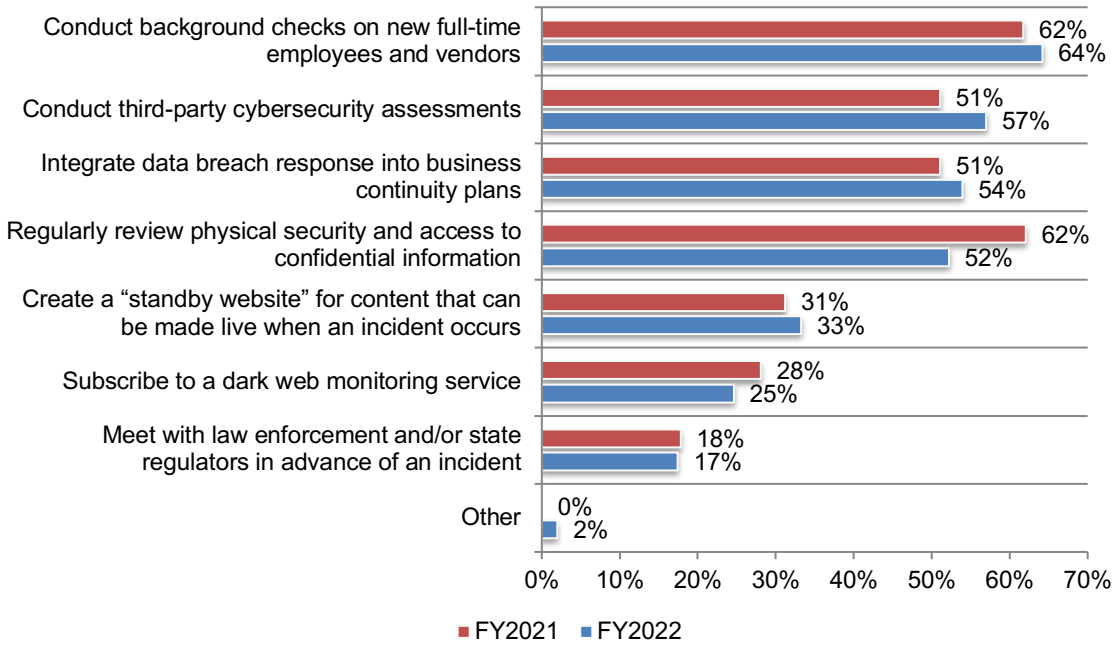
It is interesting that it continues to be more important to assign individuals with a high level of security expertise (78 percent of respondents) than to assign individuals with expertise in compliance, privacy, data protection laws and regulations to the team (44 percent of respondents). There were also significant increases in having formal documentation of incident response procedures (from 58 percent to 66 percent of respondents) and an increase in the involvement of third-party experts (from 43 percent to 52 percent of respondents).

Figure 17. How could your data breach response plan become more effective?
More than one response permitted



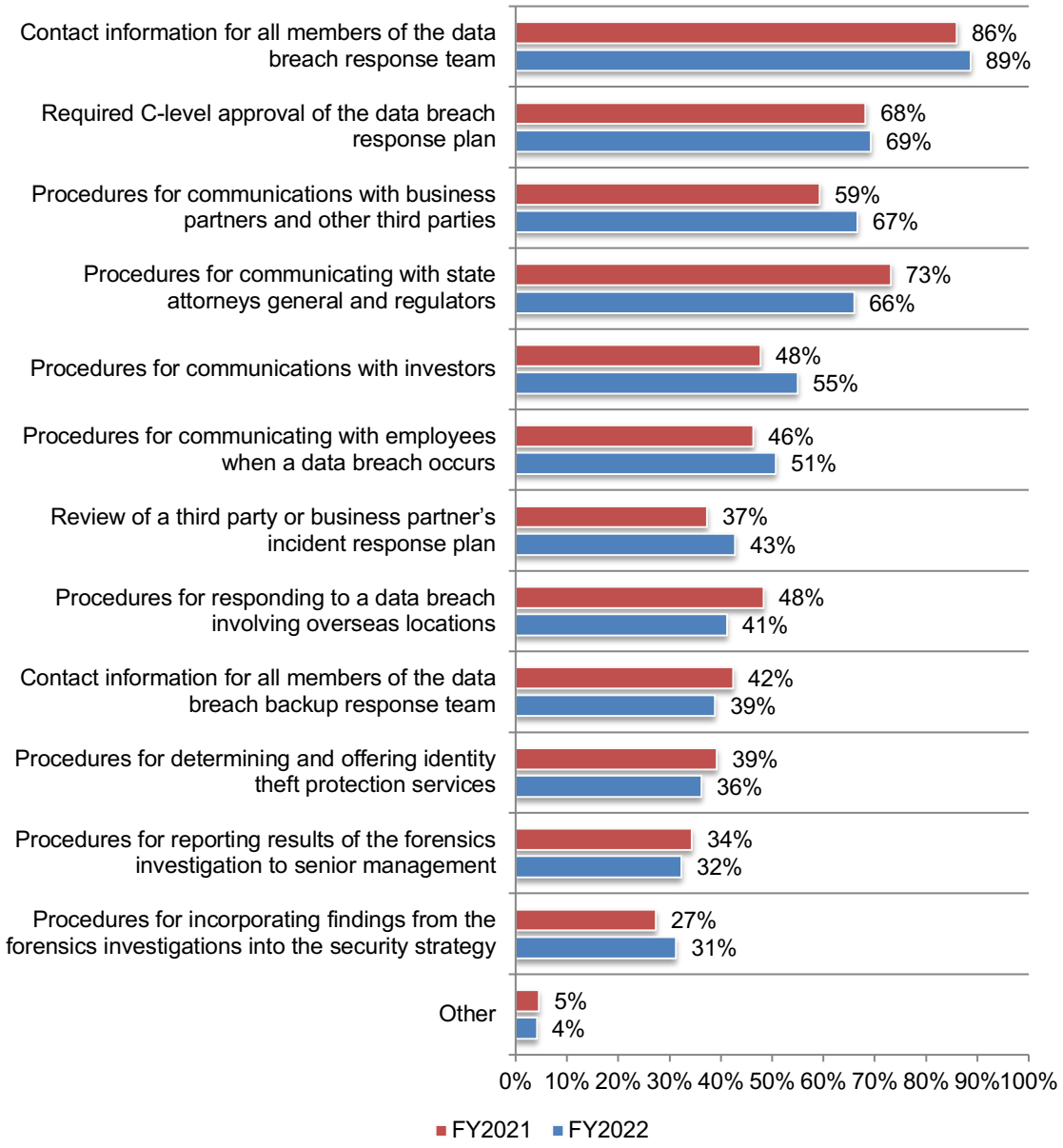
Background checks and security assessments are the top two steps to prepare for a data breach. According to Figure 18, the primary steps being taken to prepare for a data breach are background checks on new full-time employees (64 percent of respondents) and third-party cybersecurity assessments (57 percent of respondents). Reviews of physical security and access to confidential information has declined from 62 percent of respondents to 52 percent of respondents.

Figure 18. Does your organization's plan include any of the following steps?
More than one response permitted



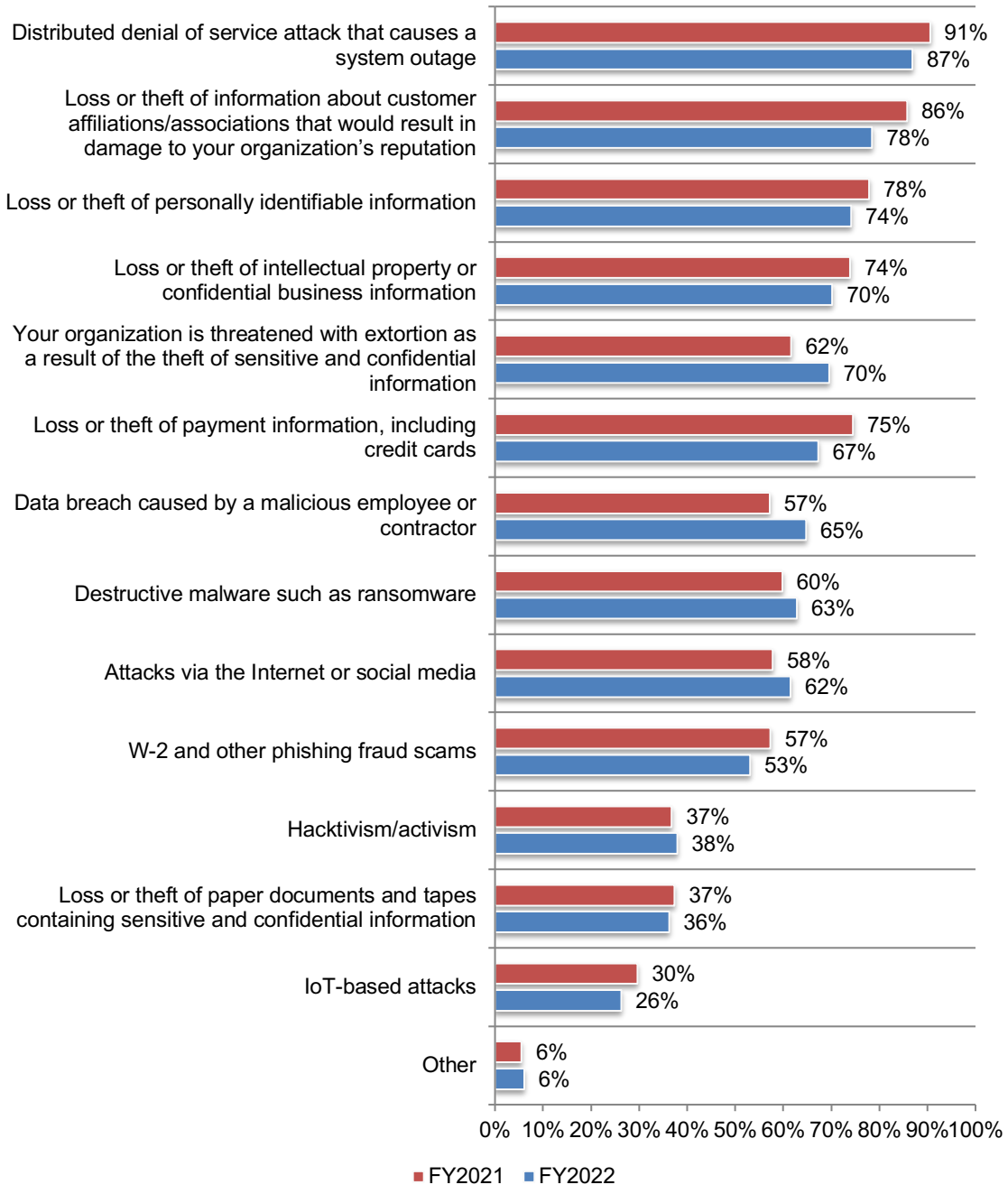
When a data breach occurs, communication with various stakeholders is critical. As shown in Figure 19, contact information for all members of the data breach response plan (89 percent of respondents), procedures for communications with business partners and third parties (67 percent of respondents), communications with state attorneys general (66 percent of respondents), communication with investors (55 percent of respondents) and communication with employees (51 percent of respondents) are the top requirements for a data breach response plan. Sixty-nine percent of respondents say C-level approval of the data breach response plan is required.

Figure 19. Does your data breach response plan include the following requirements?
More than one response permitted



Ransomware attacks are on the rise and more organizations' response plans offer guidance on how to deal with extortion. According to Figure 20, 70 percent of respondents say the plan provides guidance on dealing with extortion when sensitive and confidential information is stolen. Managing a distributed denial of service attack (DDoS) that causes a system outage continues to be number one guidance offered.

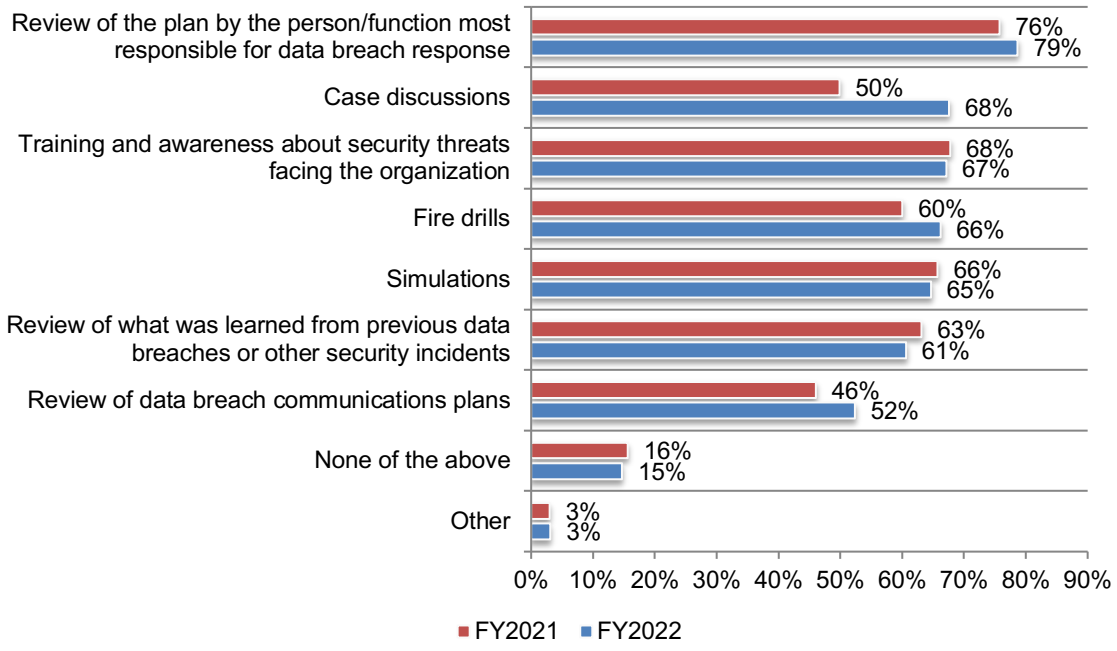
Figure 20. Does your data breach response plan offer guidance on managing the following security incidents?
More than one response permitted



Organizations are increasingly using case discussions to prepare for a data breach. Sixty-nine percent of respondents say they practice data breach response at least twice a year (49 percent), annually (13 percent) or every two years (7 percent). Nineteen percent of respondents say they never practice (2 percent) or there is no set schedule (17 percent).

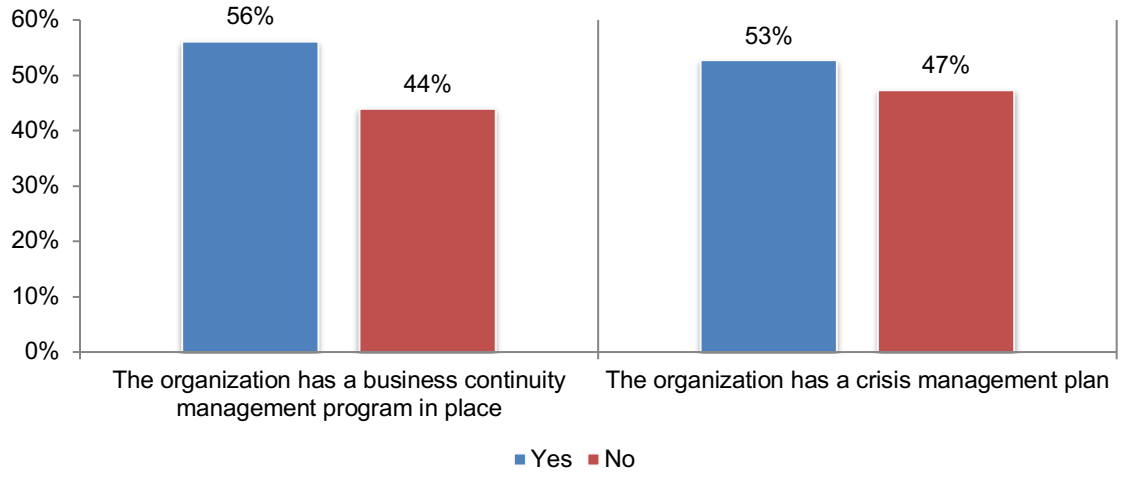
According to Figure 22, 68 percent of respondents say their organizations incorporate case discussions into their data breach planning, a significant increase from 50 percent of respondents in 2021. Review by the person/function most responsible for data breach response (79 percent of respondents) and training and awareness about security threats facing the organization (67 percent of respondents) are used to prepare for a data breach.

Figure 22. What steps are included in practicing data breach response plans?
More than one response permitted



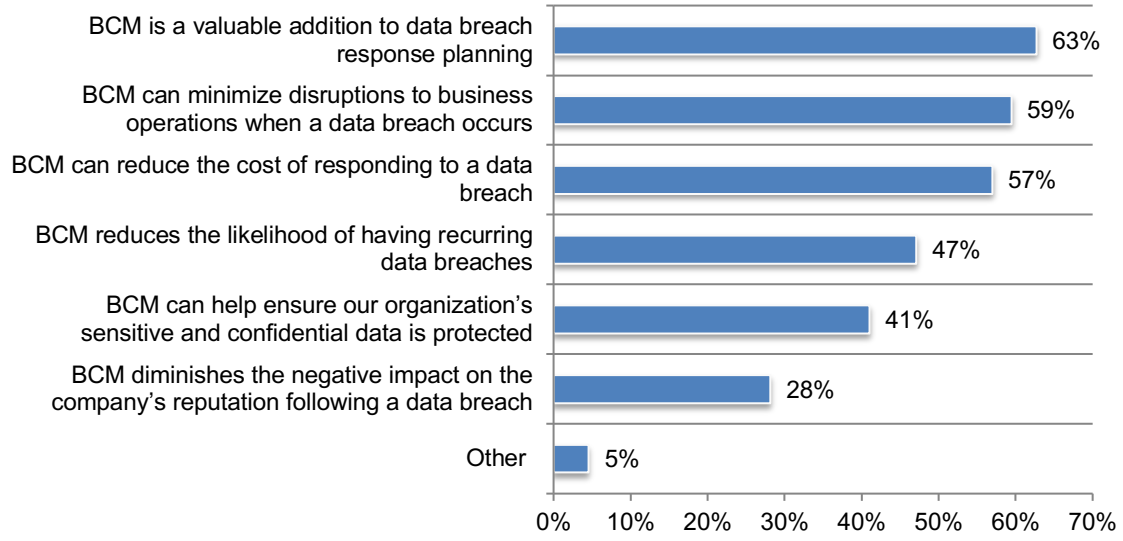
To improve the effectiveness of dealing with an incident, organizations are incorporating business continuity management (BCM) and crisis management plans in their data breach response efforts. As shown in Figure 23, 56 percent of respondents say their organizations have a BCM plan and 53 percent of respondents say their organizations have a crisis management plan.

Figure 23. Does your organization have BCM and crisis management plans?



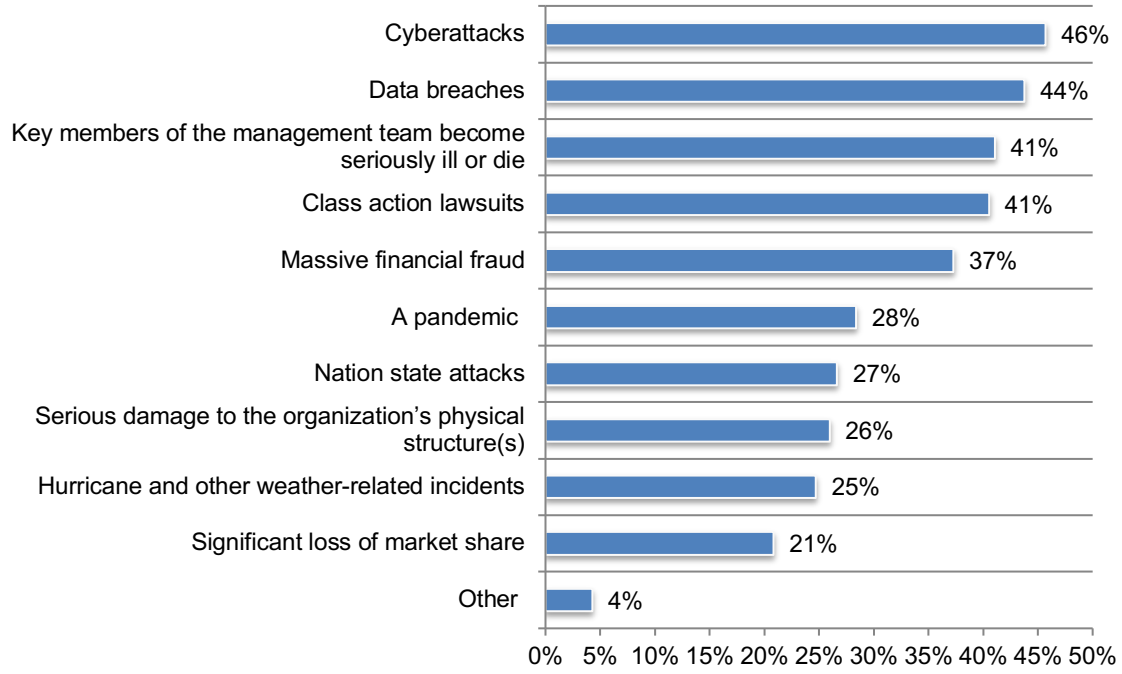
BCM increases the ability of an organization to meet its commitments to key stakeholders if it has a data breach. BCM plans involve systems to prevent and respond to a data breach. In addition to prevention and response, the goal is to enable ongoing operations before and during the resolution of the data breach. As shown in Figure 24, 63 percent of respondents say BCM is a valuable addition to data breach response planning and 59 percent of respondents say BCM minimizes disruptions to business operations when a data breach occurs.

Figure 24. What are the reasons for having a BCM plan?
Three responses permitted



Crisis management plans have proven to be effective. The purpose of a crisis management plan is to provide guidance on how organizations should respond in a crisis such as a data breach and how to reduce the long-term damage. Figure 25 presents what these plans include. Number one is a cyberattack (46 percent of respondents) followed by data breaches (44 percent of respondents). Fifty-nine percent of respondents say their organization had a crisis that necessitated the use of its crisis management plan and 61 percent of these respondents say that the plan was very or highly effective in helping to deal with the crisis.

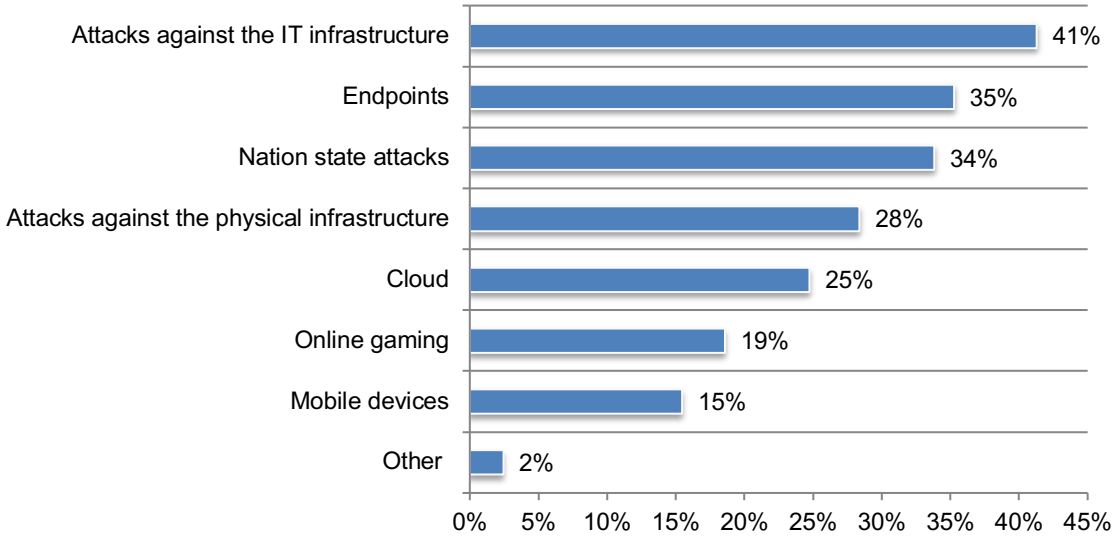
Figure 25. What does the crisis management plan cover?
More than one response permitted



The rising threats against organizations

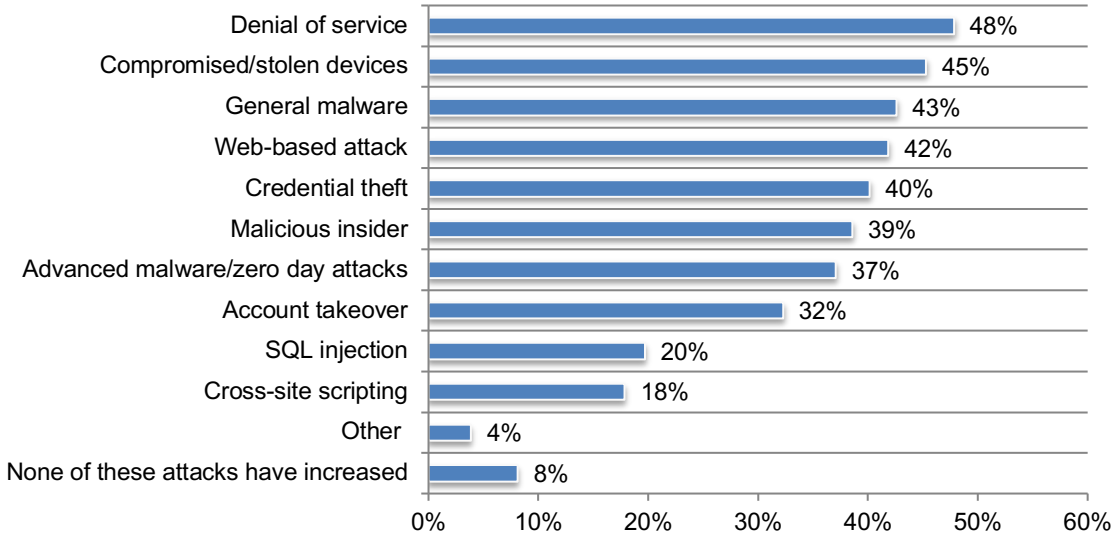
The IT infrastructure is vulnerable to attacks. As shown in Figure 26, organizations are most concerned about attacks against the IT infrastructure (41 percent of respondents) and the endpoints (35 percent of respondents).

Figure 26. What threat vectors is your organization most concerned about?
Two responses permitted



Denial of service, stolen devices and general malware have increased in the past year. According to Figure 27, almost half (48 percent) of respondents say denial of service attacks have increased followed by compromised or stolen devices (45 percent of respondents).

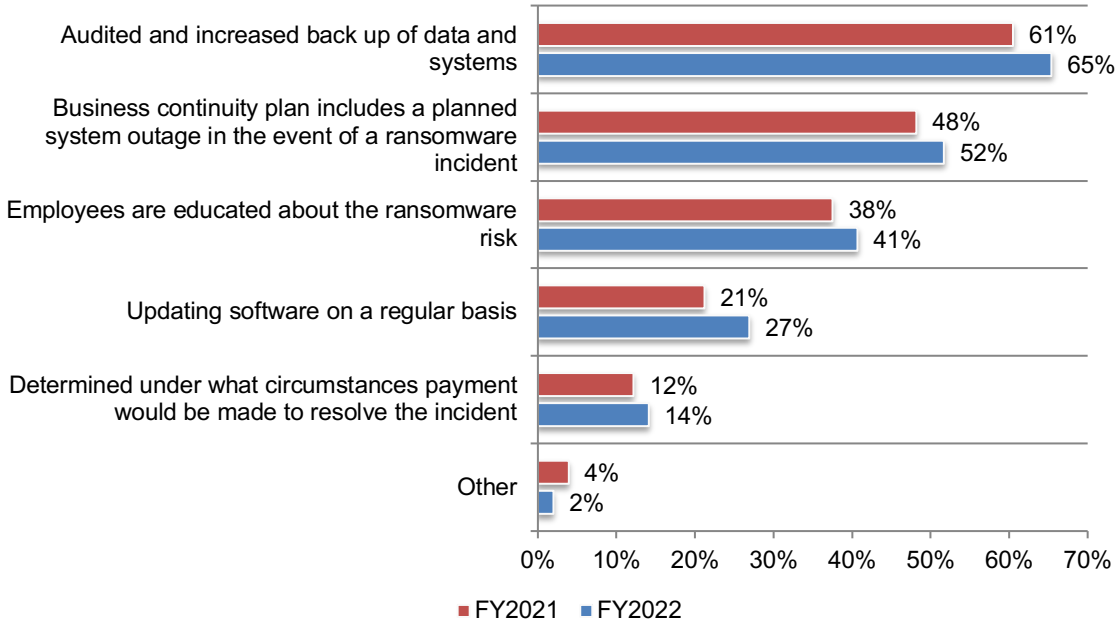
Figure 27. In the past 12 months, have any of the following attacks increased?
More than one response permitted



The majority of organizations experience spear phishing and ransomware attacks Sixty-nine percent of respondents say their organizations experienced one or more spear phishing attacks that were very significant (25 percent) or significant (49 percent).

Forty-seven percent of respondents say their organization had a ransomware attack and the average ransom paid was $551,065. Fifty-three percent of respondents paid the ransom, a decrease from 62 percent in 2021. According to Figure 28, to prepare for a ransomware attack 65 percent of respondents say 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 (52 percent of respondents).

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



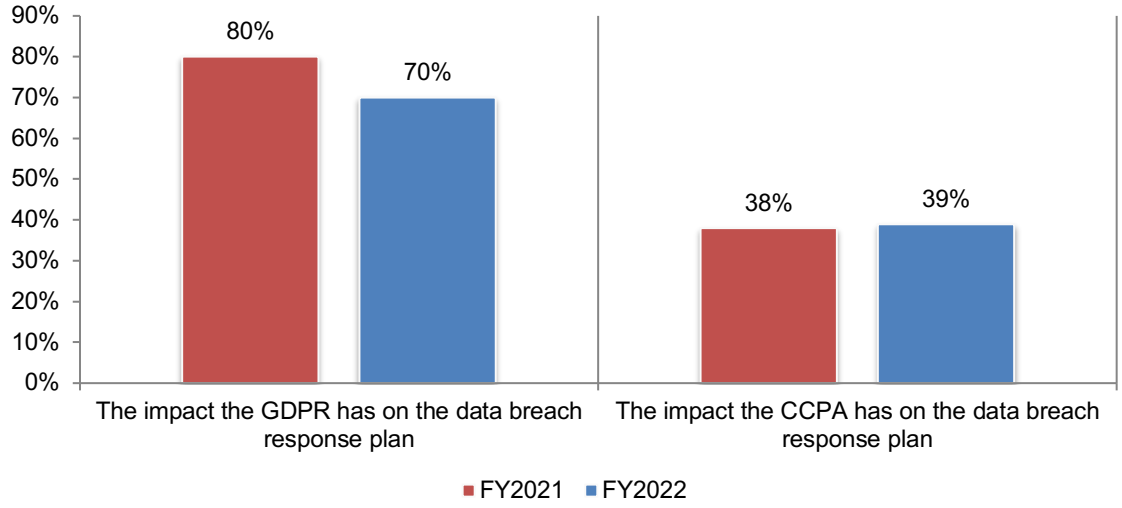
Regulations and data breach preparedness

Virtually all organizations represented in this study are subject to GDPR. Eighty 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 as discussed previously.

Respondents were asked to rate the impact of the GDPR and the California Consumer Privacy Act (CCPA) on data breach preparedness on a scale of 1 = no impact to 10 = high impact. As shown in Figure 29, 70 percent of respondents say GDPR has a significant impact on data breach preparedness. In contrast, only 39 percent of respondents say the CCPA has a significant impact.

According to respondents, an average of 7 data breaches were required to be reported to the regulators in the past 2 years. However, an average of 5 data breaches were actually reported to the regulator.

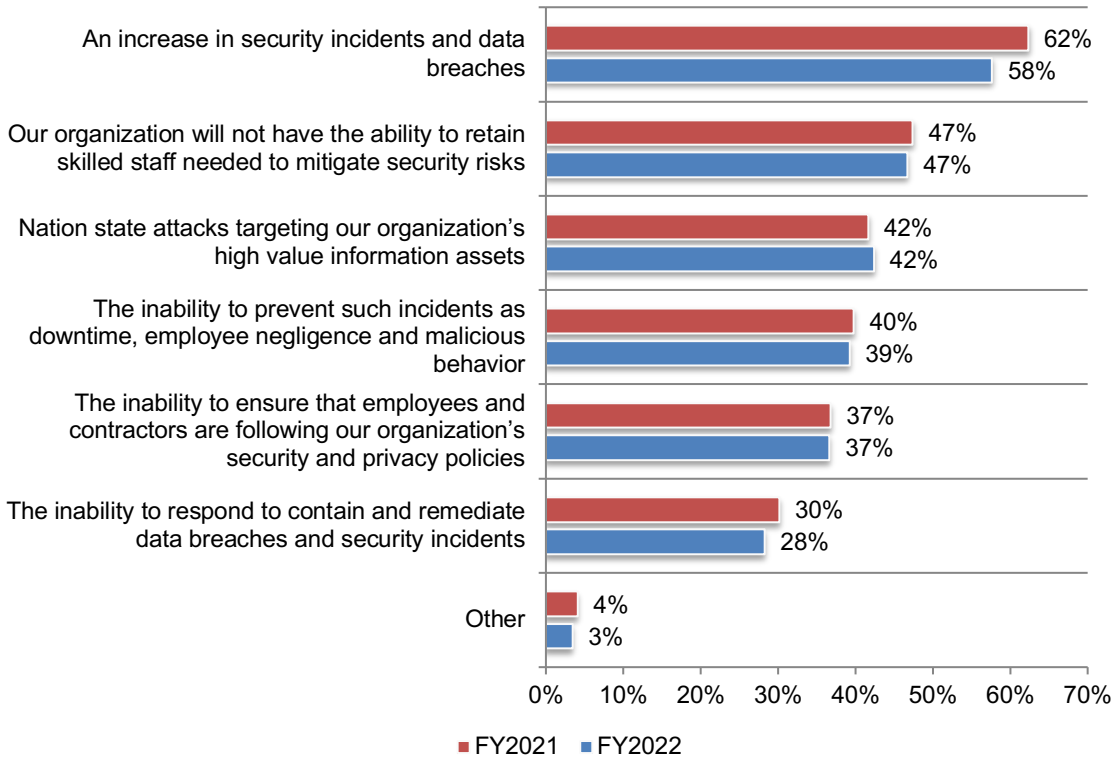
Figure 29. Regulations organizations are subject to and impact data breach preparedness
On a scale from 1 = No impact to 10 = high impact, 7+ responses presented



Perceptions about the future

Security incidents and data breaches are expected to increase. As shown in Figure 30, 58 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 30. What concerns your organization the most?
More than one response permitted

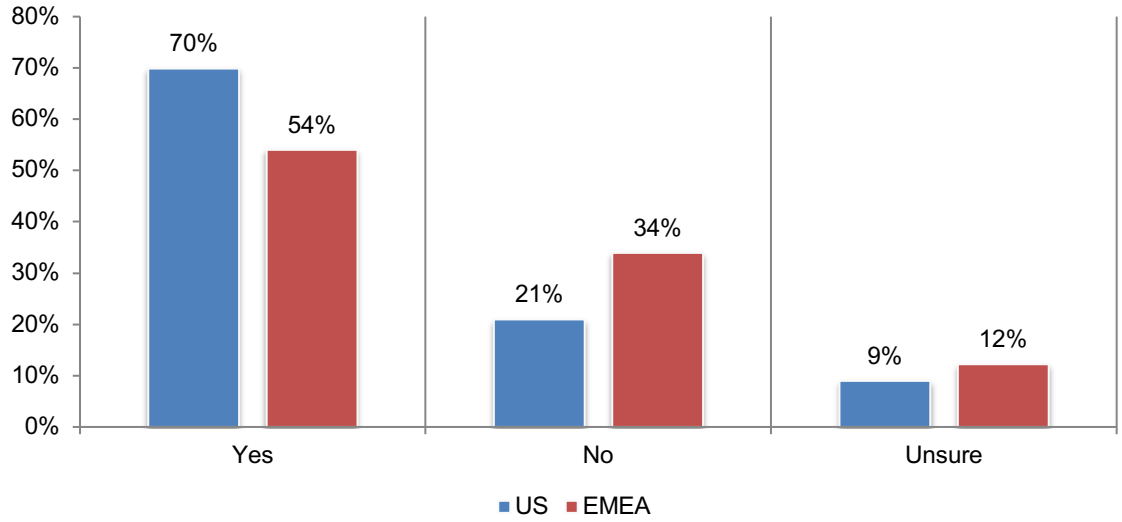


US and EMEA differences

In this section, we compare the US (605 respondents) and the EMEA (465 respondents) survey results.

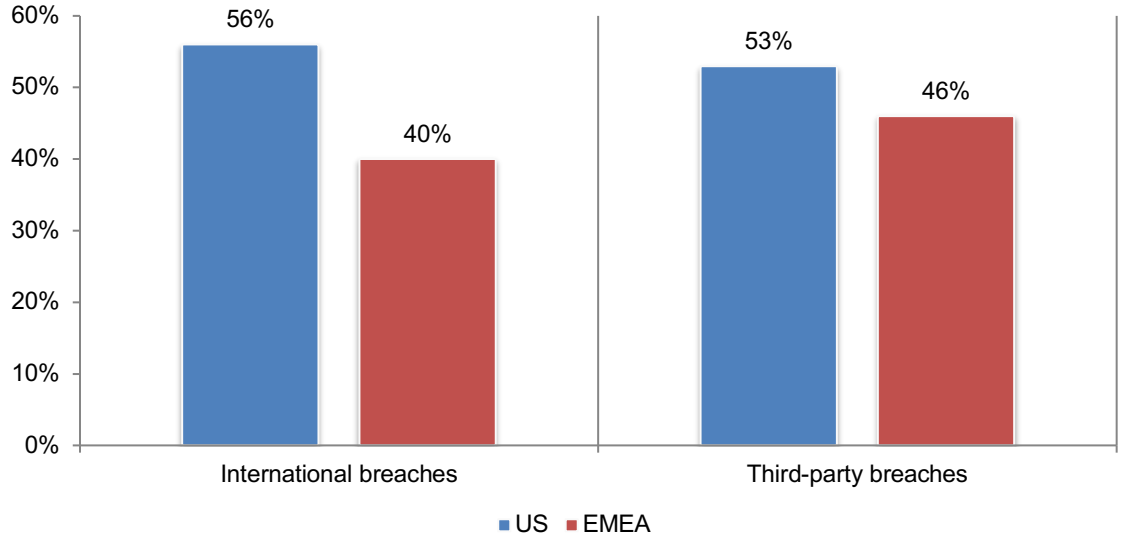
US organizations were more likely to have had a data breach in the past 2 years. As shown in Figure 31, 70 percent of respondents in the US say their organization had a data breach while only slightly more than half (54 percent) of respondents in the EMEA reported having a data breach.

Figure 31. Did your organization have a data breach in the past 2 years?



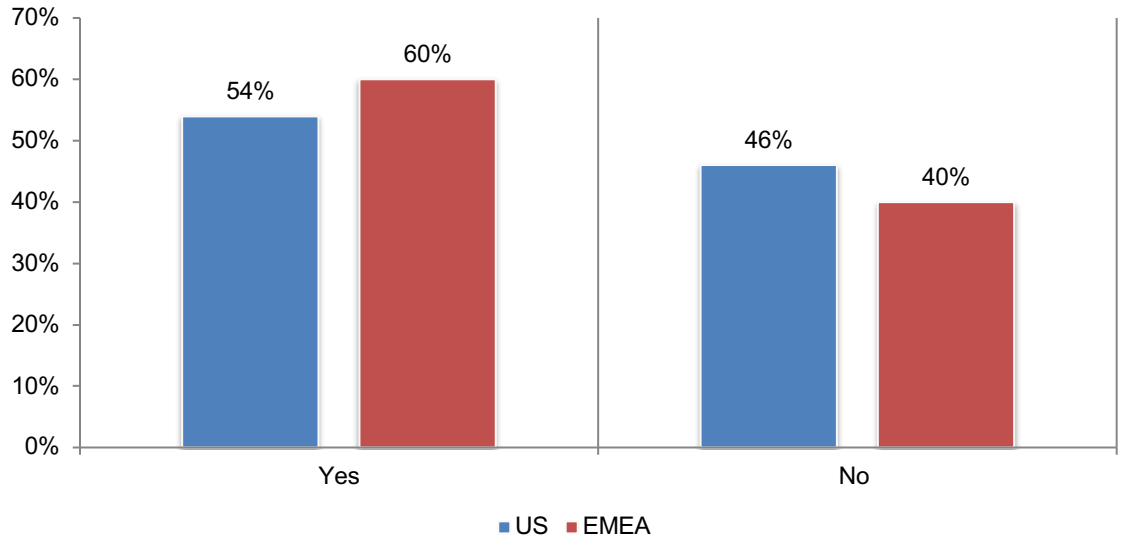
US organizations were more likely to have both international and third-party data breaches. Fifty-six percent of US respondents and 40 percent of EMEA respondents had a global data breach. Similarly, 53 percent of US organizations and 46 percent of EMEA respondents had a data breach caused by a third party.

Figure 32. Were these breaches international in scope and were they the result of a third party in your organization's supply chain?
Yes responses presented



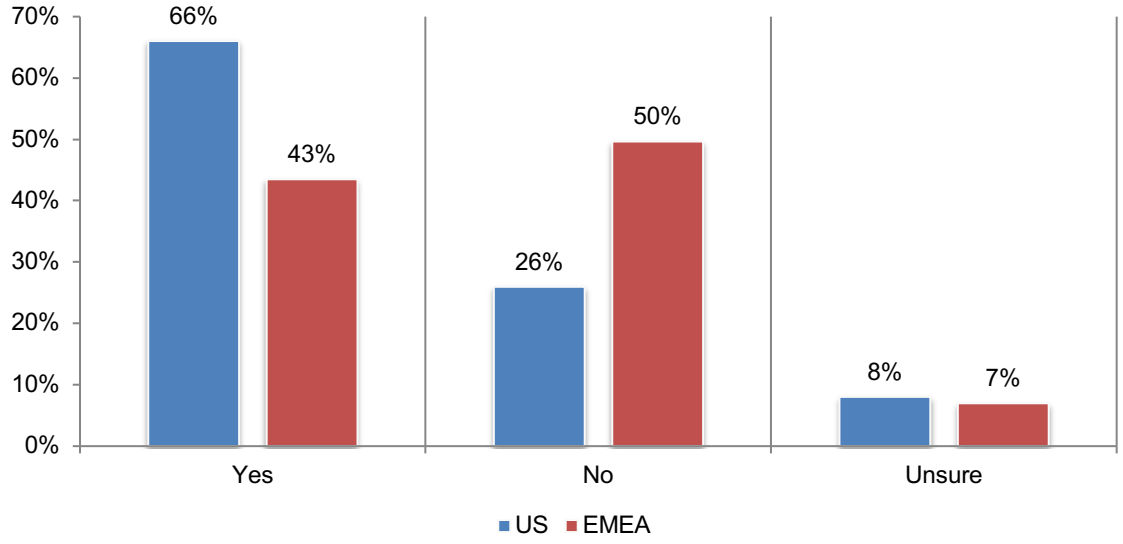
EMEA respondents are more likely to believe their boards of director and senior management are engaged in plans to deal with a possible data breach. As shown in Figure 33, 60 percent of EMEA respondents vs. 54 percent of US respondents say their boards and C-suite executives are knowledgeable about plans to respond to a data breach.

Figure 33. Do you believe your organization's board of directors and C-suite executives are knowledgeable about plans to deal with a possible data breach?



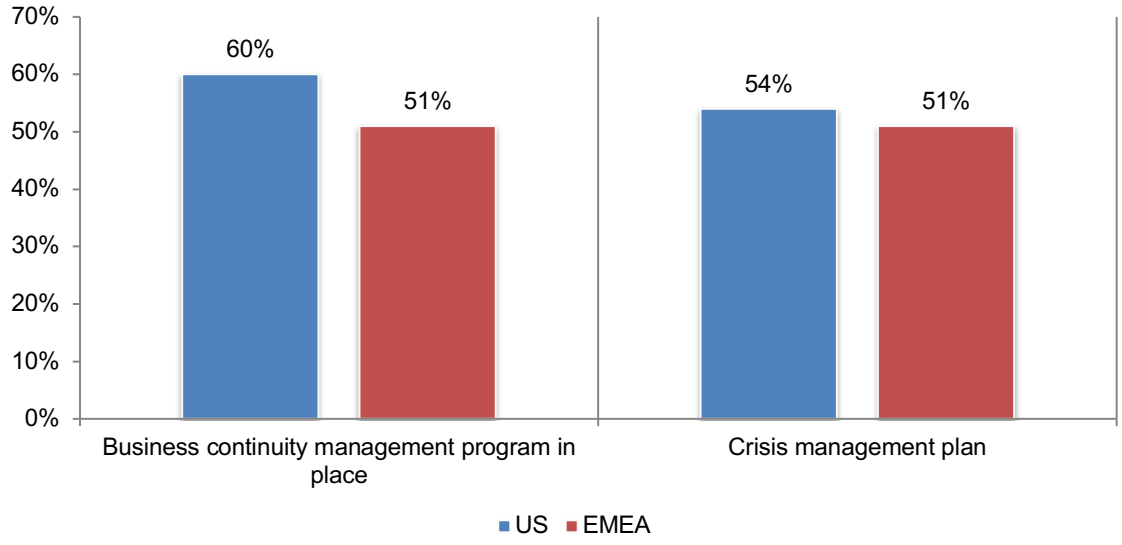
US organizations are more likely to include procedures for managing a global data breach. According to Figure 34, 66 percent of US respondents say they have a formal plan to deal with an international data breach.

Figure 34. Does your data breach response plan include how to manage an international data breach?



US organizations are more likely to have BCM and crisis management plans in place as shown in Figure 35. In addition to including steps to respond to an international data breach, more US organizations have BCM and crisis management plans (60 percent and 54 percent of respondents, respectively).

Figure 35. Does your organization have a BCM and crisis management plan?
Yes responses presented



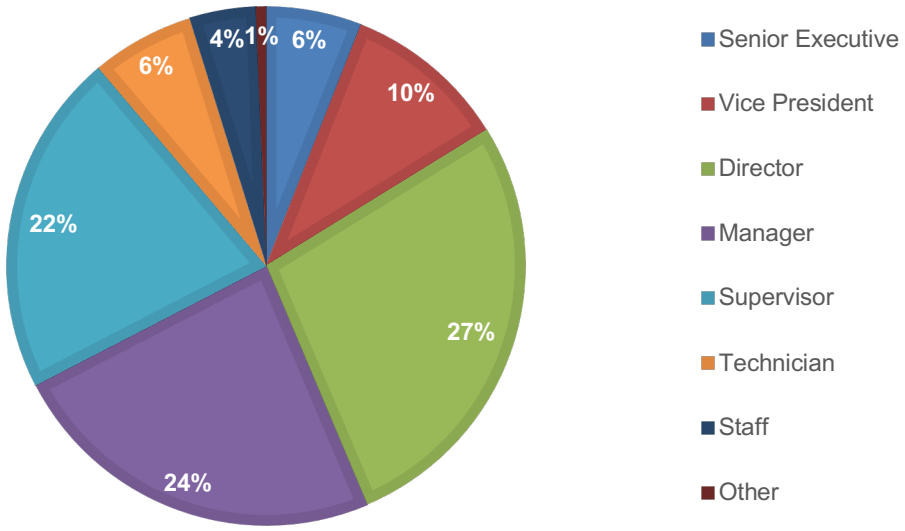
Part 3. Methods

A sampling frame of 15,251 US and 12,880 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 670 total US survey returns and 512 EMEA survey returns. Screening and reliability checks required the removal of 65 US surveys and 47 EMEA surveys. Our final sample consisted of 605 US surveys (a 4.0 percent response rate) and 465 EMEA surveys (a 3.6 percent response rate).

Table 1. Sample response	US	EMEA	Combined
Sampling frame	15,251	12,880	28,131
Total returns	670	512	1182
Rejected or screened surveys	65	47	112
Final sample	605	465	1,070
Response rate	4.0%	3.6%	3.8%

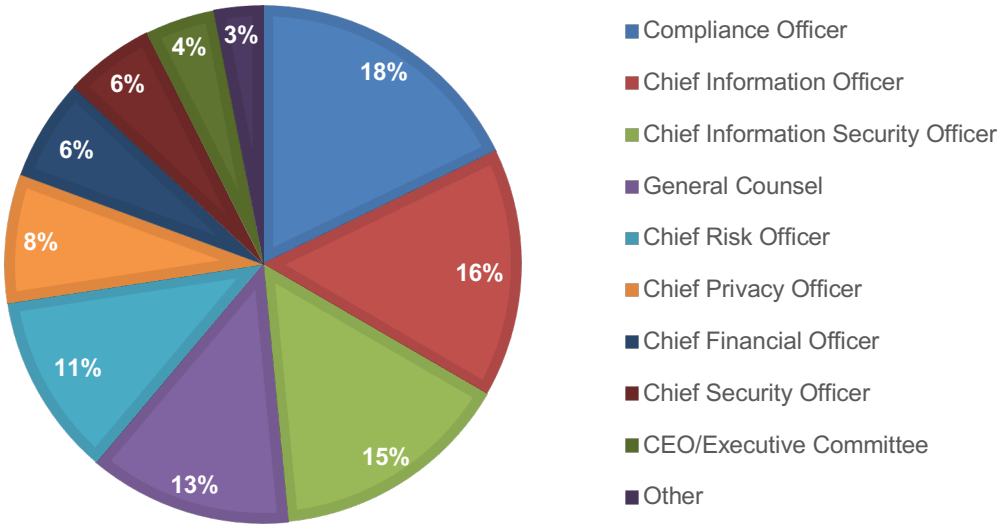
Pie Chart 1 reports the respondent's organizational level within participating organizations. By design, most respondents (89 percent) are at or above the supervisory levels. The largest segment at 27 percent of respondents is the director position.

Pie Chart 1. Current position within the organization
n=1,070



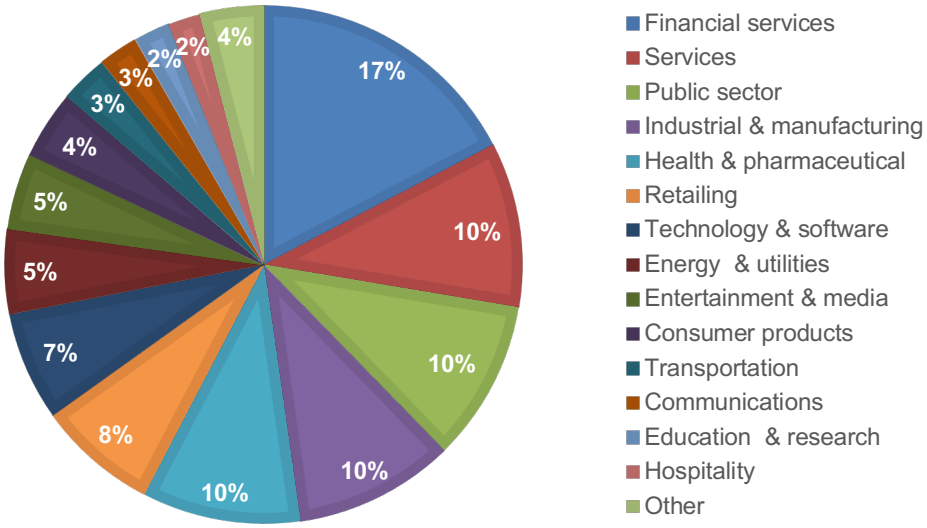
Pie Chart 2 reveals that 18 percent of respondents report to the compliance officer, 16 percent of respondents report to the chief information officer, 15 percent of respondents report to the chief information security officer, 13 percent of respondents report to the general counsel and 11 percent of respondents report to the chief risk officer.

Pie Chart 2. Primary person respondent reports to within the organization
n=1,070



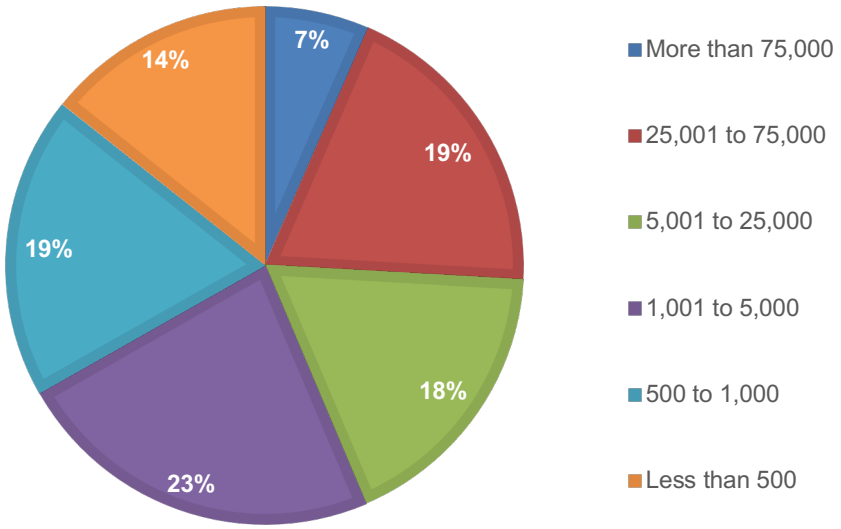
Pie Chart 3 reports the industry classification of respondents' organizations. The largest industry classification is financial services (17 percent of respondents), which includes banking, investment management, insurance, brokerage, payments and credit cards. This is followed by services (10 percent of respondents), public sector (10 percent of respondents), industrial and manufacturing (10 percent of respondents), and health and pharmaceuticals (10 percent of respondents).

Pie Chart 3. Primary industry focus
n=1,070



As shown in Pie Chart 4, 67 percent of respondents are from organizations with a global headcount of more than 1,000 employees.

Pie Chart 4. Global employee headcount
n=1,070



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 December 2021.

Survey response	FY2022	US	EMEA
Sampling frame	28,131	15,251	12,880
Total returns	1182	670	512
Rejected or screened surveys	112	65	47
Final sample	1070	605	465
Response rate	3.8%	4.0%	3.6%

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?	FY2022	US	EMEA
Yes	63%	70%	54%
No	27%	21%	34%
Unsure	10%	9%	12%
Total	100%	100%	100%

Q2. How frequently did these incidents occur during the past 2 years?	FY2022	US	EMEA
Only once	38%	35%	41%
2 to 3 times	28%	32%	23%
4 to 5 times	23%	18%	29%
More than 5 times	11%	15%	6%
Total	100%	100%	100%

Q3. Were any of these breaches international or global in scope?	FY2022	US	EMEA
Yes	49%	56%	40%
No	46%	41%	53%
Unsure	5%	3%	7%
Total	100%	100%	100%

Q4. Were any of these breaches the result of a third party in your organization's supply chain?	FY2022	US	EMEA
Yes	50%	53%	46%
No	42%	39%	45%
Unsure	8%	8%	9%
Total	100%	100%	100%

Q5. My organization is prepared to respond to a data breach caused by a remote workforce.	FY2022	US	EMEA
Strongly agree	17%	14%	20%
Agree	21%	21%	20%
Unsure	23%	22%	24%
Disagree	26%	28%	23%
Strongly disagree	14%	15%	13%
Total	100%	100%	100%

Q6. The risk of spear-phishing and ransomware attacks has increased in the past year.	FY2022	US	EMEA
Strongly agree	33%	35%	31%
Agree	29%	30%	27%
Unsure	13%	12%	14%
Disagree	17%	16%	19%
Strongly disagree	8%	7%	9%
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.	FY2022	US	EMEA
Strongly agree	25%	24%	27%
Agree	34%	38%	29%
Unsure	18%	17%	21%
Disagree	13%	12%	13%
Strongly disagree	10%	9%	12%
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?	FY2022	US	EMEA
1 year	24%	27%	21%
2 to 3 years	25%	28%	20%
4 to 7 years	15%	11%	19%
8 to 10 years	6%	7%	4%
More than 10 years	4%	4%	5%
Our organization does not provide identity theft protection	26%	22%	29%
Total	100%	100%	100%
Extrapolated value	3.14	2.81	2.77

Part 2. Data breach preparedness

Q9. What best describes the maturity of your organization's privacy and data protection program?	FY2022	US	EMEA
Early stage – many privacy and data protection program activities have not 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.	16%	13%	20%
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.	27%	29%	25%
Late-middle stage – most privacy and data protection program activities are deployed across the enterprise. The program has C-level support and adequate budget.	31%	31%	32%
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.	25%	27%	23%
Total	100%	100%	100%

Q10a. Do you believe your company's board of directors and C-suite executives are knowledgeable about plans to deal with a possible data breach?	FY2022	US	EMEA
Yes	57%	54%	60%
No	43%	46%	40%
Total	100%	100%	100%

Q10b. If yes, why do you believe your company's board of directors and C-suite executives are knowledgeable? Please select all that apply.	FY2022	US	EMEA
They regularly participate in detailed reviews of our data breach response plan	41%	43%	38%
They understand the specific security threats facing our organization	43%	46%	39%
They provide detailed feedback about the data breach response plan	33%	35%	31%
They assume responsibility for the successful execution of the incident response plan	40%	37%	43%
They have requested to be notified ASAP if a material data breach occurs	42%	39%	45%
They participate in a high-level review of the organization's data protection and privacy practices	56%	54%	59%
Other	2%	5%	4%
Total	257%	259%	259%

Q11. What types of data loss is your organization most concerned about? Please select the top two.	FY2022	US	EMEA
Loss or theft of customer information	58%	60%	55%
Loss or theft of employee personal data	35%	32%	40%
Loss or theft of medical data	10%	11%	9%
Loss or theft of consumer data	23%	21%	26%
Loss or theft of intellectual property	60%	64%	54%
Loss or theft of payment card data	11%	10%	12%
Other	3%	2%	4%
Total	200%	200%	200%

Q12. What are the two biggest barriers to improving the ability of IT security to respond to a data breach? Please select the top three	FY2022	US	EMEA
Lack of investment in much needed technologies	17%	17%	16%
Lack of expertise	40%	36%	46%
Lack of C-suite support	10%	9%	12%
Lack of security processes for third parties that have access to our data	35%	36%	33%
Lack of visibility into end-user access of sensitive and confidential information	66%	64%	69%
Lack of understanding of unsecured IoT devices	38%	35%	41%
Proliferation of mobile devices	33%	35%	29%
Proliferation of cloud services	58%	62%	53%
Other	3%	5%	1%
Total	300%	300%	300%

Part 3. Rising threats against organizations

Q13. What threat vectors is your organization most concerned about? Please select the top two.	FY2022	US	EMEA
Nation state attacks	34%	36%	31%
Attacks against the physical infrastructure	28%	31%	25%
Attacks against the IT infrastructure	41%	40%	43%
Online gaming	19%	19%	18%
Endpoints	35%	37%	33%
Cloud	25%	23%	27%
Mobile devices	15%	12%	20%
Other	2%	2%	3%
Total	200%	200%	200%

Q14. In the past 12 months, have any of the following attacks **increased**? Please select all that apply.	FY2022	US	EMEA
Account takeover	32%	34%	30%
Advanced malware / zero-day attacks	37%	41%	32%
Compromised / stolen devices	45%	44%	47%
Credential theft	40%	41%	39%
Cross-site scripting	18%	17%	19%
Denial of service	48%	50%	45%
General malware	43%	40%	46%
Malicious insider	39%	39%	38%
SQL injection	20%	21%	18%
Web-based attack	42%	41%	43%
Other (please specify)	4%	3%	5%
None of these attacks have increased	8%	9%	7%
Total	375%	380%	369%

Q15a. In the past 12 months, did your organization experience one or more spear phishing attacks?	FY2022	US	EMEA
Yes	69%	75%	61%
No	31%	25%	39%
Total	100%	100%	100%

Q15b. If yes, how significant were the negative consequences of the spear phishing attacks?	FY2022	US	EMEA
Very significant	25%	29%	21%
Significant	49%	48%	49%
Not significant	17%	14%	22%
Minimal	9%	9%	8%
Total	100%	100%	100%

Q16a. Did your organization **ever** experience a ransomware attack?	FY2022	US	EMEA
Yes	47%	48%	45%
No	48%	45%	52%
Unsure	5%	7%	3%
Total	100%	100%	100%

Q16b. If yes, how much was the ransom? If your organization has had more than one ransomware attack, please select the costliest ransom.	FY2022	US	EMEA
Less than $10,000	4%	3%	6%
$10,000 to $25,000	7%	6%	9%
$25,001 to $50,000	13%	10%	16%
$50,001 to $75,000	15%	12%	18%
$75,001 to $100,000	18%	17%	20%
$100,001 to $250,000	13%	16%	10%
$250,001 to $500,000	13%	15%	11%
$500,001 to $1,00,000	10%	11%	8%
$1,00,001 to $5,000,000	4%	5%	2%
$5,00,001 to $10,000,000	2%	3%	0%
More than $10,000,000	1%	2%	0%
Total	100%	100%	100%
Extrapolated value	$551,065	$809,075	$215,375

Q16c. Did your company pay the ransom?	FY2022	US	EMEA
Yes	53%	56%	48%
No	47%	44%	52%
Total	100%	100%	100%

Q17. Have you taken the following steps to prepare for a ransomware incident? Please select all that apply.	FY2022	US	EMEA
Determined under what circumstances payment would be made to resolve the incident	14%	17%	10%
Audited and increased back up of data and systems	65%	67%	63%
Business continuity plan includes a planned system outage in the event of a ransomware incident	52%	54%	49%
Employees are educated about the ransomware risk	41%	42%	39%
Updating software on a regular basis	27%	30%	23%
Other	2%	3%	3%
Total	201%	213%	187%

Q18a. 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?	FY2022	US	EMEA
Yes	73%	77%	67%
No	27%	23%	33%
Total	100%	100%	100%

Q18b. If yes, how often is training conducted?	FY2022	US	EMEA
On-boarding new employees	54%	57%	49%
Every six months	4%	3%	5%
Annually	21%	20%	23%
Sporadically	20%	20%	21%
Unsure	1%	0%	2%
Total	100%	100%	100%

Part 4. Cyber insurance coverage

Q19. Does your organization have a data breach or cyber insurance policy?	FY2022	US	EMEA
Yes	53%	59%	45%
No	47%	41%	55%
Total	100%	100%	100%

Q20. If your organization **does not** have a cyber insurance policy, does it plan to purchase a data breach or cyber insurance policy?	FY2022	US	EMEA
Yes, within the next six months	28%	33%	21%
Yes, within the next year	34%	31%	38%
Yes, within the next two years	9%	9%	10%
No plans to purchase	28%	25%	31%
Unsure	1%	2%	0%
Total	100%	100%	100%

Q21. What types of incidents does your organization's cyber insurance cover? Please select all that apply.	FY2022	US	EMEA
External attacks by cyber criminals	83%	91%	72%
Malicious or criminal insiders	50%	55%	44%
System or business process failures	29%	25%	33%
Human error, mistakes and negligence	41%	43%	39%
Incidents affecting business partners, vendors or other third parties that have access to your company's information assets	63%	58%	68%
Ransomware attacks	54%	54%	53%
Major security vulnerability in a product, website or service	61%	58%	64%
Other	5%	6%	5%
Unsure	2%	3%	1%
Total	387%	394%	379%

Q22. What coverage does this insurance offer your company? Please select all that apply.	FY2022	US	EMEA
Identity protection services to victims	76%	92%	55%
Call center support	49%	55%	42%
Forensics and investigative costs	74%	80%	66%
Notification costs to data breach victims	58%	59%	57%
Communication costs to regulators	15%	17%	13%
Employee productivity losses	9%	9%	9%
Replacement of lost or damaged equipment	43%	51%	31%
Revenue losses	21%	23%	18%
Legal defense costs	66%	74%	56%
Regulatory penalties and fines	29%	29%	28%
Third-party liability	63%	66%	59%
Brand damages	6%	8%	3%
IoT enabled device protection	19%	22%	16%
Other	7%	8%	6%
Total	535%	592%	461%

Part 5. Data breach response plan

Q23. What steps do you take to minimize the consequences of a data breach involving a business partner or other third party? Please select all that apply.	FY2022	US	EMEA
Require they have an incident response plan your organization can review	81%	85%	75%
Require they notify your organization when they have a data breach	86%	87%	84%
Require audits of their security procedures	56%	57%	55%
No steps being taken	7%	8%	5%
Total	229%	237%	219%

Q24a. Does your organization have a data breach response plan in place?	FY2022	US	EMEA
Yes	91%	95%	86%
No	9%	5%	14%
Total	100%	100%	100%

Q24b. If yes, has the data breach response plan added plans to respond to data breaches created by a remote workforce?	FY2022	US	EMEA
Yes	51%	57%	43%
No	49%	43%	57%
Total	100%	100%	100%

Q24c. If your organization **does not** have a data breach response plan in place, why?	FY2022	US	EMEA
No resources or budget	41%	41%	40%
Not important to have data breach response plan in place	11%	12%	9%
Lack of C-level support	18%	19%	16%
Outsourced to consultants	30%	28%	33%
Other	1%	0%	2%
Total	100%	100%	100%

Q25. How often does your company update the data breach response plan?	FY2022	US	EMEA
Each quarter	4%	5%	4%
Twice per year	5%	6%	4%
Once each year	26%	28%	24%
No set time period for reviewing and updating the plan	35%	32%	40%
We have not reviewed or updated since the plan was put in place	29%	30%	28%
Total	100%	100%	100%

Q26. 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.	FY2022	US	EMEA
Conduct third-party cybersecurity assessments	57%	61%	51%
Integrate data breach response into business continuity plans	54%	56%	51%
Create a “standby website” for content that can be made live when an incident occurs	33%	37%	29%
Regularly review physical security and access to confidential information	52%	58%	45%
Meet with law enforcement and/or state regulators in advance of an incident	17%	16%	19%
Subscribe to a dark web monitoring service	25%	25%	24%
Conduct background checks on new full-time employees and vendors	64%	69%	58%
Other	2%	0%	0%
Total	305%	322%	278%

Q27. Does your data breach response plan include the following requirements? Please select all that apply.	FY2022	US	EMEA
Required C-level approval of the data breach response plan	69%	71%	67%
Contact information for all members of the data breach response team	89%	91%	86%
Contact information for all members of the data breach backup response team	39%	44%	32%
Procedures for communicating with employees when a data breach occurs	51%	61%	37%
Procedures for responding to a data breach involving overseas locations	41%	35%	49%
Procedures for communicating with state attorneys general and regulators	66%	72%	58%
Procedures for communications with investors	55%	56%	53%
Procedures for communications with business partners and other third parties	67%	69%	64%
Review of a third party or business partner’s incident response plan	43%	40%	46%
Procedures for determining and offering identity theft protection services	36%	34%	39%
Procedures for reporting results of the forensics investigation to senior management	32%	30%	35%
Procedures for incorporating findings from the forensics investigations into the security strategy	31%	28%	36%
Other	4%	5%	3%
Total	623%	638%	604%

Q28. Does your data breach response plan offer guidance on managing the following security incidents? Please check all that apply.	FY2022	US	EMEA
Loss or theft of payment information, including credit cards	67%	72%	61%
Loss or theft of personally identifiable information	74%	74%	74%
Destructive malware such as ransomware	63%	60%	66%
IoT-based attacks	26%	25%	28%
Hacktivism/activism	38%	42%	32%
Attacks via the Internet or social media	62%	62%	61%
W-2 and other phishing fraud scams	53%	58%	47%
Distributed denial of service attack (DDoS) that causes a system outage	87%	96%	75%
Loss or theft of information about customer affiliations/associations that would result in damage to your organization's reputation	78%	76%	82%
Loss or theft of intellectual property or confidential business information	70%	68%	73%
Data breach caused by a malicious employee or contractor	65%	60%	71%
Your organization is threatened with extortion as a result of the theft of sensitive and confidential information	70%	71%	68%
Loss or theft of paper documents and tapes containing sensitive and confidential information	36%	32%	42%
Other	6%	7%	5%
Total	795%	802%	786%

Q29. How could your data breach response plan become more effective? Please select the top three choices.	FY2022	US	EMEA
Conduct more fire drills to practice data breach response	84%	95%	71%
Have formal documentation of incident response procedures	66%	76%	53%
Incorporate what was learned from previous data breaches	69%	70%	68%
Ensure seamless coordination among all departments involved in incident response	42%	42%	43%
Increase participation and oversight from senior executives	76%	85%	64%
Assign individuals with a high level of expertise in security to the team	78%	80%	77%
Assign individuals with a high level of expertise in compliance with privacy, data protection laws and regulations to the team	44%	49%	39%
Have a budget dedicated to data breach preparedness	61%	64%	57%
Increase involvement of third-party experts	52%	54%	50%
Other	4%	4%	3%
Total	578%	618%	525%

Q30a. Does your organization hire a third-party to manage your organization's data breach response plan?	FY2022	US	EMEA
Yes	61%	63%	58%
No	39%	37%	42%
Total	100%	100%	100%

Q30b. If yes, do you ask for recommendations to make a decision hiring a third-party? Please select all that apply.	FY2022	US	EMEA
Recommendations from our insurance company	51%	54%	48%
Recommendations from the general counsel	50%	52%	47%
Recommendations from other organizations	22%	24%	19%
Other	6%	6%	6%
We do not ask for recommendations	29%	34%	22%
Total	158%	170%	142%

Q30c. If yes, do you use any of the following criteria to select a third party? Please select all that apply.	FY2022	US	EMEA
Years of experience	57%	65%	47%
Client testimonials	30%	32%	28%
The services offered	56%	62%	49%
Trustworthiness of the third party	59%	62%	55%
Documented evidence of the third party's success in mitigating the consequences of the data breach	54%	57%	49%
Ability to respond to a data breach caused by the remote workforce	55%	60%	48%
Other	4%	3%	2%
Total	314%	341%	278%

Q31a. Does your organization practice data breach response?	FY2022	US	EMEA
At least twice a year	49%	51%	47%
Once each year	13%	16%	10%
Every two years	7%	7%	8%
More than two years	11%	8%	14%
Never	2%	2%	2%
No set schedule*	17%	16%	19%
Total	100%	100%	100%

*Not a response in FY2021

Q31b. If your organization practices data breach response, what is included in the practice response? Please check all that apply.	FY2022	US	EMEA
Fire drills	66%	71%	60%
Case discussions	68%	66%	69%
Simulations	65%	65%	64%
Training and awareness about security threats facing the organization	67%	58%	79%
Review of the plan by the person/function most responsible for data breach response	79%	80%	77%
Review of data breach communications plans	52%	58%	45%
Review of what was learned from previous data breaches or other security incidents	61%	58%	64%
None of the above	15%	16%	13%
Other	3%	4%	2%
Total	475%	477%	473%

Q31c. If your organization **never practices** data breach response, why not?	FY2022	US	EMEA
Not enough budget	26%	25%	28%
We are confident in our ability to respond to a data breach	43%	41%	45%
Too difficult to schedule a practice response	63%	65%	60%
Not a priority	61%	52%	73%
Total	193%	183%	205%

Q32a. Does your incident response plan include processes to manage an international data breach?	FY2022	US	EMEA
Yes	56%	66%	43%
No	36%	26%	50%
Unsure	8%	8%	7%
Total	100%	100%	100%

Q32b. If yes, is your organization's plan specific to each location where it operates?	FY2022	US	EMEA
Yes	56%	58%	53%
No	43%	42%	44%
Unsure	1%	0%	3%
Total	100%	100%	100%

Q33. How confident is your organization in its ability to deal with an international data breach?	FY2022	US	EMEA
Very confident	10%	9%	11%
Confident	21%	20%	23%
Somewhat confident	27%	25%	29%
Not confident	26%	31%	18%
No confidence	17%	15%	19%
Total	100%	100%	100%

Q34. As part of its data breach readiness efforts, does your organization have a business continuity management (BCM) program in place?	FY2022	US	EMEA
Yes	56%	60%	51%
No	44%	40%	49%
Total	100%	100%	100%

Q35. If yes, what are the reasons? Please select the top three reasons.	FY2022	US	EMEA
BCM is a valuable addition to data breach response planning	63%	64%	61%
BCM can reduce the cost of responding to a data breach	57%	60%	53%
BCM reduces the likelihood of having recurring data breaches	47%	48%	46%
BCM can minimize disruptions to business operations when a data breach occurs	59%	59%	60%
BCM can help ensure our organization's sensitive and confidential data is protected	41%	38%	45%
BCM diminishes the negative impact on the company's reputation following a data breach	28%	26%	31%
Other	5%	5%	4%
Total	300%	300%	300%

Q36. As part of its data breach readiness efforts, does your organization have a crisis management plan?	FY2022	US	EMEA
Yes	53%	54%	51%
No	47%	46%	49%
Total	100%	100%	100%

Q37. If yes, what does the crisis management plan cover? Please select all that apply.	FY2022	US	EMEA
Hurricane and other weather-related incidents	25%	26%	23%
Data breaches	44%	49%	37%
Cyberattacks	46%	47%	44%
Massive financial fraud	37%	39%	35%
Class action lawsuits	41%	44%	36%
Significant loss of market share	21%	23%	18%
Nation state attacks	27%	31%	21%
Serious damage to the organization's physical structure(s)	26%	29%	22%
Key members of the management team become seriously ill or die	41%	48%	32%
A pandemic	28%	31%	25%
Other	4%	6%	2%
Total	339%	373%	295%

Q38a. Did your organization have a crisis that necessitated the use of its crisis management plan?	FY2022	US	EMEA
Yes	59%	61%	56%
No	41%	39%	44%
Total	100%	100%	100%

Q38b. If yes, using the following 10-point scale from 1 = not effective to 10 = highly effective, please rate the effectiveness of your organization's crisis management plan in dealing with the crisis.	FY2022	US	EMEA
1 to 2	9%	10%	7%
3 to 4	11%	11%	11%
5 to 6	20%	23%	15%
7 to 8	30%	31%	29%
9 to 10	31%	25%	38%
Total	100%	100%	100%
Extrapolated value	6.76	6.50	7.10

Part 6. Regulations

Q39a. Is your company subject to the General Data Protection Regulation (GDPR)?	FY2022	US	EMEA
Yes	80%	70%	93%
No *	20%	30%	7%
Total	100%	100%	100%

*No and unsure responses combined in FY2019

Q39b. 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.	FY2022	US	EMEA
1 to 2	4%	5%	3%
3 to 4	12%	12%	13%
5 to 6	13%	11%	15%
7 to 8	35%	35%	36%
9 to 10	35%	37%	33%
Total	100%	100%	100%
Extrapolated value	7.92	8.21	7.54

Q40a. Is your company subject to the California Consumer Privacy Act (CCPA)?	FY2022	US	EMEA
Yes	31%	39%	20%
No	69%	61%	80%
Total	100%	100%	100%

Q40b. 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.	FY2022	US	EMEA
1 to 2	16%	13%	21%
3 to 4	15%	12%	19%
5 to 6	29%	31%	26%
7 to 8	26%	29%	23%
9 to 10	13%	15%	11%
Total	100%	100%	100%
Extrapolated value	5.60	5.92	5.18

Q41a. In the past two years, how many personal data breaches did your organization have that were required to be reported to regulators?	FY2022	US	EMEA
None	27%	29%	26%
1 to 5	41%	42%	40%
6 to 20	19%	15%	24%
More than 20	12%	14%	10%
Total	100%	100%	100%
Extrapolated value	6.50	6.11	6.98

Q41b. How many of the data breaches did you report to the Regulator?	FY2022	US	EMEA
None	35%	30%	41%
1 to 5	40%	40%	39%
6 to 20	11%	13%	9%
More than 20	13%	17%	8%
Total	92%	100%	81%
Extrapolated value	4.75	4.7	4.82

Part 7. Perceptions about the future

Q42. In the next 12 months, what concerns your organization most? Please select all that apply.	FY2022	US	EMEA
An increase in security incidents and data breaches	58%	59%	55%
Nation state attacks targeting our organization's high value information assets	42%	45%	39%
Our organization will not have the ability to retain skilled staff needed to mitigate security risks	47%	48%	45%
The inability to ensure that employees and contractors are following our organization's security and privacy policies	37%	44%	27%
The inability to prevent such incidents as downtime, employee negligence and malicious behavior	39%	49%	27%
The inability to respond to contain and remediate data breaches and security incidents	28%	30%	26%
Other	3%	4%	2%
Total	254%	280%	221%

Part 8. Organizational characteristics & respondent demographics

D1. What organizational level best describes your current position?	FY2022	US	EMEA
Senior Executive	6%	6%	6%
Vice President	10%	11%	9%
Director	27%	26%	29%
Manager	24%	21%	28%
Supervisor	21%	24%	18%
Technician	6%	7%	5%
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.	FY2022	US	EMEA
CEO/Executive Committee	4%	5%	4%
Chief Financial Officer	6%	7%	6%
General Counsel	13%	12%	14%
Chief Privacy Officer	8%	8%	8%
Chief Information Officer	16%	14%	17%
Compliance Officer	18%	18%	18%
Human Resources VP	1%	2%	0%
Chief Security Officer	6%	6%	5%
Chief Risk Officer	11%	13%	10%
Other	2%	1%	3%
Chief Information Security Officer	15%	14%	16%
Total	100%	100%	100%

D3. What industry best describes your organization's industry focus?	FY2022	US	EMEA
Communications	2%	2%	4%
Defense & aerospace	1%	1%	0%
Education & research	2%	2%	3%
Energy & utilities	5%	6%	5%
Entertainment & media	5%	4%	6%
Agriculture & food services	1%	1%	0%
Health & pharmaceutical	10%	10%	10%
Hospitality	2%	2%	2%
Industrial & manufacturing	10%	11%	9%
Retailing	8%	8%	7%
Services	10%	11%	10%
Technology & software	7%	7%	7%
Transportation	3%	4%	2%
Public sector	10%	11%	9%
Consumer products	4%	4%	5%
Financial services	17%	18%	17%
Other	2%	0%	5%
Total	100%	100%	100%

D4. What is the worldwide headcount of your organization?	FY2022	US	EMEA
Less than 500	14%	12%	17%
500 to 1,000	19%	16%	23%
1,001 to 5,000	23%	22%	24%
5,001 to 25,000	18%	19%	16%
25,001 to 75,000	19%	23%	14%
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 Reserved Response™

Experian's Reserved Response™ program is the industry's first proactive data breach response solution that offers decades of 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. Visit Experian.com/Data-Breach for more information.