LogRhythm®

Security and the C-Suite: Making Security Priorities Business Priorities

Evaluating the Influence of Security Leaders in Enterprise Organizations

Contents

01 Introduction

To gain organizational influence, cybersecurity leaders should report to the CEO.

The purpose of this research is to learn valuable information about the role and responsibilities of today's cybersecurity leaders and the challenges they face in creating a strong security posture. Ponemon Institute surveyed 1,426 cybersecurity professionals in the United States, EMEA and Asia-Pacific.

Most of these professionals hold the title of Chief Information Security Officer (17 percent), Security Manager (15 percent), Chief Information Officer (12 percent), Chief Technology Officer (11 percent) and Security Director (11 percent).

According to the research, 93 percent of respondents are not reporting directly to the CEO.

In fact, on average respondents are three levels away from the CEO which makes it very difficult to ensure that leadership has an accurate and complete understanding of security risks facing the organization. Sixty percent of respondents say the IT security leader should report directly to the CEO because it would create greater awareness about security throughout the organization.

The majority of organizations are experiencing cyberattacks.

Sixty percent of respondents say their organization had a cyberattack in the past two years. As shown in Figure 1, 35 percent of respondents say no one was held accountable for the cyberattack followed by the CEO and IT security leader (28 percent of respondents). However, 42 percent of respondents say the IT security leader should be the person most accountable for preventing or mitigating the consequences of a cyberattack. It is easy to conclude, therefore, that the majority of respondents, (54 percent) worry about their job security.

Fifty-five percent of respondents say their organizations had a data breach in the past two years. Thirty percent of respondents say no one was held accountable followed by both the CEO and cybersecurity leader were held accountable for the breach. Thirty-six percent of respondents say the IT security leader should be held accountable for the data breach, as shown in Figure 2.

TAKEAWAY

Similar to cyberattacks, in the future the IT security leader will be the person held most responsible if the organization has a data breach.

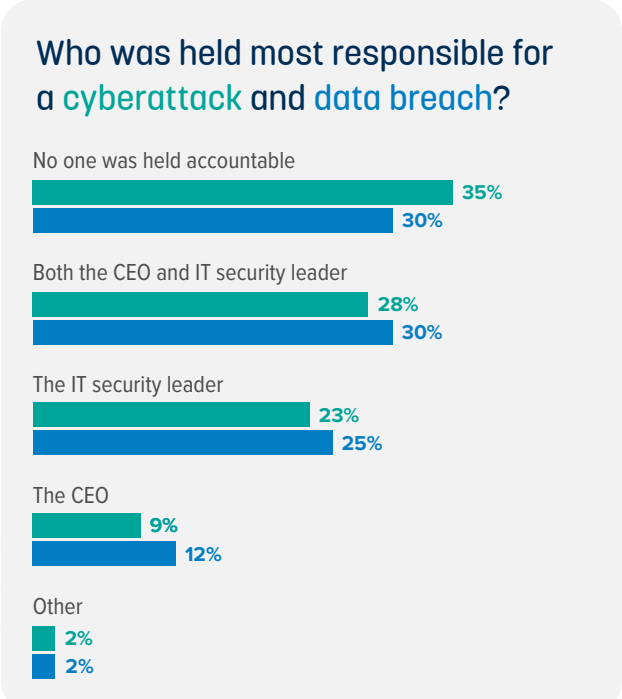


FIGURE 1

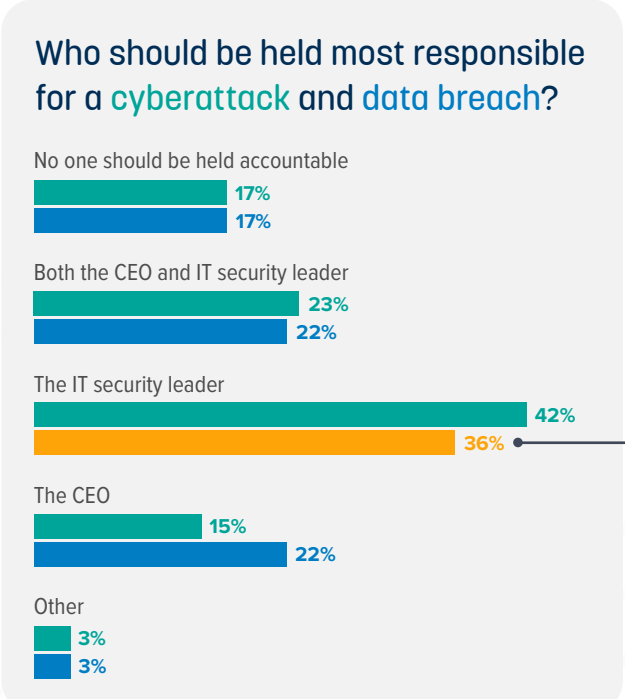


FIGURE 2

The importance of making security priorities business priorities.

Following are reasons why a strong security posture is at risk because IT security leaders are not as influential and valued as they should be.

The significant increase in employees working remotely due to COVID-19 has created the biggest security challenge for IT security leaders, according to the research. The following findings indicate why it is a risk to sensitive and confidential information:

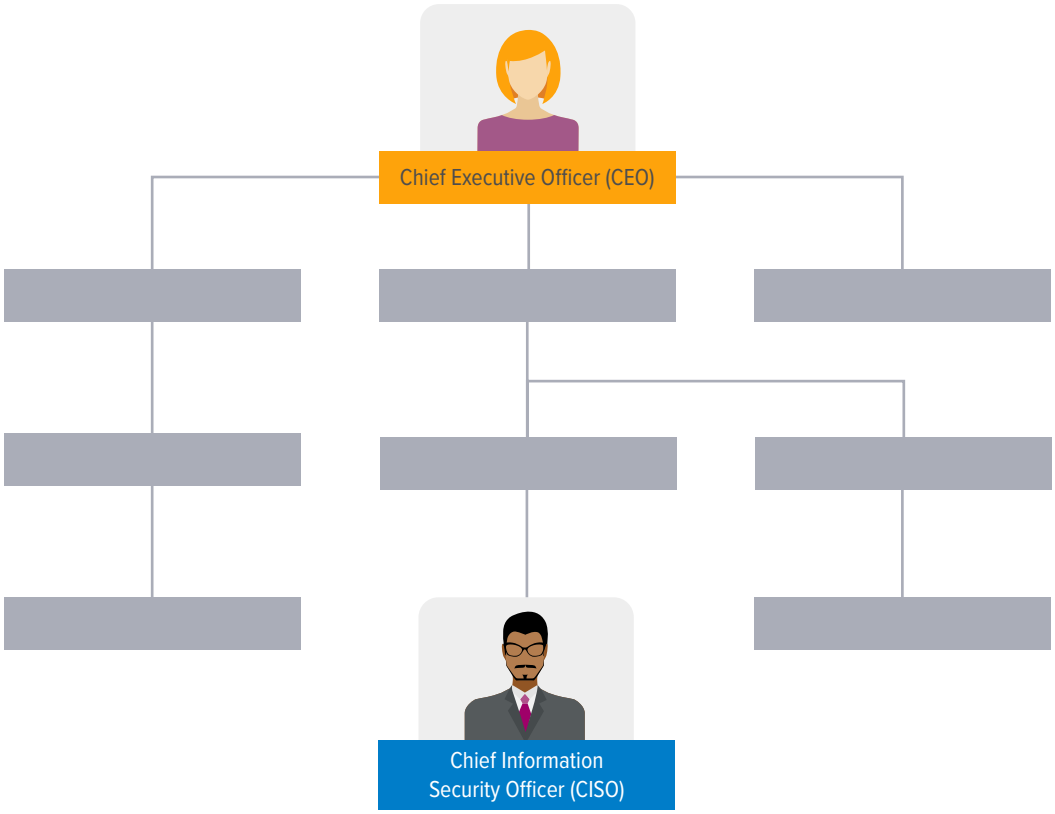
say a family member is allowed to use the work device

of respondents say less secure home networks are used

of respondents say employees and contractors believe the organization is not monitoring their activities

Sixty-three percent of respondents say they are not briefing the board of directors on risks, such as those created by remote working and what is being done to prevent and detect security incidents.

Of the 37 percent of respondents who say they do report to the board, 41 percent of these respondents say briefings only happen following a security incident. This reactive vs. proactive approach is a deterrent to improving the organization's security posture.



Only 29 percent of respondents say they have a board-level committee dedicated to cybersecurity threats and issues facing the organization. If they do have such a committee, only 43 percent of respondents say someone from the cybersecurity function is a member of the committee.

Despite 57 percent of respondents having complete ownership (23 percent) or significant influence (34 percent) over an average annual budget of $38 million, most IT security leaders are still not having a direct relationship with the CEO and board of directors.

As a result of the findings above, only 43 percent of respondents say their organization values and effectively leverages the expertise of cybersecurity leaders.

Moreover, less than half of respondents (46 percent) say senior leadership has confidence that the cybersecurity leader understands the business goals.

As shown in this research, the importance of having people, process and technologies in place to proactively prevent and detect attacks from hackers, malicious insiders as well as negligent insiders is often being overlooked by the CEO and the board of directors. Today, in most organizations the cybersecurity function does not have a direct voice to the c-suite. Instead, as shown in the research, leadership is more often focused on having a skilled workforce, improving corporate culture and customer experience.

Following are recommendations to elevate the importance of the IT security leader's role.

Sensitive and confidential data should be considered the currency of the information age.	IT security leaders should communicate the solutions that are in place to safeguard important data assets such as intellectual property and customer records in a way that does not have a negative impact on business goals and operations.
Ensure security policies are appropriate and adequate to support business objectives.	If there are security risks that are not being addressed, provide recommendations and concrete actions that the CEO and board can approve or disapprove.
IT security leaders should have put an effective incident response and disaster recovery plan in place and assure that the CEO and board of directors understand the level of preparedness.	As discussed, many briefings are occurring after the security incident and it will be important to communicate that these procedures are in place. According to the research, 76 percent of respondents say their organizations have an incident response plan. Unfortunately, 58 percent of respondents say there is no set time to review and update the plan (34 percent) or the plan has not been reviewed or updated since the plan was put in place (24 percent).
Be persistent in scheduling meetings with the c-suite and board of directors.	Include in these presentations the financial, regulatory and reputational quantifiable and qualitative consequences of a security incident.

02

Key Findings

In this section, we provide an analysis of the global research findings. The following topics are covered in this report.

- Influence of the cybersecurity leader
- The value of cyber insurance
- Factors and challenges affecting the cybersecurity leader's role
- How cybersecurity leaders are managing third-party risk and preparing for security incidents
- Regional differences

How influential is the cybersecurity leader?

Cybersecurity leaders on average are three levels away from reporting to the CEO. As discussed previously, 93 percent of respondents do not report directly to the CEO. According to Figure 3, most respondents are reporting to the CIO (24 percent), director/manager of IT (19 percent), CTO (12 percent) and VP of IT (11 percent). The cybersecurity respondents in this research have held their positions an average of six years.

To whom does the cybersecurity leader report to?

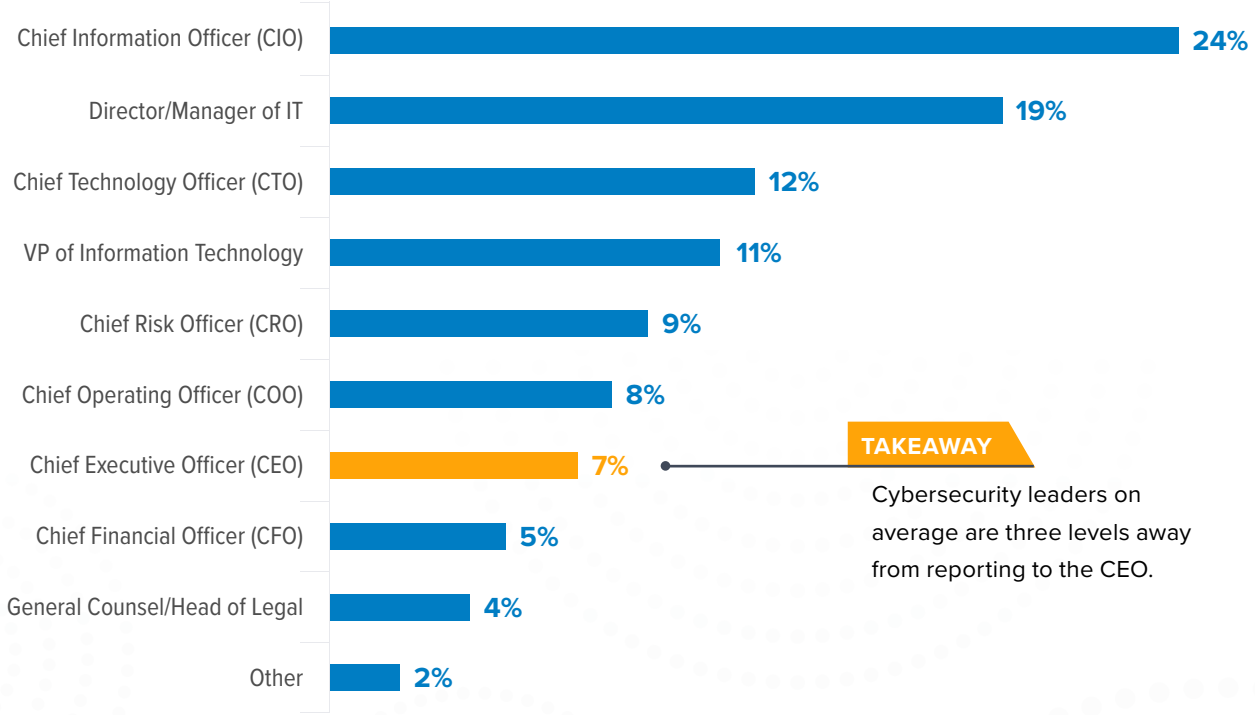


FIGURE 3

The Security Leader

Perceptions about the cybersecurity leader's role.

The benefit of having a direct reporting relationship with the CEO is that the importance of safeguarding sensitive and confidential information is elevated throughout the organization.

According to Figure 4, 60 percent of respondents say the cybersecurity leader should be part of the C-suite and report directly to the CEO because it would give the cybersecurity leader more authority and create greater awareness of security issues throughout the organization. As a consequence of this reporting relationship, only 37 percent of respondents say their organization values and effectively leverages the expertise of the cybersecurity leader.

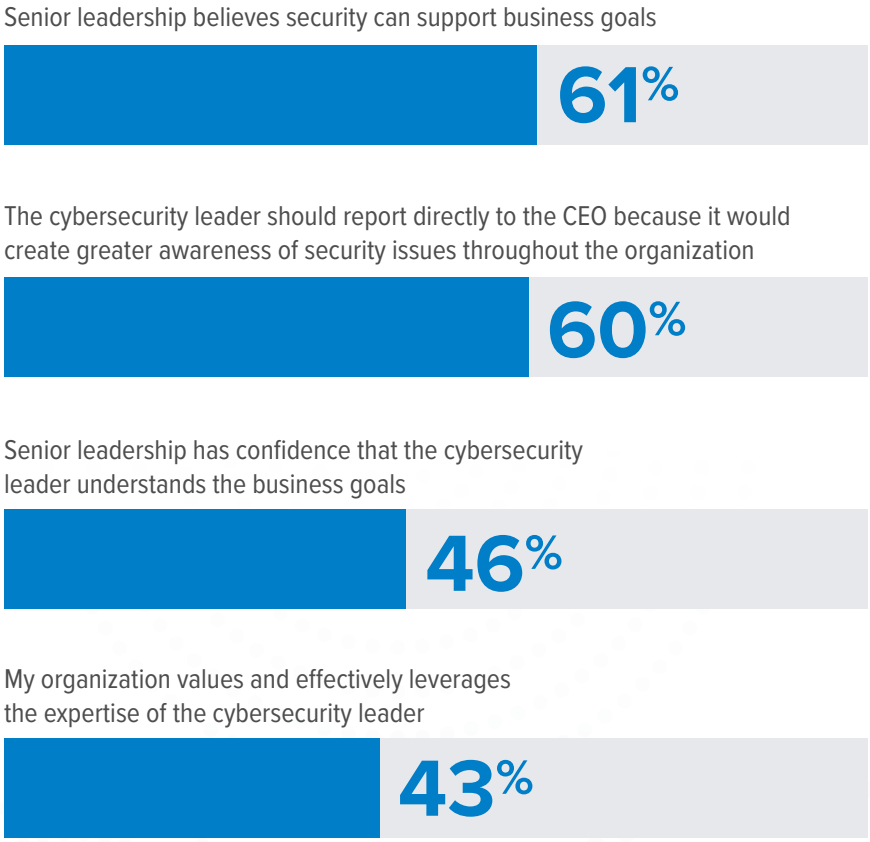


FIGURE 4 Strongly agree and Agree responses combined

The Security Leader

How often do you or someone responsible for cybersecurity report to the board of directors?

Overwhelmingly, the board of directors is not getting a clear picture of the organization's security posture.

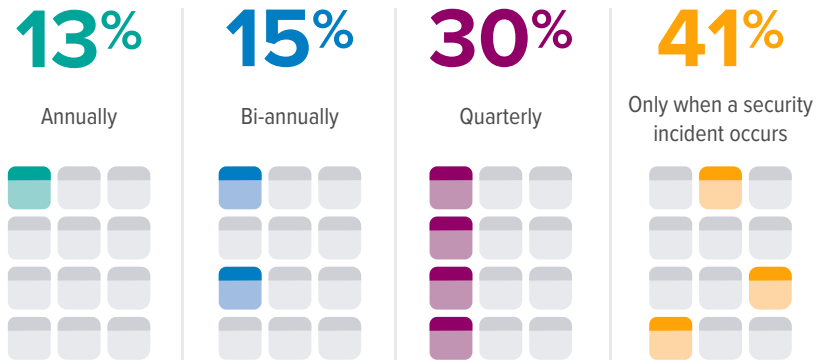


FIGURE 5

IT security leaders are not as influential as they should be with the board of directors, as well. Only 37 percent of respondents say they report or someone in their security function reports directly to the board of directors.

As shown in Figure 5, of these respondents, 41 percent of respondents say they brief the board only when a security incident occurs. Thirty percent say reporting occurs quarterly. Moreover, only 29 percent of respondents say they have a committee dedicated to cybersecurity threats and issues facing the organization. If they do have such a committee, only 43 percent of respondents say someone from the cybersecurity function is a member of the committee.

As will be discussed later, organizations allocate on average $38 million to security activities, which 63 percent of respondents say is insufficient to invest in the right technologies. The lack of influence with the board of directors is a possible barrier to increasing cybersecurity budgets.

The Security Leader

What topics are covered during the board meetings?

Cybersecurity leaders are most often asked about the effectiveness and efficiency of security programs rather than the threats facing the organization.

According to Figure 6, of the 37 percent of respondents who say they report to the board, 64 percent of respondents say they brief the board of directors on the effectiveness and efficiency of security programs followed by the state of compliance with regulations (52 percent of respondents). Only 40 percent of respondents say they report on changes to the organizations' security and risk posture or changes to threats, attacks and vulnerabilities.

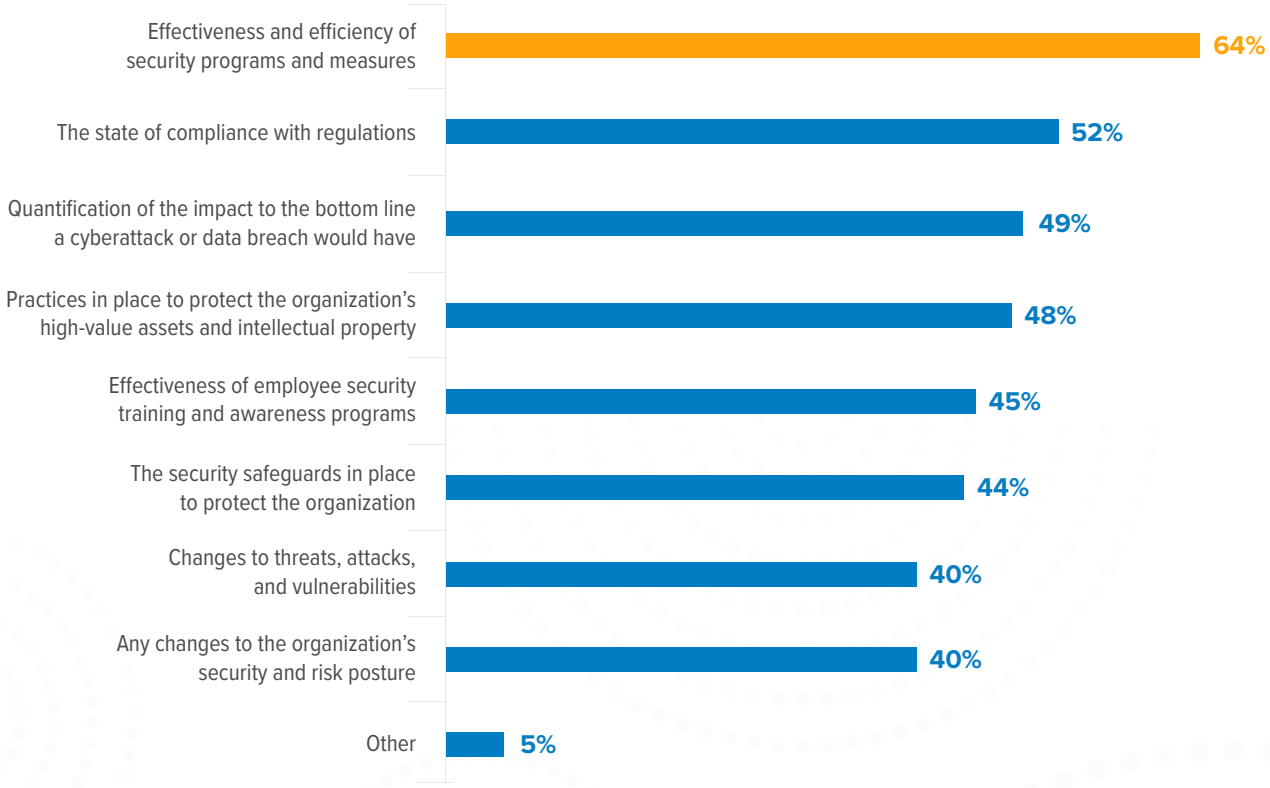


FIGURE 6 More than one response permitted

Security Budget

How much influence do you have over the security budget?

Cybersecurity leaders do have influence over the security budget.

The average annual IT budget is $159 million and an average of 24 percent or $38 million is allocated to security activities. According to Figure 7, 57 percent of respondents say they have complete ownership (23 percent) or significant influence (34 percent) over the security budget. Despite the funds they have control over, it is difficult to understand why IT security leaders are not reporting directly to the CEO and board of directors.

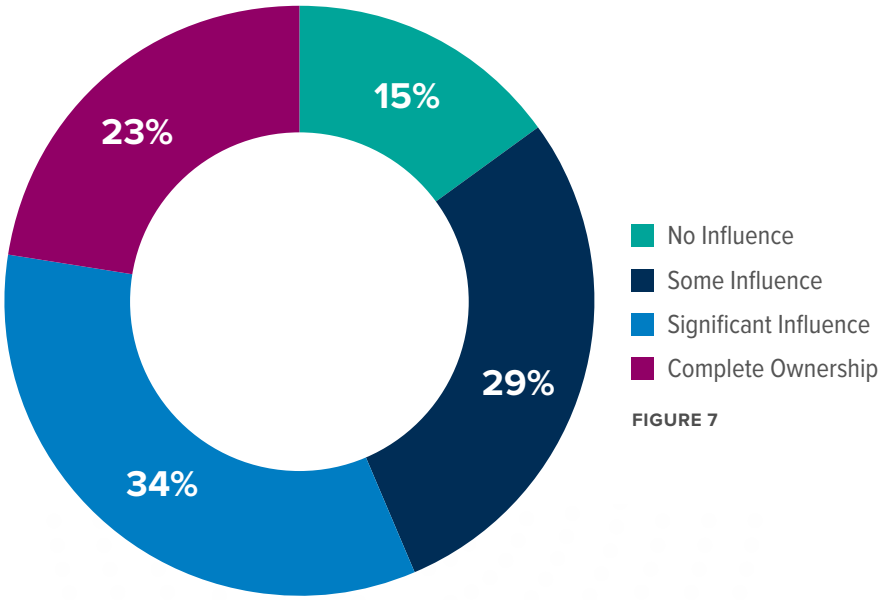


FIGURE 7

Security Budget

What factors would influence an increase in the security budget?

> Changes in threats, attacks and vulnerabilities would influence an increase in the security budget.

According to Figure 8, 62 percent of respondents say they will recommend an increase in the budget if they see changes in threats, attacks and vulnerabilities. This is followed by concerns about ensuring a secure digital transformation (59 percent of respondents) or having a data breach (54 percent of respondents). Less than half (45 percent) of respondents will request an increase in the budget because of compliance issues.

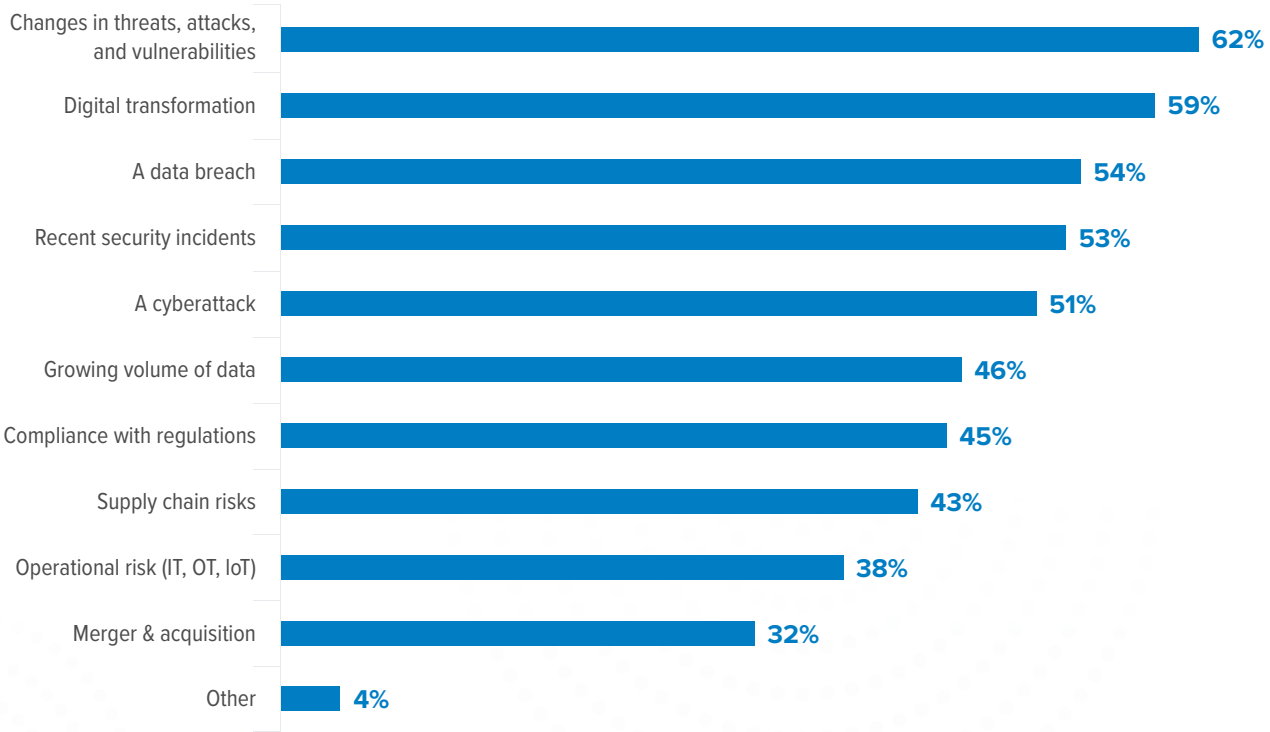


FIGURE 8 More than one response permitted

Security Budget

What are your spending priorities in 2021?

> Investment in advanced technologies and in-house expertise are the spending priorities for 2021.

As shown in Figure 9, 46 percent of respondents say the priority for spending is the investment in technologies such as automation, AI and machine learning followed by investment in additional in-house expertise (45 percent of respondents).

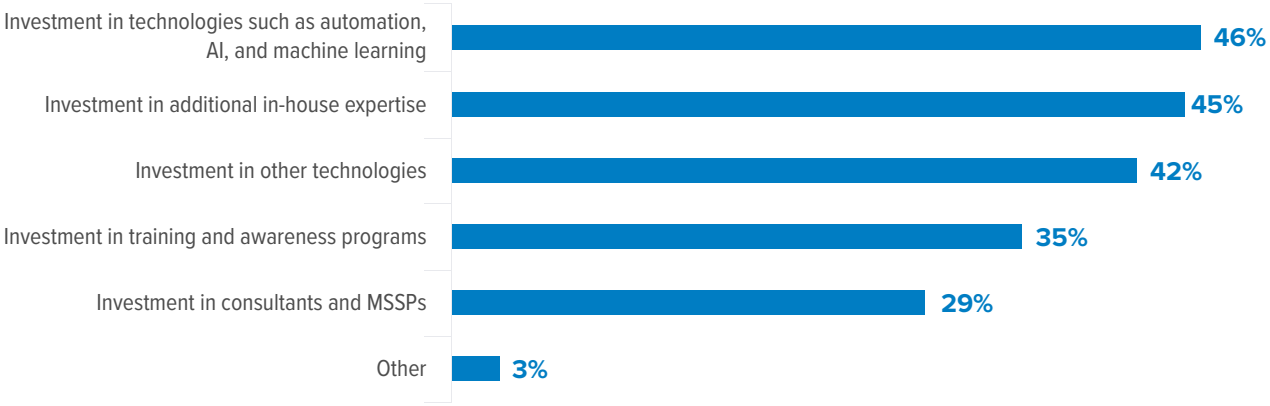


FIGURE 9 Two responses permitted

Security Budget

The budget is considered insufficient to invest in the right technologies.

Fifty-four percent of respondents are worried about their job security. As shown in Figure 10, 63 percent of these respondents say the reason is an insufficient budget to invest in the right technologies, which is one of their spending priorities. More than half (53 percent) of respondents say it is because senior leadership does not understand their role, and 51 percent of respondents say they lack executive support.

TAKEAWAY

Insufficient security budget contributes to IT security leaders' job insecurity.

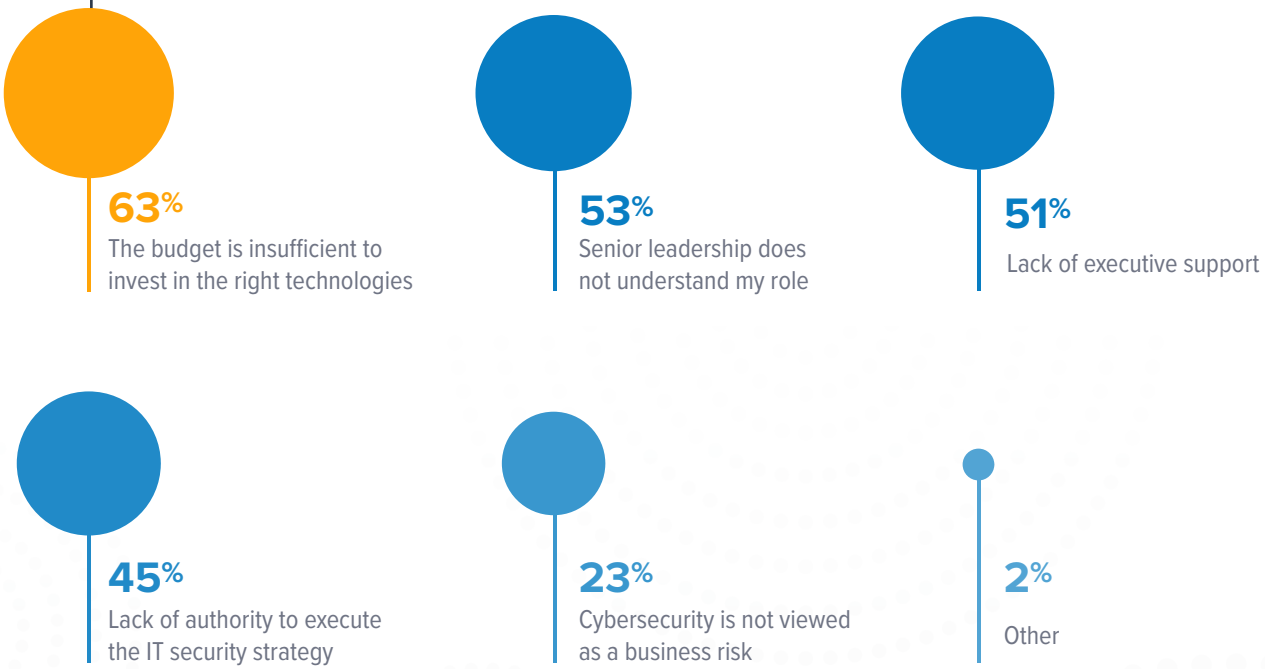


FIGURE 10 More than one response permitted

Cyber Insurance

Cyber insurance coverage is not considered sufficient.

Forty-seven respondents say their organizations have purchased cyber insurance and the average limit purchased is $32 million. Only 36 percent of respondents say coverage is sufficient. Sixty-nine percent of respondents who say their organization currently does not have cyber insurance plan to purchase a policy in the future.

Incidents involving third parties are most often covered by cyber insurance. According to Figure 11, 52 percent of respondents say incidents affecting business partners, vendors or other third parties that have access to their information assets is covered followed by external attacks by criminals (46 percent of respondents).

According to Figure 12, the top two approaches to determining the level of coverage is having a third-party specialist review the terms and conditions (54 percent of respondents) and the maximum available from the insurance market (49 percent of respondents).

TAKEAWAY

Only 24 percent of respondents say amount of coverage is based on a formal risk assessment by a third party.

What types of incidents does your organization's cyber insurance cover?

FIGURE 11 More than one response permitted

How does your organization determine the level of coverage it considers adequate?

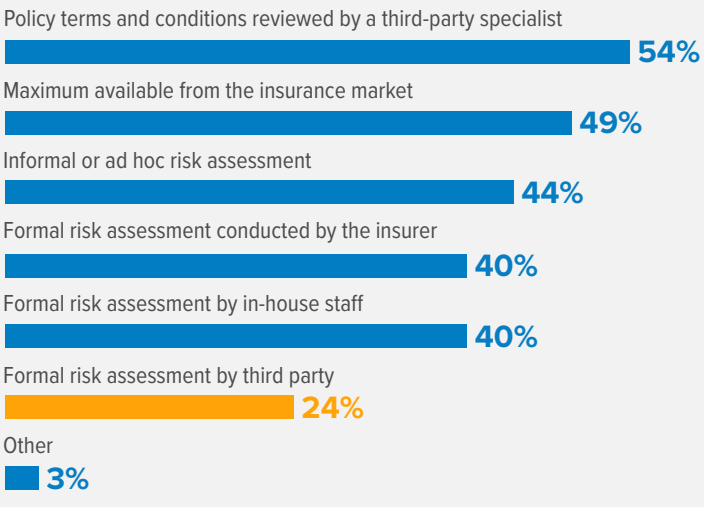


FIGURE 12 More than one response permitted

Cyber Insurance

What coverage does this cyber insurance offer your organization?

According to Figure 13, 51 percent of respondents say notification costs to data breach victims are covered, and 50 percent of respondents say legal costs are covered. Only 25 percent of respondents say damage to their brand is covered.

TAKEAWAY

Victim notification and legal costs are most likely to be covered.

51% Notification costs to data breach victims	**50%** Legal defense costs
43% Third-party liability	**40%** Forensics and investigative costs
38% Revenue losses	**36%** Replacement of lost or damaged equipment
34% Regulatory penalties and fines	**25%** Loss of asset value
25% Brand damages	**22%** Communication costs to regulators
18% Employee productivity losses	**4%** Other

FIGURE 13 More than one response permitted

Factors and Challenges

Factors and challenges affecting the cybersecurity leader's role.

Cybersecurity leaders are assuming more accountability and risk, but without receiving higher salaries.

Less than half of respondents (48 percent) say their salaries have increased. As shown in Figure 14, 56 percent of respondents say they have assumed more accountability and risk for ensuring a strong security posture in the past year.

Seventy percent of respondents say they do receive an annual bonus, but only 26 percent say it has increased. Fifty-five percent of these respondents say the increase has offset the increased accountability and risk assumed.

As shown in Figure 15, 59 percent of respondents say they have termination protections written into their contract and the average payout is approximately $3.8 million. Of the 41 percent of respondents who say they don't have termination protections, 58 percent of respondents say they would like such protections to offset the risk associated with their jobs.

Have you assumed more accountability and risk for ensuring a strong security posture?

FIGURE 14

Do you have termination protections written into your contract?

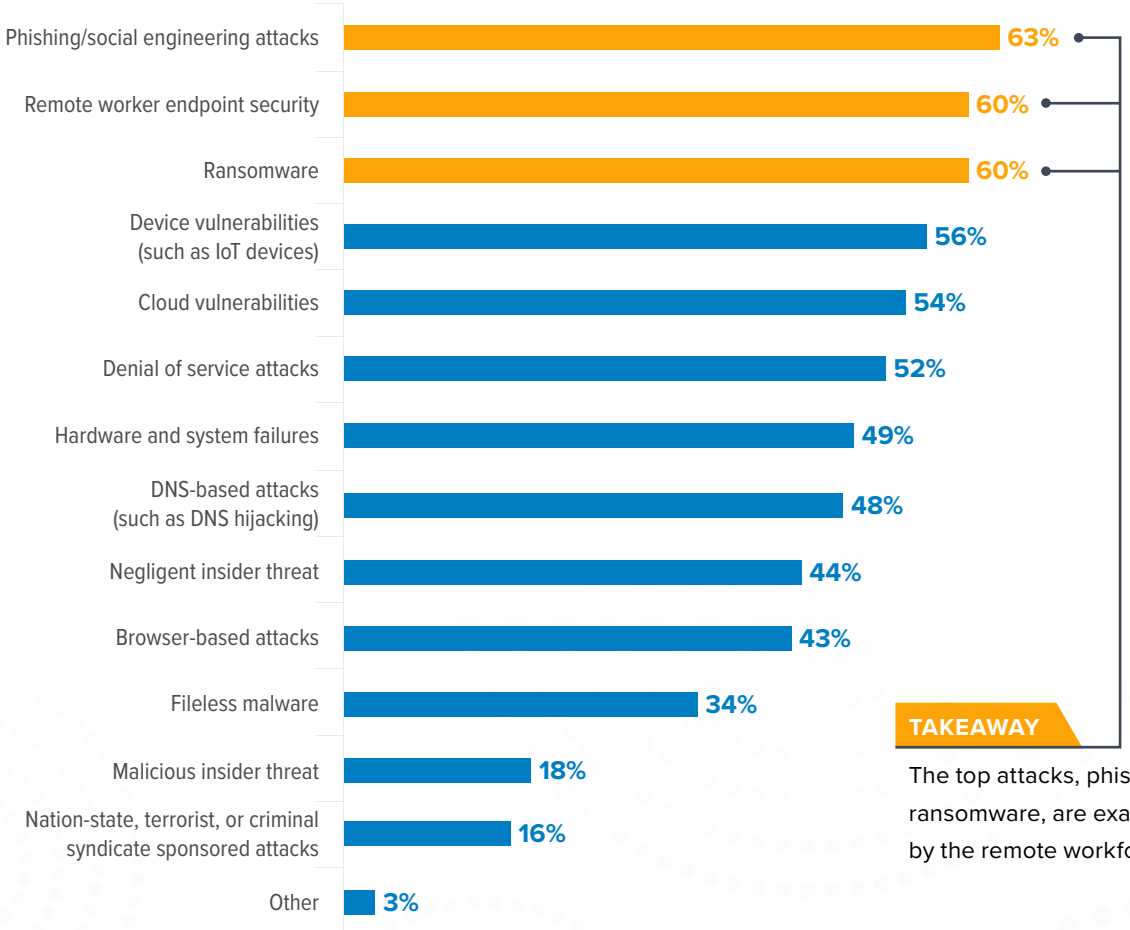
FIGURE 15

Factors and Challenges

What are the top cybersecurity risks affecting your organization?

Remote worker endpoint security is in the top three risks facing organizations.

As shown in Figure 16, the top attacks, phishing and ransomware, are exacerbated by the remote workforce. Sixty-three percent of respondents say the top risk is phishing/social engineering attacks, and 60 percent of respondents say it is the remote worker endpoint security and ransomware.



TAKEAWAY

The top attacks, phishing and ransomware, are exacerbated by the remote workforce.

FIGURE 16 Six responses permitted

Factors and Challenges

Why does the remote workforce increase the risk to your organization's sensitive data?

Sixty-two percent of respondents say a remote workforce increases the risk to their organization's sensitive data. An average of 48 percent of employees and contractors in the organizations represented in this research are working remotely.

As shown in Figure 17, the primary reason for an increase in risk is that less secure home networks are used (73 percent of respondents), followed by employees and contractors believe the organization is not monitoring their activities (68 percent of respondents) and a family member is allowed to use the work device (67 percent of respondents).

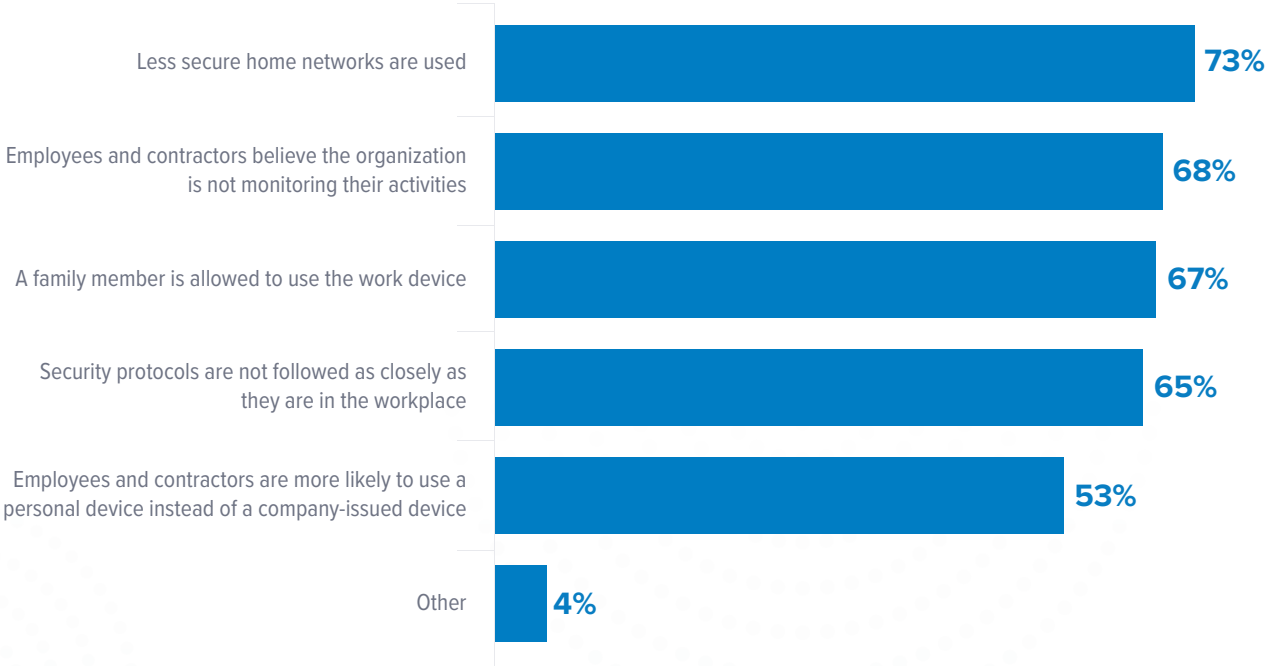
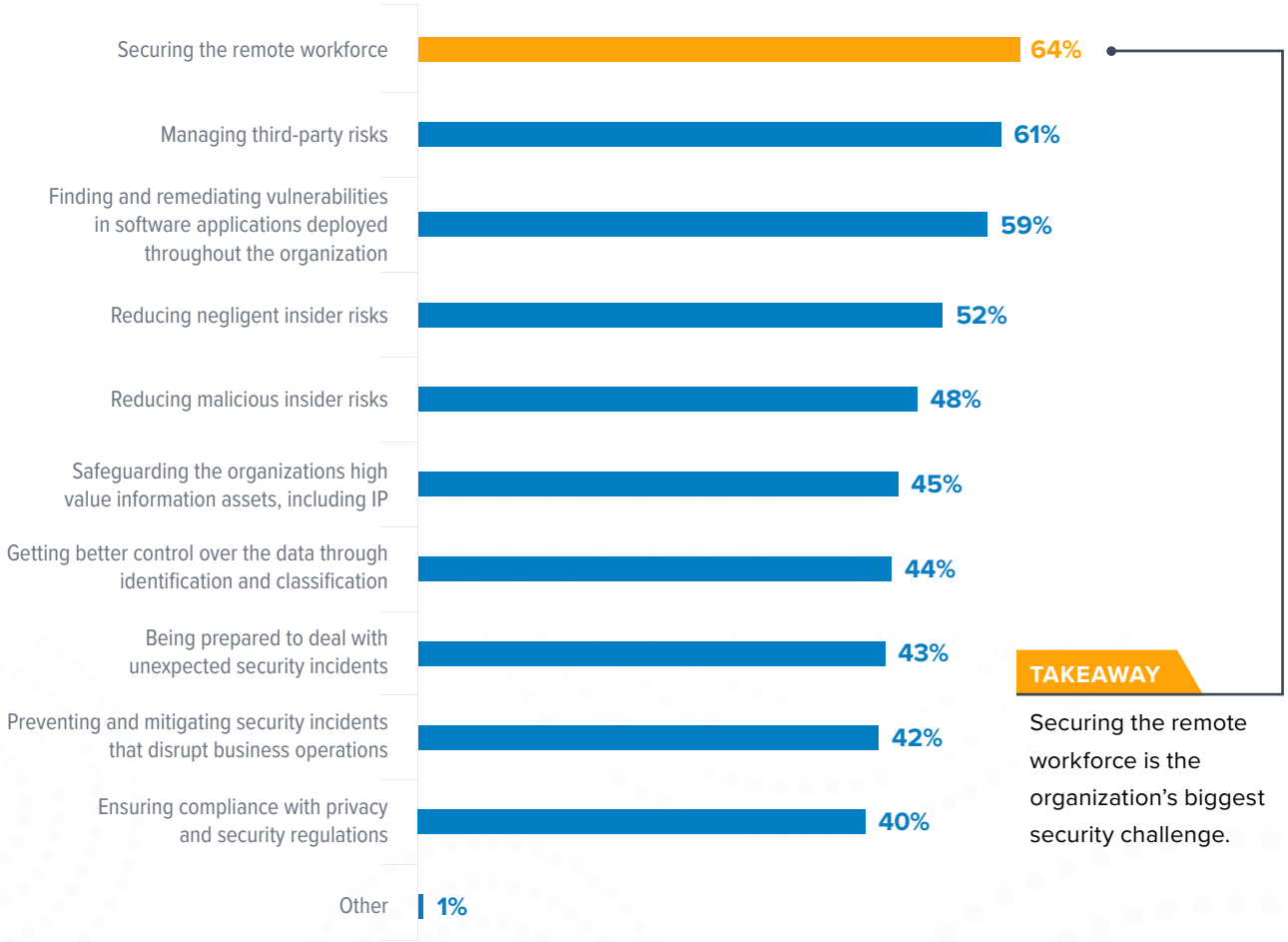


FIGURE 17 More than one response permitted

Factors and Challenges

What are your organization's biggest security challenges?

In addition to being one of the biggest security risks, the remote workforce is also the biggest security challenge. According to Figure 18, 64 percent of respondents say mitigating the risk of the remote workforce is the biggest challenge facing cybersecurity leaders. This is followed by managing third-party risks (61 percent of respondents) and finding and remediating vulnerabilities in software applications deployed throughout the organization (59 percent of respondents).



TAKEAWAY

Securing the remote workforce is the organization's biggest security challenge.

FIGURE 18 Five responses permitted

Factors and Challenges

What methods do you use to determine the potential damage to your organization?

Many organizations (53 percent of respondents) say they are able to evaluate the threats discussed above based on their ability to do the most damage to their organization such as the loss of high-value assets, fines, the loss of reputation and downtime. The method primarily used, as shown in Figure 19, is the Cyber Kill Chain (56 percent of respondents) and NIST (47 percent of respondents).

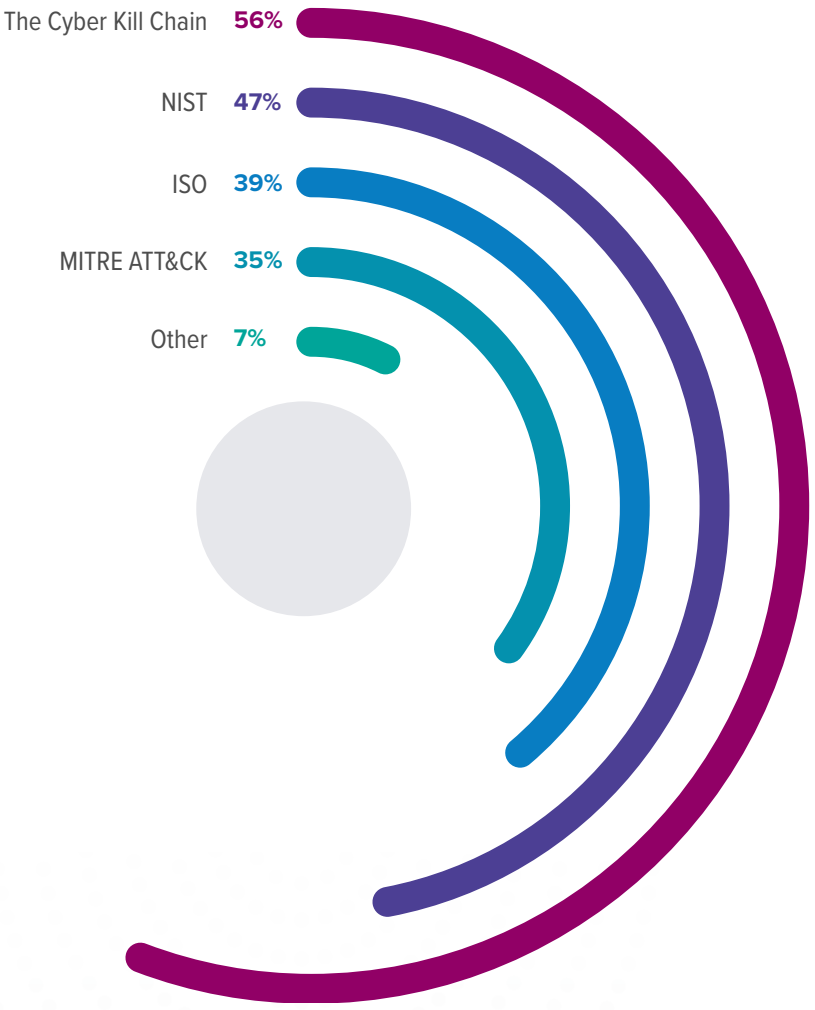


FIGURE 19 More than one response permitted

Factors and Challenges

What are the biggest organizational challenges?

In most organizations, the cybersecurity function is not aligned with organizational challenges.

As discussed previously, cybersecurity leaders are assuming more accountability for a strong security posture. Therefore, the challenges they face are different than the enterprise's challenges. It is understandable, therefore, that only 46 percent of respondents say the cybersecurity function is aligned and supportive of addressing the organizational challenges listed in Figure 20.

Having a skilled workforce is the biggest organizational challenge, according to 60 percent of respondents. This is followed by improving corporate culture (54 percent of respondents) and improving the customer experience (53 percent of respondents). Challenges involving profitability are not considered as significant. Specifically, only 36 percent of respondents say decreasing costs and only 38 percent say increasing revenues are the biggest organizational challenge.

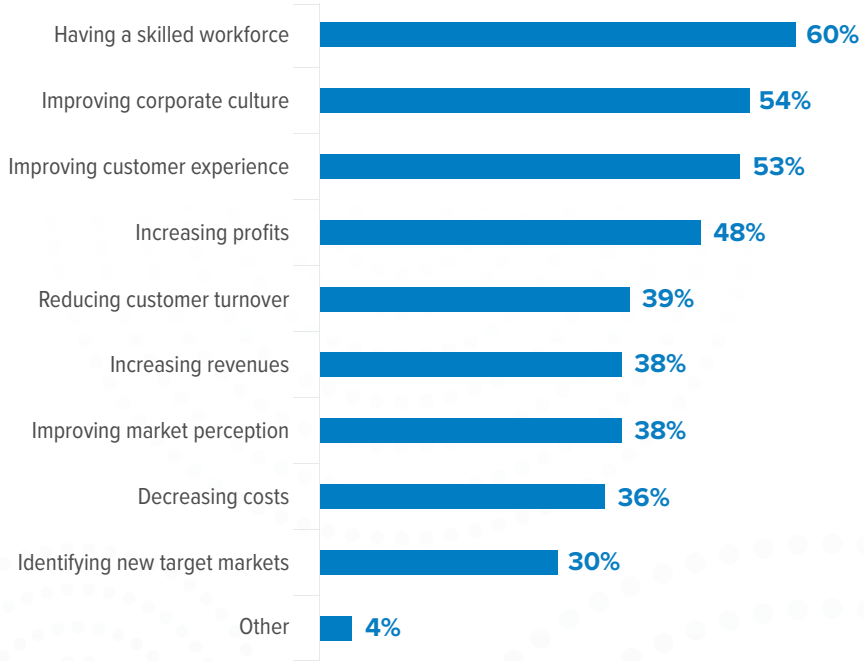


FIGURE 20 Four responses permitted

Third-Party Risk

How cybersecurity leaders are managing the third-party risk and preparing to respond to a security incident.

Third-party risk is the second biggest security challenge for cybersecurity leaders.

However, only 42 percent of respondents say their organizations are evaluating the security and privacy practices before they are engaged in a business relationship that requires the sharing of sensitive or confidential information.

According to Figure 21, if they do evaluate third parties slightly over half (52 percent) of respondents review written policies and procedures and 50 percent of respondents say they acquire signature on contracts that legally obligates the third party to adhere to security and privacy practices. Only 40 percent of respondents assess the third party's security and privacy practices.

If yes, how do you evaluate third-party privacy and security practices?

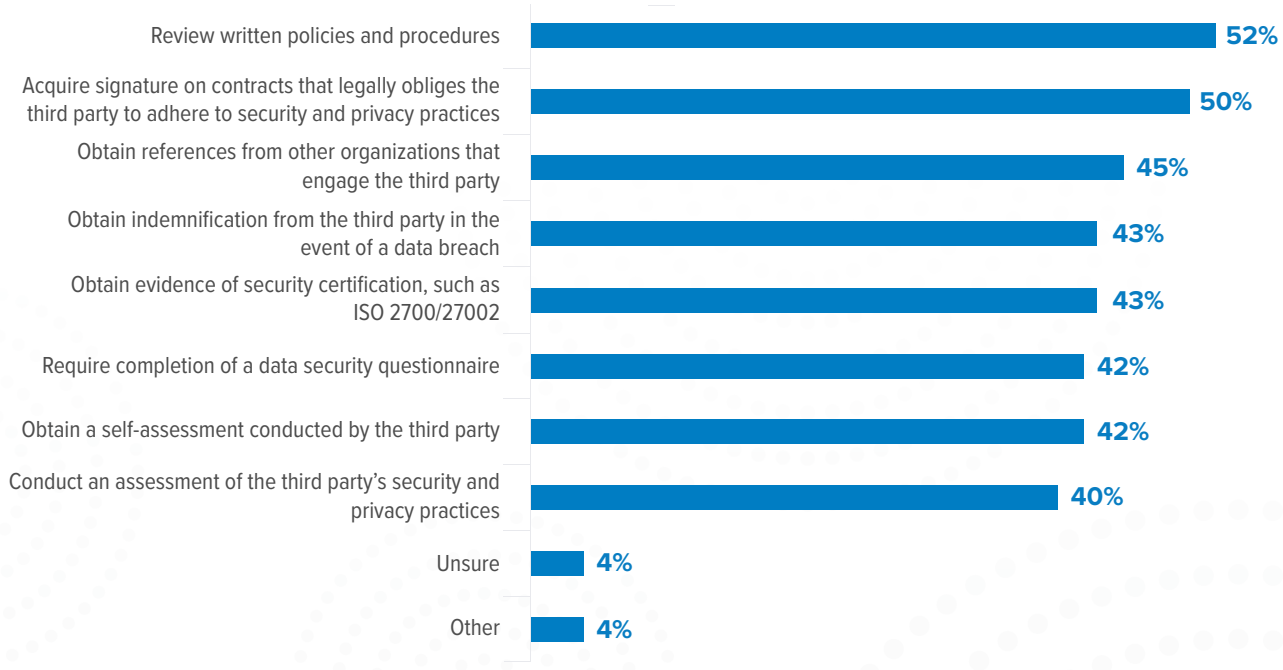


FIGURE 21 More than one response permitted

Of the 42 percent of respondents who evaluate the security and privacy practice of third parties, slightly more than half (54 percent) are evaluating the security and privacy practices of all third-party subcontractors before permitting their third parties to share sensitive or confidential information with them.

As shown in Figure 22, the three primary methods for such an evaluation are the use of technologies that can reveal the identity of their third-party's subcontractors (54 percent of respondents), require signatures on contracts that legally obligates the third-party's subcontractors to adhere to security and privacy practices (50 percent of respondents) and require completion of a data security questionnaire (49 percent of respondents).

If yes, how do you evaluate third-party subcontractors?

54% Use technologies that can reveal the identity of your third-party subcontractors	**50%** Require signatures on contracts that legally obligate the third party's subcontractors to adhere to security and privacy practices
49% Require completion of a data security questionnaire	**47%** Require third parties to obtain your specific approval before they share sensitive or confidential information with a subcontractor
45% Obtain references from other organizations that engage the third parties subcontractors	**45%** Require third parties to disclose any subcontractors with whom they will share your sensitive or confidential information
45% Obtain evidence that third party's subcontractors have security certification such as ISO 2700/27002	**43%** Obtain evidence of security certification such as ISO 2700/27002
43% Obtain indemnification from the third party's subcontractors in the event of a data breach	**43%** Conduct an assessment of the third party's subcontractors' security and privacy practices
4% Other	**1%** Unsure

FIGURE 22 More than one response permitted

Incident Response

How often does your organization update the incident response plan?

Organizations have an incident response plan, but most are not updated.

Seventy-six percent of respondents say their organizations have an incident response plan, but 58 percent of respondents say there is no set time period for reviewing and updating the plan (34 percent) or they have not reviewed or updated since the plan was put in place (24 percent), as shown in Figure 23.

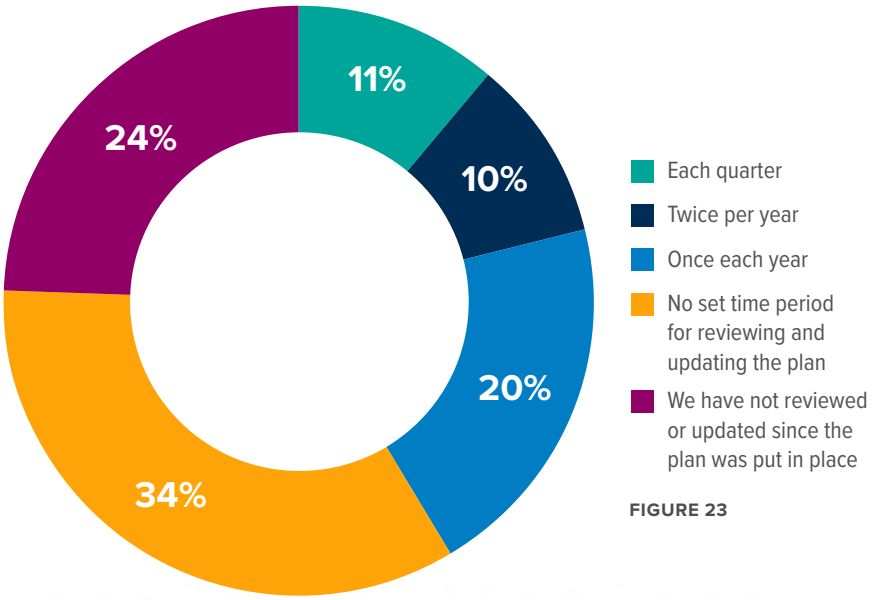


FIGURE 23

Incident Response

How does your organization prepare for an incident?

Organizations have an incident response plan, but most are not updated.

Figure 24 presents the steps organizations take to prepare for an incident. Fifty-four percent of respondents say they document and practice their data breach plan, less than half (48 percent) of respondents say their organizations conduct background checks on new full-time employees and vendors or create a "standby website" for content that can be made live when an incident occurs.

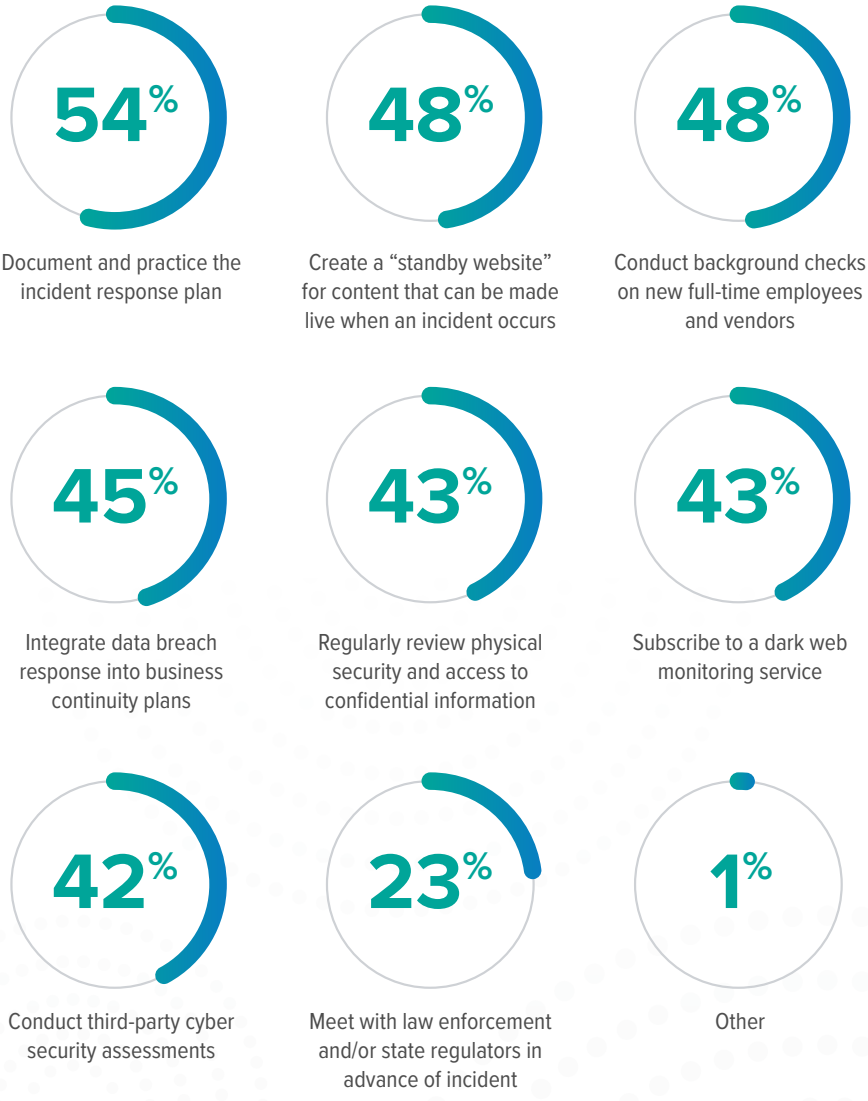


FIGURE 24 More than one response permitted

Incident Response

What does your organization's incident response plan require?

Most organizations require C-level approval of the incident response plan (83 percent of respondents).

Figure 25 lists the typical requirements included in an incident response plan. Eighty-one percent of respondents say the third-party's incident response plan is reviewed followed by procedures for communications with state attorneys general and regulators (78 percent of respondents) and business partners and third parties (76 percent of respondents).

FIGURE 25 More than one response permitted

Incident Response

Does the incident response plan offer guidance on managing security incidents?

Figure 26 presents a list of security incidents that could affect organizations. Sixty-two percent of respondents say the plan provides guidance on dealing with the loss or theft of intellectual property or confidential information followed by the loss or theft of paper documents and tapes containing sensitive information (58 percent of respondents). Only 25 percent of respondents say there is guidance on managing attacks by hackers and only 30 percent of respondents say it covers IoT-based attacks.

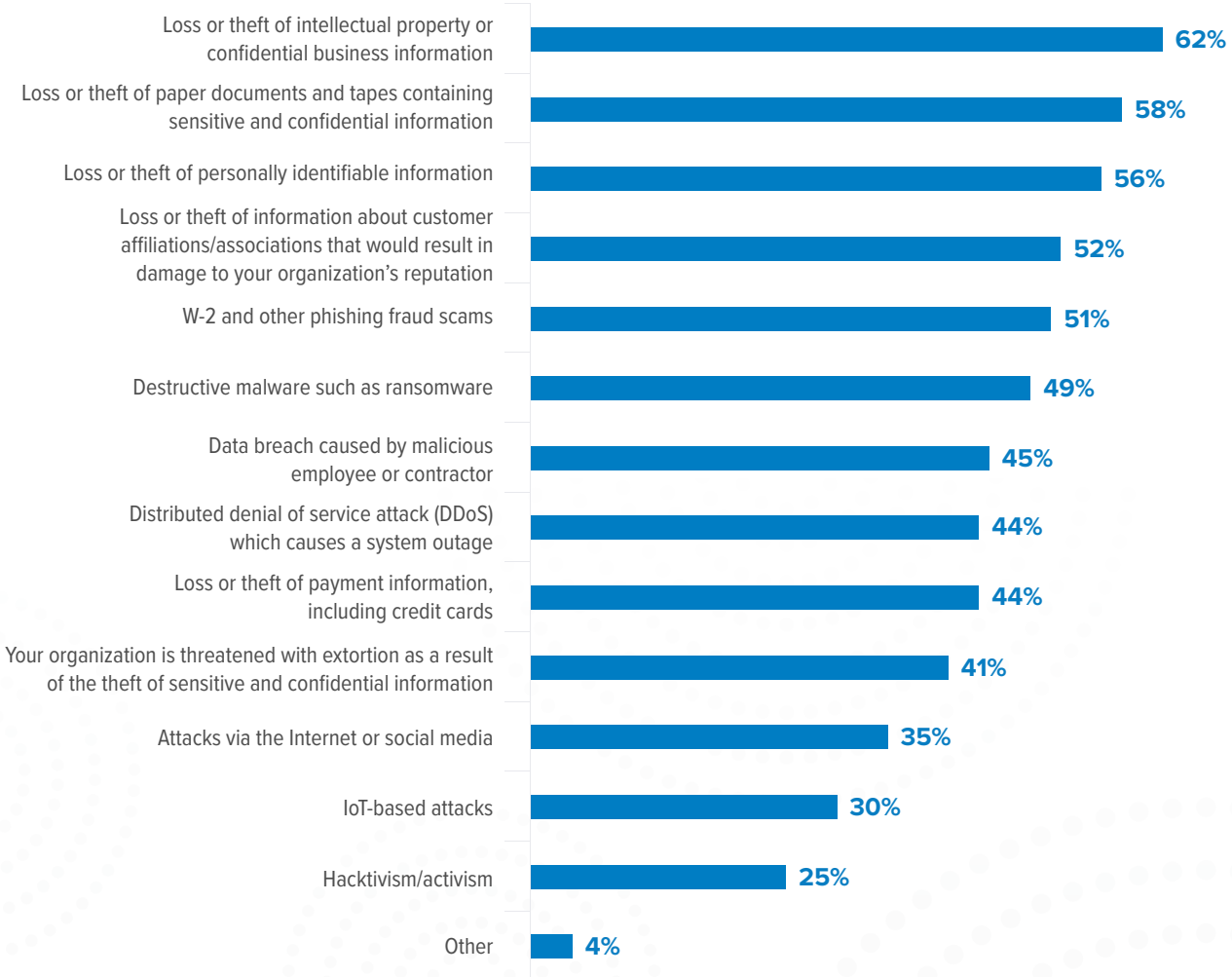


FIGURE 26 More than one response permitted

Regional Differences

In this section, the most significant differences in findings among the United States (625 respondents), EMEA (416 respondents) and Asia-Pacific (385 respondents) are presented.

US organizations are most likely to report to the board of directors. As shown in Figure 27, 45 percent of US respondents report to the board of directors. Only 29 percent of respondents in Asia-Pacific say they report to the board.

US organizations are also most likely to have a board of directors committee dedicated to cybersecurity threats and issues facing their organizations, as shown in Figure 28.

FIGURE 27 Yes responses presented

FIGURE 28 Yes responses presented

More respondents in Asia-Pacific are assuming responsibility for ensuring a strong security posture in the past year, as shown in Figure 29.

In all regions, the majority of senior leadership does not have confidence that the cybersecurity leader understands the business goals, as shown in Figure 30.

All regions are supportive of the importance of cybersecurity leaders reporting directly to the CEO because it would create greater awareness of security issues throughout the organization.

FIGURE 29 Yes responses presented

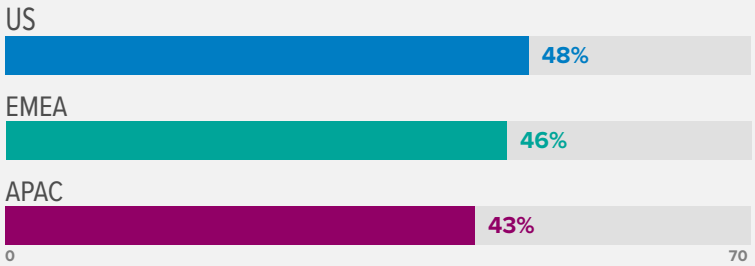


FIGURE 30 Strongly agree and Agree responses combined

FIGURE 31 Strongly agree and Agree responses combined

03

Methodology

Methodology

A sampling frame of 39,066 cybersecurity professionals in the United States, EMEA, and APAC were selected as participants to this survey. Table shows 1,581 total returns. Screening and reliability checks required the removal of 155 surveys. Our final sample consisted of 1,426 surveys or a 3.7 percent response.

Survey response	Global	US	EMEA	APAC
Sampling frame	39,066	16,704	11,590	10,772
Total returns	1,581	688	463	430
Rejected or screened surveys	155	63	47	45
Final sample	1,426	625	416	385
Response rate	3.7%	3.7%	3.6%	3.6%

Chart 1 reports the industry focus of respondents' organizations. This chart identifies financial services (17 percent) as the largest industry focus, which includes banking, investment management, insurance, brokerage, payments and credit cards. This is followed by public sector (11 percent of respondents), industrial and manufacturing (11 percent of respondents), healthcare and pharmaceuticals (10 percent of respondents), retail (10 percent of respondents), services (9 percent of respondents) and technology and software (9 percent of respondents).

As shown in Chart 2, 59 percent of respondents are from organizations with a global headcount of more than 5,000 employees.

Industry of Survey Respondents

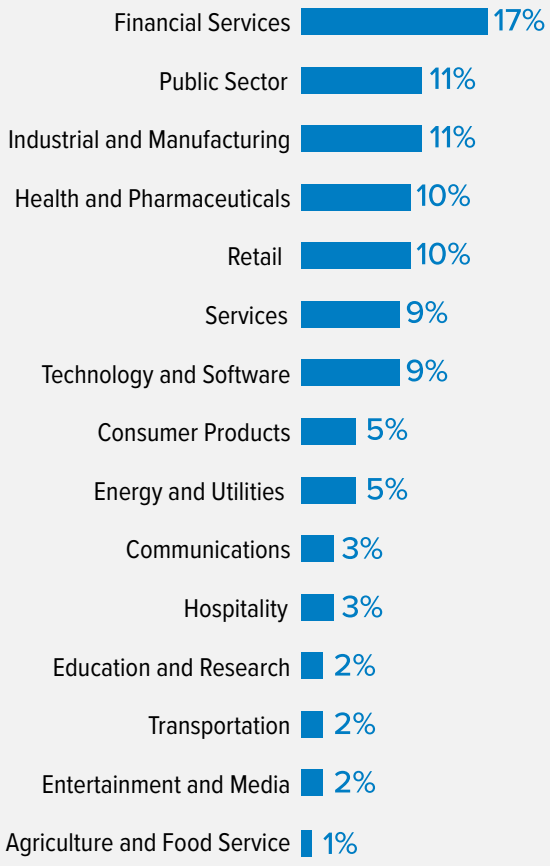


CHART 1

Headcount of Respondents' Organization

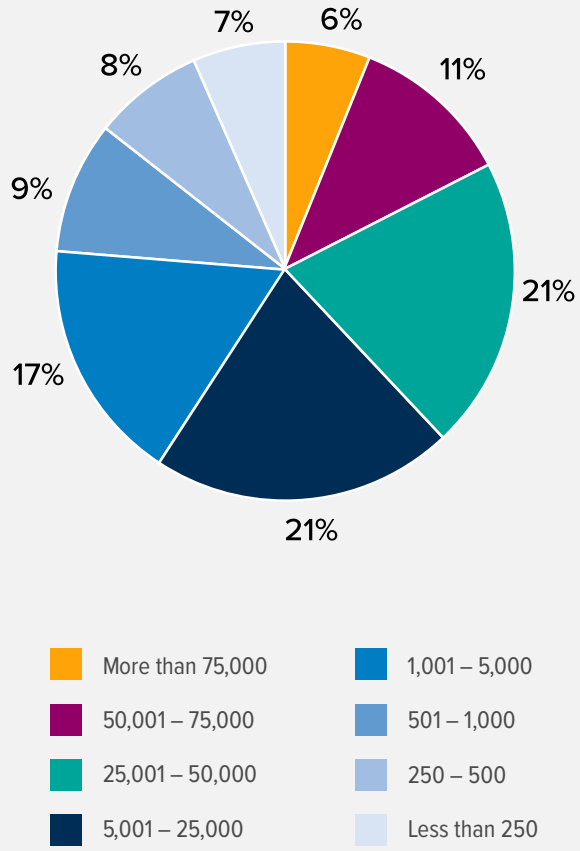


CHART 2

04

Caveats to this Study

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 are cybersecurity professionals. 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.

05

Appendix

Appendix With the Detailed Audited Findings

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 February 2021.

Survey response	Global	US	EMEA	APAC
Total sampling frame	39,066	16,704	11,590	10,772
Total returns	1,581	688	463	430
Rejected or screened surveys	155	63	47	45
Final sample	1,426	625	416	385
Response rate	3.7%	3.7%	3.6%	3.6%

Part 1. Background

Q1. What is your approximate title?	Global	US	EMEA	APAC
Chief Information Officer (CIO)	12%	11%	13%	11%
Chief Information Security Officer (CISO)	17%	19%	16%	16%
Chief Risk Officer	5%	7%	4%	4%
Chief Security Officer (CSO)	4%	3%	2%	6%
Chief Technology Officer (CTO)	11%	12%	11%	10%
General Counsel/Head of Legal	4%	3%	5%	4%
Security Administrator	8%	7%	9%	8%
Security Auditor	5%	4%	6%	5%
Security Director	11%	10%	12%	11%
Security Manager	15%	15%	13%	18%
Vice President of Security	8%	9%	7%	6%
Other	1%	0%	2%	1%
Total	**100%**	**100%**	**100%**	**100%**

Q2. How long have you held this position?	Global	US	EMEA	APAC
1 to 2 years	10%	9%	11%	9%
3 to 4 years	21%	19%	23%	23%
5 to 6 years	23%	23%	21%	25%
7 to 8 years	19%	21%	18%	17%
9 to 10	16%	18%	15%	13%
More than 10 years	11%	10%	12%	13%
Total	**100%**	**100%**	**100%**	**100%**
Extrapolated value	**6.44**	**6.55**	**6.34**	**6.39**

Q3a. To whom do you report?	Global	US	EMEA	APAC
Chief Executive Officer (CEO) (please proceed to Q4a)	7%	8%	5%	6%
Chief Financial Officer (CFO)	5%	5%	5%	4%
Chief Information Officer (CIO)	24%	21%	27%	25%
Chief Operating Officer (COO)	8%	8%	9%	8%
Chief Risk Officer (CRO)	9%	9%	8%	10%
Chief Technology Officer (CTO)	12%	11%	12%	13%
Director/Manager of IT	19%	20%	19%	18%
General Counsel/Head of Legal	4%	4%	3%	5%
VP of Information Technology	11%	12%	9%	11%
Other	2%	2%	3%	0%
Total	**100%**	**100%**	**100%**	**100%**

Q3b. If you don't report to the CEO, how many levels are you away from the CEO?	Global	US	EMEA	APAC
1	17%	23%	13%	12%
2	19%	28%	16%	9%
3	19%	21%	14%	20%
4	23%	18%	25%	30%
5	22%	10%	32%	29%
Total	**100%**	**100%**	**100%**	**100%**
Extrapolated value	**3.1**	**2.6**	**3.5**	**3.6**

Q4. Do you or someone in cybersecurity report to the Board of Directors?	Global	US	EMEA	APAC
Yes	37%	45%	31%	29%
No (please skip to Q8)	63%	55%	69%	71%
Total	**100%**	**100%**	**100%**	**100%**

Q5. How often do you or someone in cybersecurity report to the Board of Directors?	Global	US	EMEA	APAC
Annually	13%	13%	15%	12%
Bi-annually	15%	12%	18%	16%
Quarterly	30%	33%	28%	29%
Only when a security incident occurs	41%	42%	39%	43%
Total	**100%**	**100%**	**100%**	**100%**

Q6. What topics do you cover during the board meetings? Please check all that apply.	Global	US	EMEA	APAC
Any changes to the organization's security and risk posture	40%	43%	38%	36%
Changes to threats, attacks, and vulnerabilities	40%	39%	43%	40%
Effectiveness and efficiency of security programs and measures	64%	67%	63%	59%
Effectiveness of employee security training and awareness programs	45%	47%	45%	40%
Practices in place to protect the organization's high-value assets and intellectual property	48%	53%	46%	42%
Quantification of the impact to the bottom line a cyberattack or data breach would have	49%	58%	47%	38%
The security safeguards in place to protect the organization	44%	43%	41%	49%
The state of compliance with regulations	52%	50%	63%	44%
Other	5%	4%	5%	4%
Total	**387%**	**404%**	**391%**	**352%**

Q7a. Does the board of directors have a committee dedicated to cybersecurity threats and issues facing your organization?	Global	US	EMEA	APAC
Yes	29%	34%	27%	24%
No	71%	66%	73%	76%
Total	**100%**	**100%**	**100%**	**100%**

Q7b. If yes, are you or someone from cybersecurity a member of the committee?	Global	US	EMEA	APAC
Yes	43%	39%	44%	47%
No	57%	61%	56%	53%
Total	**100%**	**100%**	**100%**	**100%**

Part 2. Budget and Salary

Q8. Approximately, what range best defines your organization's 2021 IT budget?	Global	US	EMEA	APAC
< $1 million	4%	2%	4%	6%
$1 to 5 million	7%	5%	8%	9%
$6 to $10 million	14%	4%	20%	22%
$11 to $50 million	19%	12%	26%	21%
$51 to $100 million	18%	17%	14%	23%
$101 to $250 million	19%	23%	17%	15%
$251 to $500 million	12%	21%	5%	6%
> $500 million	10%	16%	6%	4%
Total	**100%**	**100%**	**100%**	**100%**
Extrapolated value (US$ million)	**$158.90**	**$232.01**	**$104.89**	**$98.56**

Q9. Approximately, what percentage of the 2021 IT budget will be allocated to security activities?	Global	US	EMEA	APAC
< 1%	2%	1%	2%	3%
1% to 2%	5%	4%	5%	7%
3% to 5%	9%	7%	10%	11%
6% to 10%	10%	9%	8%	13%
11% to 15%	13%	8%	15%	18%
16% to 20%	12%	11%	12%	14%
21% to 30%	14%	16%	13%	11%
31% to 40%	19%	19%	21%	15%
41% to 50%	11%	13%	11%	6%
> 50%	7%	12%	3%	2%
Total	**100%**	**100%**	**100%**	**100%**
Extrapolated value	**24%**	**28%**	**23%**	**18%**

Q10. How much influence do you have over the security budget?	Global	US	EMEA	APAC
Complete ownership	23%	23%	25%	19%
Significant influence	34%	35%	30%	36%
Some influence	29%	29%	28%	30%
No influence	15%	13%	17%	15%
Total	**100%**	**100%**	**100%**	**100%**

Q11. What factors would influence an increase in the security budget? Please select all that apply.	Global	US	EMEA	APAC
A cyberattack	51%	54%	51%	47%
A data breach	54%	59%	54%	46%
Changes in threats, attacks, and vulnerabilities	62%	62%	65%	60%
Compliance with regulations	45%	42%	47%	49%
Digital transformation	59%	60%	62%	55%
Growing volume of data	46%	45%	48%	47%
Merger & acquisition	32%	29%	33%	34%
Operational risk (IT, OT, IoT)	38%	39%	35%	39%
Recent security incidents	53%	51%	56%	53%
Supply chain risks	43%	46%	39%	42%
Other	4%	3%	4%	5%
Total	**488%**	**490%**	**494%**	**477%**

Q12. What are your spending priorities in 2021? Please check the top two priorities.	Global	US	EMEA	APAC
Investment in additional in-house expertise	45%	45%	43%	48%
Investment in consultants and MSSPs	29%	30%	26%	31%
Investment in technologies such as automation, AI, and machine learning	46%	43%	48%	47%
Investment in other technologies	42%	41%	44%	42%
Investment in training and awareness programs	35%	38%	36%	30%
Other	3%	3%	3%	2%
Total	**200%**	**200%**	**200%**	**200%**

Q13a. Does your organization have cyber insurance coverage?	Global	US	EMEA	APAC
Yes	47%	60%	38%	35%
No [skip to Q14]	53%	40%	62%	65%
Total	**100%**	**100%**	**100%**	**100%**

Q13b. If yes, what limits do you purchase?	Global	US	EMEA	APAC
Less than $1 million	14%	11%	17%	15%
$1 million to $5 million	28%	28%	27%	29%
$6 million to $20 million	22%	23%	21%	20%
$21 million to $100 million	26%	23%	30%	28%
More than $100 million	10%	15%	5%	8%
Total	**100%**	**100%**	**100%**	**100%**
Extrapolated value (US$ millions)	**$31.84**	**$35.73**	**$27.69**	**$30.01**

Q13c. Is your organization's cyber insurance coverage sufficient?	Global	US	EMEA	APAC
Yes	36%	38%	35%	33%
No	59%	57%	60%	63%
Unsure	5%	5%	5%	4%
Total	**100%**	**100%**	**100%**	**100%**

Q13d. How does your organization determine the level of coverage it deems adequate? Please select all that apply.	Global	US	EMEA	APAC
Formal risk assessment by in-house staff	40%	43%	34%	40%
Formal risk assessment conducted by the insurer	40%	38%	40%	42%
Formal risk assessment by third party	24%	23%	27%	23%
Informal or ad hoc risk assessment	44%	45%	41%	46%
Policy terms and conditions reviewed by a third-party specialist	54%	56%	53%	52%
Maximum available from the insurance market	49%	51%	46%	49%
Other	2%	2%	3%	2%
Total	**253%**	**258%**	**244%**	**254%**

Q13e. What types of incidents does your organization's cyber insurance cover? Please check all that apply.	Global	US	EMEA	APAC
External attacks by cyber criminals	46%	50%	43%	42%
Malicious or criminal insiders	36%	34%	36%	40%
System or business process failures	28%	27%	31%	28%
Human error, mistakes, and negligence	22%	19%	23%	24%
Incidents affecting business partners, vendors, or other third parties that have access to your company's information assets	52%	52%	54%	50%
Other	3%	4%	2%	3%
Total	**187%**	**186%**	**189%**	**187%**

Q13f. What coverage does this cyber insurance offer your organization? Please check all that apply.	Global	US	EMEA	APAC
Forensics and investigative costs	40%	41%	38%	39%
Notification costs to data breach victims	51%	57%	49%	45%
Communication costs to regulators	22%	23%	21%	23%
Employee productivity losses	18%	16%	19%	21%
Replacement of lost or damaged equipment	36%	36%	37%	35%
Revenue losses	38%	37%	41%	38%
Legal defense costs	50%	50%	52%	49%
Loss of asset value	25%	26%	28%	21%
Regulatory penalties and fines	34%	33%	34%	37%
Third-party liability	43%	41%	45%	44%
Brand damages	25%	23%	27%	25%
Other	4%	4%	5%	3%
Total	**388%**	**387%**	**396%**	**380%**

Q13g. Does your organization take any of the following steps to demonstrate its commitment to minimizing cyber risks? Please check all that apply.	Global	US	EMEA	APAC
A formal security budget	65%	65%	61%	68%
A skilled security team in place	60%	63%	55%	60%
Compliance with regulations	47%	49%	48%	44%
Employee security training and awareness programs	55%	58%	52%	52%
Investment in better security controls	60%	61%	60%	58%
Senior leadership is committed to a strong security posture	33%	34%	35%	31%
Other	3%	2%	3%	3%
Total	**322%**	**332%**	**314%**	**316%**

Q14. If your organization does not have insurance, does it plan to purchase a cyber insurance policy?	Global	US	EMEA	APAC
Yes, within the next six months	17%	18%	16%	15%
Yes, within the next year	21%	21%	20%	22%
Yes, within the next two years	29%	34%	26%	25%
No plans to purchase	31%	24%	36%	36%
Unsure	2%	3%	2%	2%
Total	**100%**	**100%**	**100%**	**100%**

Part 3. Factors affecting cybersecurity leaders

Q15a. Have you assumed more accountability and risk for ensuring a strong security posture in the past year?	Global	US	EMEA	APAC
Yes	56%	52%	59%	61%
No	44%	48%	41%	39%
Total	**100%**	**100%**	**100%**	**100%**

Q15b. If yes, how has the increased accountability and risk impacted your salary?	Global	US	EMEA	APAC
Salary has increased	48%	47%	51%	45%
Salary has remained the same	52%	53%	49%	55%
Total	**100%**	**100%**	**100%**	**100%**

Q16a. Do you receive an annual bonus?	Global	US	EMEA	APAC
Yes	70%	73%	70%	65%
No	30%	27%	30%	35%
Total	**100%**	**100%**	**100%**	**100%**

Q16b. If yes, how has your bonus changed over the past two years?	Global	US	EMEA	APAC
Increased	26%	32%	23%	21%
Stayed the same	56%	50%	59%	63%
Decreased (please skip to 17a)	17%	18%	18%	16%
Total	**100%**	**100%**	**100%**	**100%**

Q16c. If your bonus increased or stayed the same, does it offset the increased accountability and risk you have assumed in the past year?	Global	US	EMEA	APAC
Yes	55%	54%	57%	55%
No (please skip to 17c)	45%	46%	43%	45%
Total	**100%**	**100%**	**100%**	**100%**

Q17a. Do you have termination protections written into your contract?	Global	US	EMEA	APAC
Yes	59%	60%	61%	54%
No (please skip to Q18a)	41%	40%	39%	46%
Total	**100%**	**100%**	**100%**	**100%**

17b. If yes, how much is the payout associated with the termination protections?	Global	US	EMEA	APAC
$500,000 or less	3%	3%	4%	3%
$500,000 to $1,000,000	11%	12%	13%	9%
$1,000,001 to $2,000,000	19%	18%	20%	18%
$2,000,001 to $5,000,000	22%	23%	21%	20%
More than $5,000,000	45%	44%	42%	50%
Total	**100%**	**100%**	**100%**	**100%**
Extrapolated value US$ millions	**$3.83**	**$3.81**	**$3.66**	**$4.05**

Q17c. If no, would you like termination protections in your contract to offset the risk associated with your job?	Global	US	EMEA	APAC
Yes	58%	59%	57%	58%
No	42%	41%	43%	42%
Total	**100%**	**100%**	**100%**	**100%**

Q18a. Did your organization experience a cyberattack in the past two years?	Global	US	EMEA	APAC
Yes	60%	63%	59%	55%
No (please skip to Q19a)	40%	37%	41%	45%
Total	**100%**	**100%**	**100%**	**100%**

Q18b. If yes, who was held most responsible for the cyberattack against your organization?	Global	US	EMEA	APAC
The CEO	9%	9%	8%	9%
The IT security leader	23%	19%	25%	28%
Both the CEO and IT security leader	28%	35%	30%	27%
No one was held accountable	35%	34%	35%	36%
Other	2%	3%	2%	0%
Total	**100%**	**100%**	**100%**	**100%**

Q18c. Who should be held most responsible for the cyberattack against your organization?	Global	US	EMEA	APAC
The CEO	15%	15%	13%	18%
The IT security leader	42%	40%	45%	43%
Both the CEO and IT security leader	23%	24%	22%	22%
No one should be held accountable	17%	19%	17%	14%
Other	3%	2%	3%	3%
Total	**100%**	**100%**	**100%**	**100%**

Q19a. Did your organization experience a data breach in the past two years?	Global	US	EMEA	APAC
Yes	55%	58%	54%	51%
No (please skip to Q20a)	45%	42%	46%	49%
Total	**100%**	**100%**	**100%**	**100%**

Q19b. If yes, who was held most responsible for the data breach against your organization?	Global	US	EMEA	APAC
The CEO	12%	13%	12%	11%
The IT security leader	25%	25%	21%	30%
Both the CEO and IT security leader	30%	25%	37%	31%
No one was held accountable	30%	35%	26%	27%
Other	2%	2%	4%	1%
Total	**100%**	**100%**	**100%**	**100%**

Q19c. Who should be held most responsible for the data breach against your organization?	Global	US	EMEA	APAC
The CEO	22%	20%	23%	23%
The IT security leader	36%	37%	33%	39%
Both the CEO and IT security leader	22%	23%	23%	21%
No one should be held accountable	17%	18%	17%	15%
Other	3%	2%	4%	2%
Total	**100%**	**100%**	**100%**	**100%**

Q20a. Are you worried about your job security?	Global	US	EMEA	APAC
Yes	54%	61%	51%	45%
No	46%	39%	49%	55%
Total	**100%**	**100%**	**100%**	**100%**

Q20b. If yes, why? Please check all that apply.	Global	US	EMEA	APAC
Cybersecurity is not viewed as a business risk	23%	21%	23%	27%
Lack of authority to execute the IT security strategy	45%	45%	43%	48%
Lack of executive support	51%	53%	49%	51%
Senior leadership does not understand my role	53%	56%	49%	52%
The budget is insufficient to invest in the right technologies	63%	65%	63%	61%
Other	2%	3%	2%	0%
Total	**238%**	**243%**	**229%**	**239%**

Part 4. The security leader's challenges

Q21. What are the top cybersecurity risks affecting your organization? Please check your top six choices only.	Global	US	EMEA	APAC
Browser-based attacks	43%	44%	39%	45%
Cloud vulnerabilities	54%	56%	51%	53%
Denial of service attacks	52%	58%	46%	49%
Device vulnerabilities (such as IoT devices)	56%	51%	60%	58%
DNS-based attacks (such as DNS hijacking)	48%	55%	41%	45%
Fileless malware	34%	33%	39%	30%
Hardware and system failures	49%	47%	50%	52%
Malicious insider threat	18%	18%	16%	20%
Nation-state, terrorist, or criminal syndicate sponsored attacks	16%	15%	18%	17%
Negligent insider threat	44%	34%	50%	55%
Phishing/social engineering attacks	63%	62%	67%	61%
Ransomware	60%	59%	61%	59%
Remote worker endpoint security	60%	64%	60%	53%
Other	3%	4%	2%	3%
Total	**600%**	**600%**	**600%**	**600%**

Q22a. Are you able to evaluate these threats based on their ability to do the most damage to your organization such as the loss of high-value assets, fines, the loss of reputation and downtime?	Global	US	EMEA	APAC
Yes	53%	53%	56%	49%
No (please skip to Q23a)	47%	47%	44%	51%
Total	**100%**	**100%**	**100%**	**100%**

Q22b. If yes, what methods do you use to determine the potential damage?	Global	US	EMEA	APAC
NIST	47%	58%	41%	34%
MITRE ATT&CK	35%	37%	34%	33%
The Cyber Kill Chain	56%	60%	55%	51%
ISO	39%	45%	60%	48%
Other	7%	7%	8%	6%
Total	**195%**	**207%**	**198%**	**172%**

Q23a. What are your organization's biggest security challenges? Please check your top five choices only.	Global	US	EMEA	APAC
Being prepared to deal with unexpected security incidents	43%	44%	41%	43%
Ensuring compliance with privacy and security regulations	40%	43%	39%	38%
Finding and remediating vulnerabilities in software applications deployed throughout the organization	59%	60%	56%	59%
Getting better control over the data through identification and risk classification	44%	43%	49%	41%
Managing third-party risks	61%	63%	61%	56%
Preventing and mitigating security incidents that disrupt business operations	42%	41%	43%	44%
Reducing malicious insider risks	48%	46%	50%	49%
Reducing negligent insider risks	52%	52%	55%	50%
Safeguarding the organization's high value information assets, including IP	45%	47%	39%	48%
Securing the remote workforce	64%	60%	67%	69%
Other	1%	1%	0%	3%
Total	**500%**	**500%**	**500%**	**500%**

Q23b. What are the biggest organizational challenges? Please check your four choices only.	Global	US	EMEA	APAC
Decreasing costs	36%	33%	40%	36%
Having a skilled workforce	60%	54%	65%	63%
Identifying new target markets	30%	29%	32%	31%
Improving corporate culture	54%	54%	51%	56%
Improving customer experience	53%	59%	48%	50%
Improving market perception	38%	41%	32%	39%
Increasing profits	48%	42%	54%	52%
Increasing revenues	38%	45%	34%	31%
Reducing customer turnover	39%	38%	39%	40%
Other	4%	5%	5%	2%
Total	**400%**	**400%**	**400%**	**400%**

Q24. Since COVID-19, what percent of your organization's employees and contractors are working remotely?	Global	US	EMEA	APAC
Less than 10%	12%	11%	14%	12%
10% to 25%	16%	18%	11%	19%
26% to 50%	22%	21%	25%	21%
51% to 75%	27%	27%	25%	29%
76% to 100%	23%	23%	25%	19%
Total	**100%**	**100%**	**100%**	**100%**
Extrapolated value	**48%**	**49%**	**50%**	**47%**

Q25a. Does a remote workforce increase the risk to your organization's sensitive data?	Global	US	EMEA	APAC
Yes	62%	65%	60%	59%
No (please skip to Q26a)	33%	30%	34%	36%
Unsure (please skip to Q26a)	5%	5%	6%	5%
Total	**100%**	**100%**	**100%**	**100%**

Q25b. If yes, why? Please check all that apply.	Global	US	EMEA	APAC
Employees and contractors are more likely to use a personal device instead of a company-issued device	53%	59%	48%	47%
A family member is allowed to use the work device	67%	69%	67%	65%
Security protocols are not followed as closely as they are in the workplace	65%	67%	65%	63%
Less secure home networks are used	73%	74%	72%	71%
Employees and contractors believe the organization is not monitoring their activities	68%	71%	69%	63%
Other	4%	4%	5%	4%
Total	**330%**	**344%**	**326%**	**313%**

Part 5. Attributions about the security leader role

Strongly agree and Agree responses combined.		Global	US	EMEA	APAC
Q26a.	Senior leadership believes security can support business goals.	61%	65%	61%	56%
Q26b.	The cybersecurity leader should report directly to the CEO because it would create greater awareness of security issues throughout the organization.	60%	61%	58%	60%
Q26c.	The cybersecurity function is aligned with my organization's challenges as described above.	46%	49%	45%	41%
Q26d.	Senior leadership has confidence that the cybersecurity leader understands the business goals.	46%	48%	46%	43%
Q26e.	Conflicts between the priorities of the cybersecurity leader and IT leader can result in fewer resources allocated to cybersecurity.	55%	58%	52%	53%
Q26f.	My organization values and effectively leverages the expertise of the cybersecurity leader.	43%	49%	41%	37%

Part 6. Third party risks and incident response plans

Q27a. Do you evaluate the security and privacy practices of all third parties before you engage them in a business relationship that requires the sharing of sensitive or confidential information?	Global	US	EMEA	APAC
Yes	42%	44%	40%	41%
No (please skip to Q29a)	52%	50%	53%	54%
Unsure (please skip to Q29a)	6%	6%	7%	5%
Total	**100%**	**100%**	**100%**	**100%**

Q27b. If yes, how do you perform this evaluation? Please check all that apply.	Global	US	EMEA	APAC
Review written policies and procedures	52%	57%	47%	48%
Acquire signature on contracts that legally obligates the third party to adhere to security and privacy practices	50%	54%	50%	45%
Obtain indemnification from the third party in the event of a data breach	43%	48%	41%	38%
Conduct an assessment of the third party's security and privacy practices	40%	43%	39%	37%
Obtain a self-assessment conducted by the third party	42%	40%	42%	44%
Obtain references from other organizations that engage the third party	45%	44%	46%	47%
Obtain evidence of security certification such as ISO 2700/27002	43%	47%	41%	38%
Require completion of a data security questionnaire	42%	43%	40%	43%
Other	4%	3%	4%	5%
Unsure	4%	4%	5%	3%
Total	**365%**	**383%**	**355%**	**348%**

Q28a. Do you evaluate the security and privacy practices of all third-party subcontractors before permitting your third parties to share sensitive or confidential with them?	Global	US	EMEA	APAC
Yes	54%	56%	54%	49%
No (please skip to Q29a)	46%	44%	46%	51%
Total	**100%**	**100%**	**100%**	**100%**

Q28b. If yes, how do you perform this evaluation? Please check all that apply.	Global	US	EMEA	APAC
Require third parties to disclose any subcontractors with whom they will share your sensitive or confidential information	45%	49%	43%	41%
Use technologies that can reveal the identity of your third party's subcontractors	54%	57%	52%	50%
Require third parties to obtain your specific approval before they share sensitive or confidential information with a subcontractor	47%	49%	43%	48%
Require signatures on contracts that legally obligate the third party's subcontractors to adhere to security and privacy practices	50%	54%	50%	45%
Obtain indemnification from the third party's subcontractors in the event of a data breach	43%	48%	41%	38%
Conduct an assessment of the third party's subcontractors' security and privacy practices	43%	43%	44%	41%
Obtain references from other organizations that engage the third party's subcontractors	45%	44%	46%	47%
Obtain evidence that third party's subcontractors have a security certification such as ISO 2700/27002	45%	47%	42%	45%
Require completion of a data security questionnaire	49%	51%	50%	45%
Obtain evidence of security certification such as ISO 2700/27002	43%	47%	41%	40%
Other	4%	4%	5%	4%
Unsure	1%	2%	0%	0%
Total	**470%**	**495%**	**457%**	**444%**

Q29a. Does your organization have an incident response plan in place?	Global	US	EMEA	APAC
Yes (please skip to Q30)	76%	83%	69%	71%
No	24%	17%	31%	29%
Total	**100%**	**100%**	**100%**	**100%**

Q30. How often does your organization update the incident response plan?	Global	US	EMEA	APAC
Each quarter	11%	12%	9%	12%
Twice per year	10%	9%	11%	12%
Once each year	20%	19%	20%	23%
No set time period for reviewing and updating the plan	34%	35%	34%	31%
We have not reviewed or updated since the plan was put in place	24%	25%	26%	22%
Total	**100%**	**100%**	**100%**	**100%**

Q31. Does your organization take any of the following additional steps to prepare? Please check all that apply.	Global	US	EMEA	APAC
Conduct background checks on new full-time employees and vendors	48%	47%	49%	47%
Conduct third-party cyber security assessments	42%	43%	40%	41%
Create a “standby website” for content that can be made live when an incident occurs	48%	51%	49%	43%
Document and practice the incident response plan	54%	53%	55%	56%
Integrate data breach response into business continuity plans	45%	46%	47%	42%
Meet with law enforcement and/or state regulators in advance of an incident	23%	21%	28%	19%
Regularly review physical security and access to confidential information	43%	44%	43%	43%
Subscribe to a dark web monitoring service	43%	43%	40%	46%
Other	1%	1%	0%	1%
Total	**347%**	**349%**	**351%**	**338%**

Q32. Does your incident response plan include the following requirements? Please check all that apply.	Global	US	EMEA	APAC
Contact information for all members of the incident response team	51%	55%	51%	44%
Procedures for communicating with employees when an incident occurs	58%	56%	62%	58%
Procedures for communicating with state attorneys general and regulators	78%	78%	81%	73%
Procedures for communications with business partners and other third parties	76%	79%	77%	69%
Procedures for communications with investors	61%	60%	63%	59%
Procedures for incorporating findings from the forensics investigations into the security strategy	60%	55%	67%	60%
Procedures for reporting results of the forensics investigation to senior management	46%	49%	46%	42%
Procedures for responding to a incident involving overseas locations	30%	31%	29%	30%
Required C-level approval of the incident response plan	83%	88%	80%	79%
Review of a third party or business partner's incident response plan	81%	84%	78%	80%
Other	5%	5%	4%	5%
Total	**628%**	**640%**	**638%**	**599%**

Q33. Does your incident response plan offer guidance on managing the following security incidents? Please check all that apply.	Global	US	EMEA	APAC
Attacks via the Internet or social media	35%	34%	37%	34%
Data breach caused by a malicious employee or contractor	45%	45%	44%	47%
Destructive malware such as ransomware	49%	51%	46%	48%
Distributed denial of service attack (DDoS) which causes a system outage	44%	48%	42%	41%
Hacktivism/activism	25%	27%	23%	25%
IoT-based attacks	30%	29%	31%	30%
Loss or theft of information about customer affiliations/associations that would result in damage to your organization's reputation	52%	56%	50%	46%
Loss or theft of intellectual property or confidential business information	62%	59%	65%	63%
Loss or theft of paper documents and tapes containing sensitive and confidential information	58%	60%	50%	62%
Loss or theft of payment information, including credit cards	44%	43%	41%	50%
Loss or theft of personally identifiable information	56%	61%	56%	49%
W-2 and other phishing fraud scams	51%	50%	55%	49%
Your organization is threatened with extortion as a result of the theft of sensitive and confidential information	41%	43%	41%	38%
Other	4%	5%	3%	4%
Total	**596%**	**611%**	**584%**	**586%**

Part 7. Organizational characteristics

D1. What industry best describes your organization's industry focus?	Global	US	EMEA	APAC
Agriculture & food service	1%	1%	1%	0%
Communications	3%	3%	3%	4%
Consumer products	5%	5%	6%	5%
Defense & aerospace	0%	1%	0%	0%
Education & research	2%	2%	1%	4%
Energy & utilities	5%	4%	5%	6%
Entertainment & media	2%	2%	2%	2%
Financial services	17%	18%	16%	15%
Health & pharmaceuticals	10%	11%	9%	10%
Hospitality	3%	2%	3%	3%
Industrial & manufacturing	11%	11%	12%	10%
Public sector	11%	12%	11%	11%
Retail	10%	9%	10%	10%
Services	9%	9%	10%	9%
Technology & software	9%	8%	9%	10%
Transportation	2%	2%	2%	1%
Other	0%	0%	0%	0%
Total	**100%**	**100%**	**100%**	**100%**

D2. What is the worldwide headcount of your organization?	Global	US	EMEA	APAC
Less than 250	7%	4%	8%	9%
250 to 500	8%	7%	9%	8%
501 to 1,000	9%	9%	11%	8%
1,001 to 5,000	17%	19%	15%	16%
5,001 to 25,000	21%	21%	23%	20%
25,001 to 50,000	21%	20%	19%	23%
50,001 to 75,000	11%	12%	10%	12%
More than 75,000	6%	8%	5%	4%
Total	**100%**	**100%**	**100%**	**100%**

For more information about this study, please contact Ponemon Institute by sending an email to **research@ponemon.org** or call at **1.800.887.3118**.

About LogRhythm

LogRhythm's award-winning NextGen SIEM Platform makes the world safer by protecting organizations, employees, and customers from the latest cyberthreats. It does this by providing a comprehensive platform with the latest security functionality, including security analytics; network detection and response (NDR); user and entity behavior analytics (UEBA); and security orchestration, automation, and response (SOAR).

Learn how LogRhythm empowers companies to be security first at logrhythm.com.

About 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 quality standards to ensure that subjects are not asked extraneous, irrelevant or improper questions.

LogRhythm®

1.866.384.0713 // info@logrhythm.com // 4780 Pearl East Circle, Boulder CO, 80301