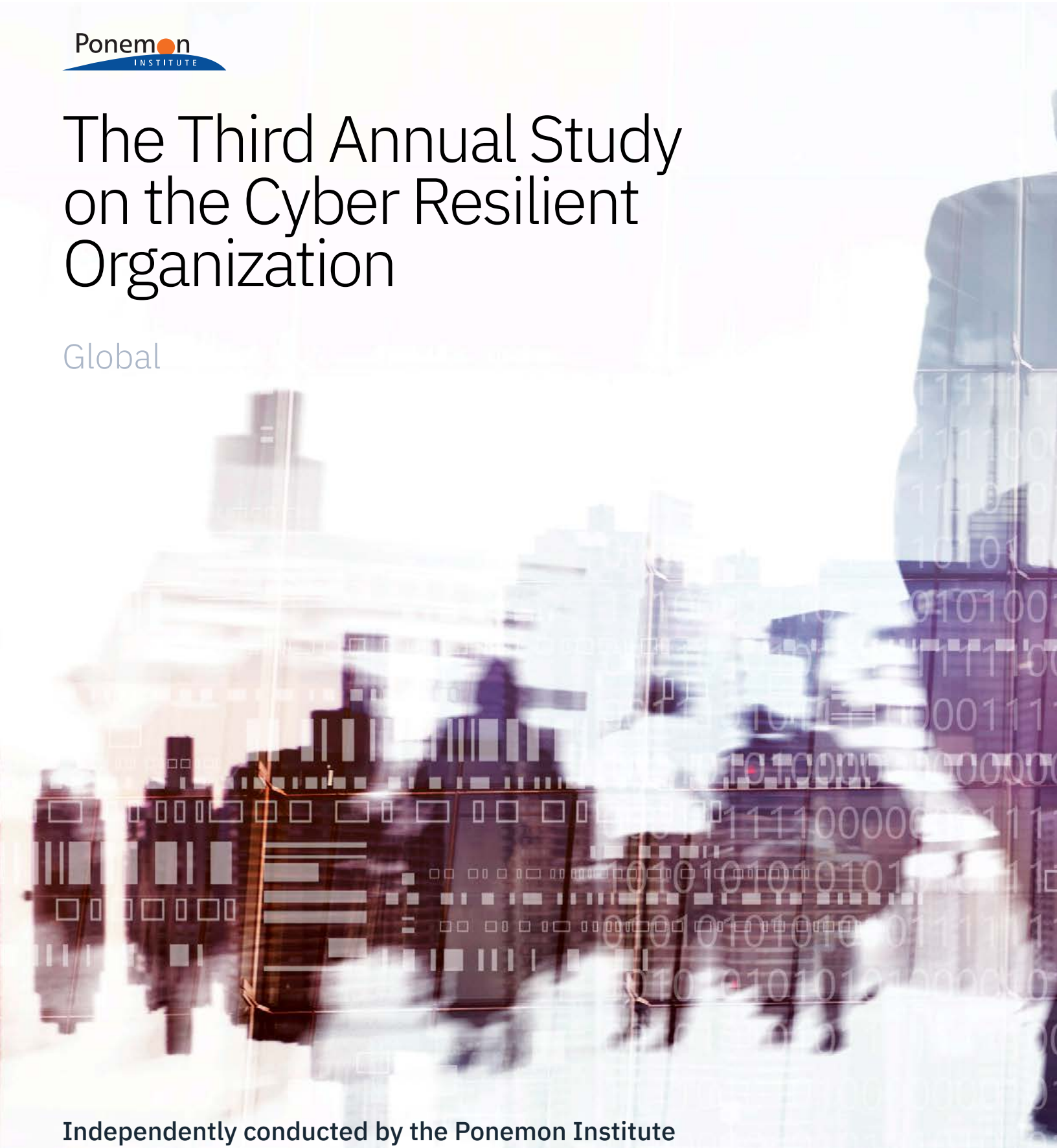
Ponemon INSTITUTE

The Third Annual Study on the Cyber Resilient Organization

Global



Independently conducted by the Ponemon Institute

Sponsored by IBM Resilient
Publication Date: March 2018

IBM Security

The Third Annual Study on the Cyber Resilient Organization

Ponemon Institute, March 2018

Part 1. Introduction

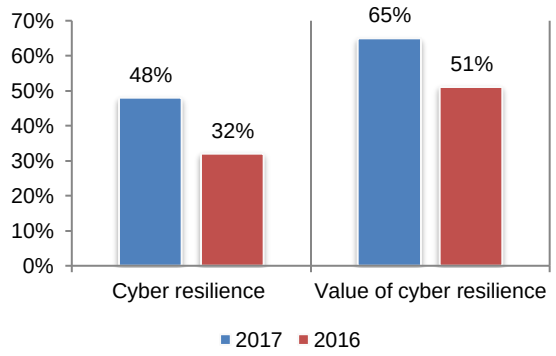
The Ponemon Institute and IBM Resilient are pleased to release the findings of the third annual study on the importance of cyber resilience for a strong security posture. *The key takeaway from this year's research is that organizations globally continue to struggle with responding to cybersecurity incidents. Lack of formal incident response plans and insufficient budgets were reported as the main causes of this challenge.*

In the context of this research, we define cyber resilience as the alignment of prevention, detection and response capabilities to manage, mitigate and move on from cyber attacks. This refers to an enterprise's capacity to maintain its core purpose and integrity in the face of cyber attacks. A cyber resilient enterprise is one that can prevent, detect, contain and recover from a myriad of serious threats against data, applications and IT infrastructure.

More than 2,848 IT and IT security professionals from around the world[1] were surveyed and despite these challenges, almost half (48 percent) rate their organizations' cyber resilience as high or very high, a significant increase from 32 percent of respondents in the 2016 study, as shown in Figure 1. Respondents' perceptions about the value of cyber resilience to their organizations also increased significantly.

Figure 1. The value and level of cyber resilience increases significantly

1 = low to 10 = high, 7+ responses reported



Major challenges to achieving Cyber Resilience remain

Companies represented in this research revealed that there are a number of areas that hinder effective and efficient incident response. Chief among them is that 77 percent of organizations admit they do not have a formal cybersecurity incident response plan (CSIRP) that is applied consistently across the organization. The report also found that just 31 percent of respondents feel that they have an adequate cyber resilience budget in place.

Other important factors that highlight the challenges faced by security practitioners in this year's research include:

- 57 percent of respondents said the time to resolve an incident has increased
- 65 percent reported the severity of attacks has increased
- Lack of investment in AI and machine learning, important new tools for cyber resilience, was ranked as the biggest barrier to cyber resilience, and investment in this area was ranked as the lowest priority for the next 12 months
- Having insufficient skilled personal dedicated to cybersecurity was the second biggest barrier to cyber resilience, with only 29 percent having the ideal staffing level.

[1] Countries represented in this study are United States, United Kingdom, France, Germany, Australia, United Arab Emirates and Brazil.

Following are steps that would improve organizations' cyber resilience.

- Increase staffing of the IT security function. The average FTE is 39, and respondents believe that the average FTE should be 55 in order to achieve a higher level of cyber resilience.
- Expand the influence and involvement of the CSIRPs to be enterprise-wide.
- Invest in such technologies as automation, machine learning artificial intelligence and orchestration that will help address the increase in the severity and volume of cyber attacks and the difficulty in hiring skilled IT security practitioners.
- Increase funding for cyber resilience activities to be able to hire and retain qualified professionals and invest in technologies.
- Take steps to reduce the time to detect, contain and respond to cyber attacks.

The study also provides a deeper analysis into the practices of those companies that have a very high level of cyber resilience and compare them to organizations that believe they have achieved only an average level of cyber resilience. The most salient differences between the two groups include the following.

- **More mature cybersecurity programs and activities**. Sixty-nine percent of high performers vs. 53 percent of overall respondents have a mature cybersecurity program with most or all activities deployed across the enterprise.
- **Greater ability to prevent, detect, contain and respond to a cyber attack.** High performing organizations have a greater ability to prevent, detect, contain and respond to a cyber attack (72 percent vs. 55 percent, 68 percent vs. 52 percent, 61 percent vs. 50 percent and 67 percent vs. 54 percent, respectively).
- **Fewer data breaches and cybersecurity incidents**. Highly cyber resilient organizations are far less likely to have a data breach (48 percent of high performing organizations vs. 56 percent of overall respondents) and cybersecurity incidents (40 percent of high performing organizations vs. 55 percent of overall respondents)
- **Fewer disruptions to businesses processes or IT services**. High performing organizations are less likely to have disruptions to business processes or IT services (30 percent of high performing organizations vs. 45 percent of overall respondents).
- **More likely to share information about data breaches with government and industry peers.** Sixty-seven percent of high performers are involved in sharing intelligence while 57 percent of overall respondents share intelligence.
- **Better support from senior management for cyber resilience**. Senior management in high performing organizations are more likely to recognize the impact cyber resilience has on brand, reputation and revenues. They are also more likely to recognize the enterprise risks that affect cyber resilience.

Part 2. Key findings

In this section of the report, we provide an analysis of the key findings. The complete audited findings are presented in the Appendix of this report. We have organized the findings according to the following topics.

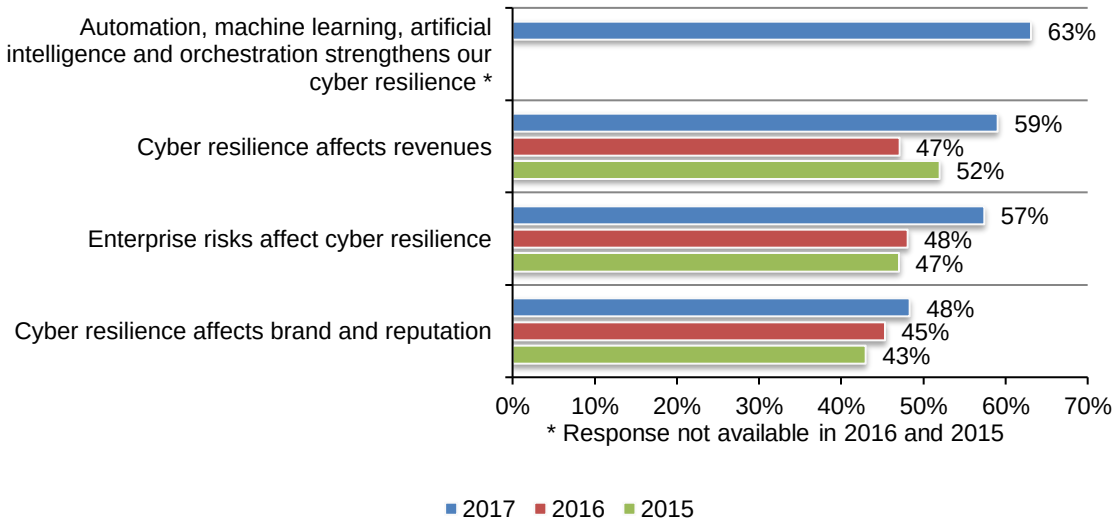
- Cyber resilience effectiveness increases significantly
- Hurdles to further improvement in cyber resilience
- Technologies & governance practices to support cyber resilience
- The characteristics of organizations with a high degree of cyber resilience
- Country differences

Cyber resilience effectiveness increases significantly

More respondents believe senior management recognizes the value of cyber resilience. According to Figure 2**,** since 2015, recognition among senior leadership about how enterprise risks affect their organizations' ability to withstand cyber attacks has increased significantly from 47 percent to 57 percent of respondents. They also are more aware that cyber resilience affects revenues, brand and reputation. Sixty-three percent of respondents say their leaders understand that automation, machine learning, artificial intelligence and orchestration strengthens cyber resilience.

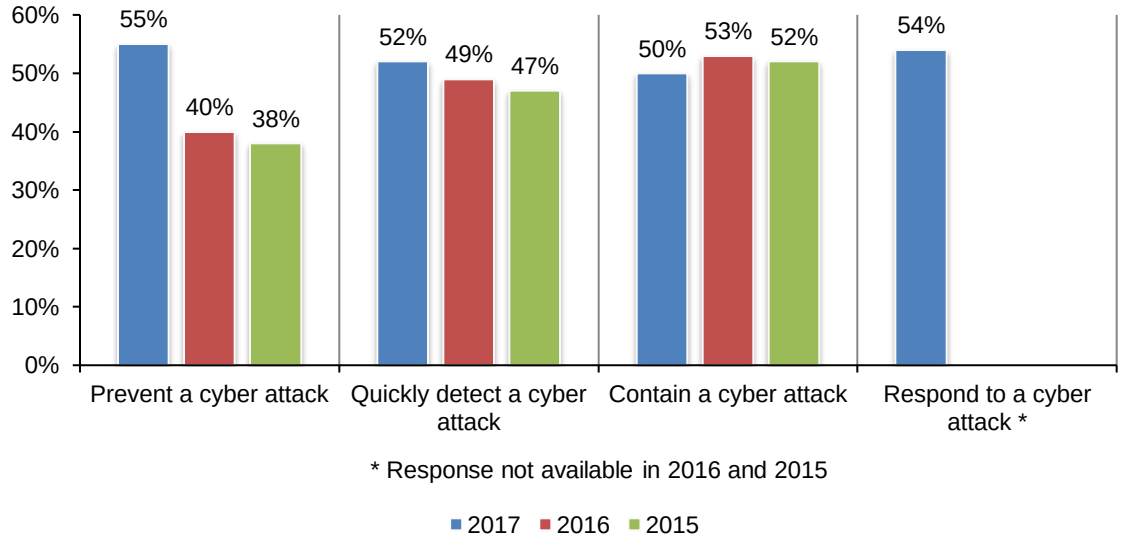
Figure 2. Senior management's awareness about the positive impact of cyber resilience on the enterprise

Strongly agree and Agree responses combined



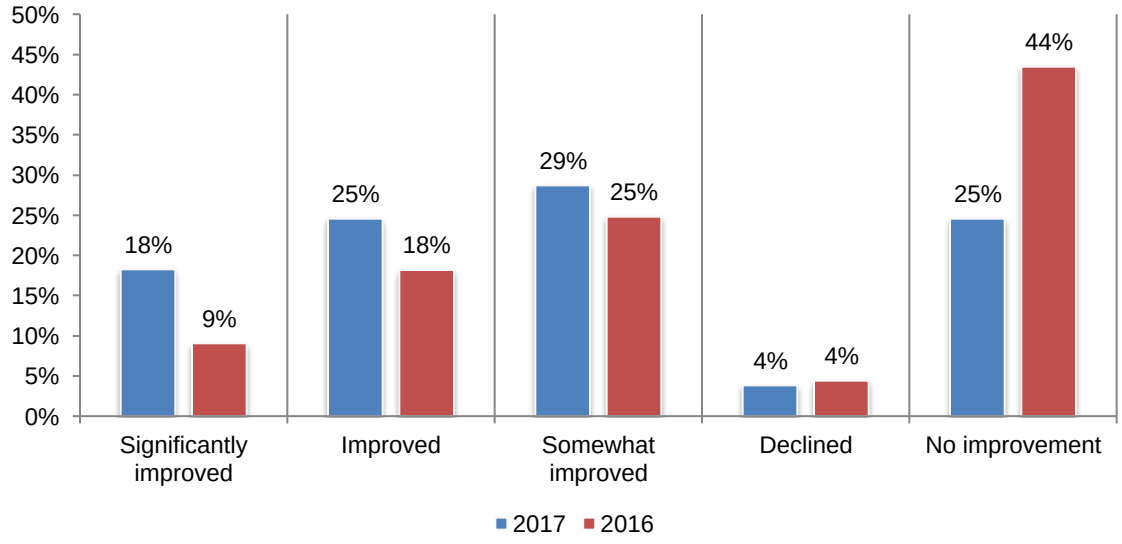
More companies are succeeding in improving their cyber resilience. As shown in Figure 3, respondents are rating their ability to prevent, detect and contain a cyber attack as much higher than in previous years. Fifty-four percent of respondents rate their ability to respond to a cyber attack as high or very high.

Figure 3. Ability to prevent, detect and contain a cyber attack improves
1 = low ability to 10 = high ability, 7+ responses reported



Seventy-two percent of respondents say their organizations' cyber resilience has improved over the past 12 months. In last year's study, 52 percent of respondents said their organizations' cyber resilience improved.

Figure 4. How has your organization's cyber resilience changed in the past 12 months?



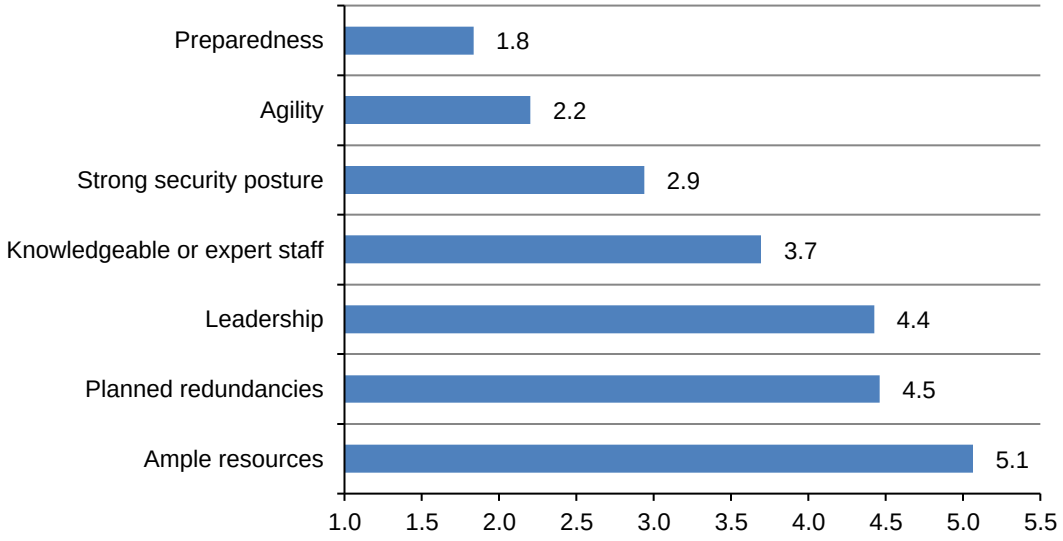
Reasons for improvement include hiring skilled personnel (61 percent of respondents), improved information governance practices (60 percent of respondents) and visibility into applications and data assets (57 percent of respondents), as shown in Figure 5.

Figure 5. Why did your organization's cyber resilience improve?
Four choices allowed

Preparedness, agility and strong security posture are the most important factors to achieving a high level of cyber resilience. Respondents were asked to rate the most important factors for achieving cyber resilience. According to Figure 6, preparedness and agility are the most important. Planned redundancies have increased in importance over the past three years.

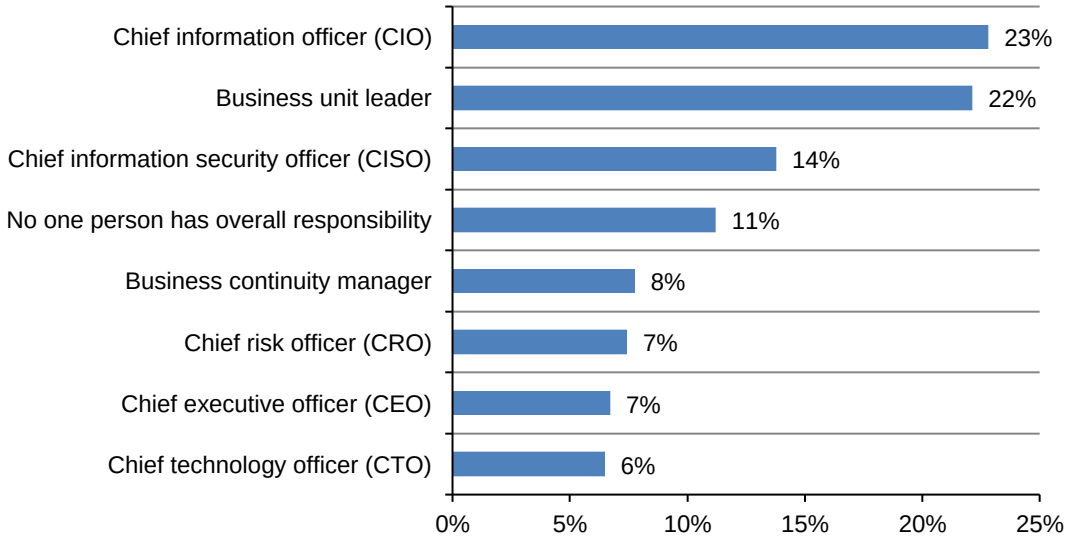
Figure 6. The seven factors considered important in achieving a high level of cyber resilience

1 = most important to 7 = least important



IT and IT security are responsible for ensuring a high level of cyber resilience. Figure 7 presents the functions with overall responsibility for the strength of their organizations' cyber resilience activities. If you combine the chief information officer (23 percent of respondents), chief technology officer (6 percent) and chief information security officer (14 percent of respondents), 43 percent of respondents say the overall responsibility for cyber resilience resides in the IT and IT security function.

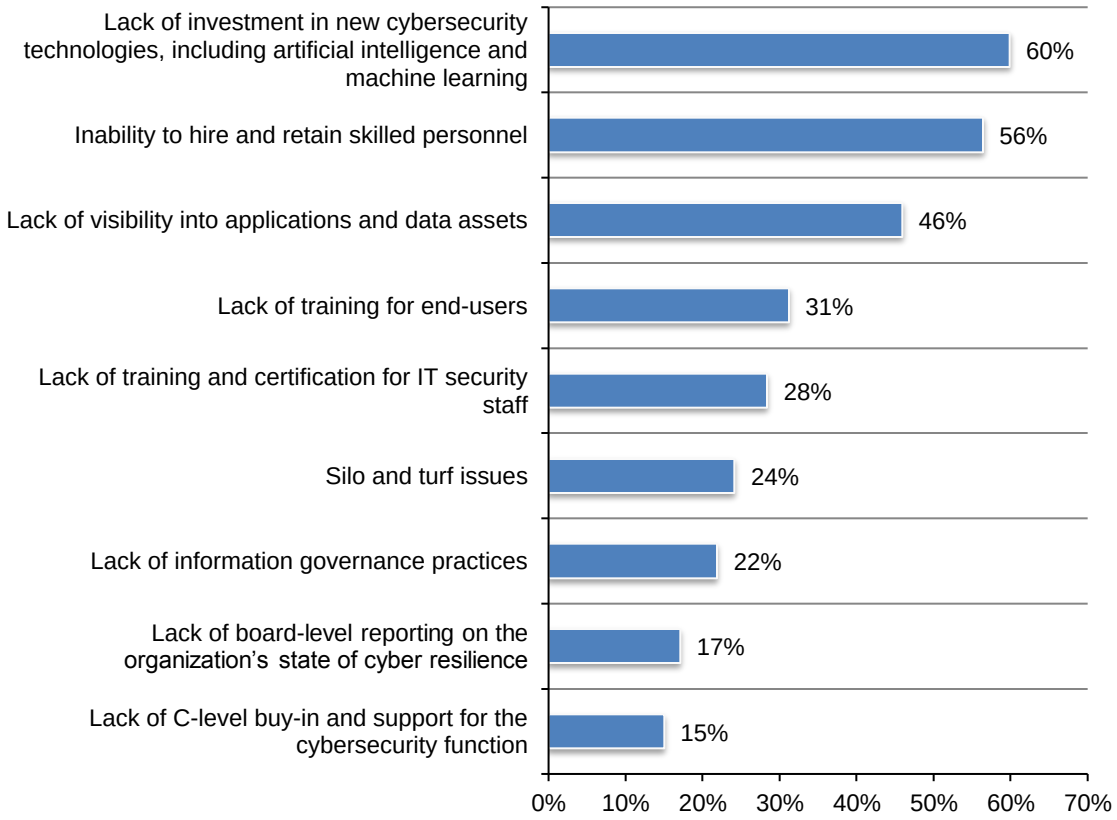
Figure 7. Who has overall responsibility for directing your organization's efforts to ensure a high level of cyber resilience?



Hurdles to further improvements in cyber resilience

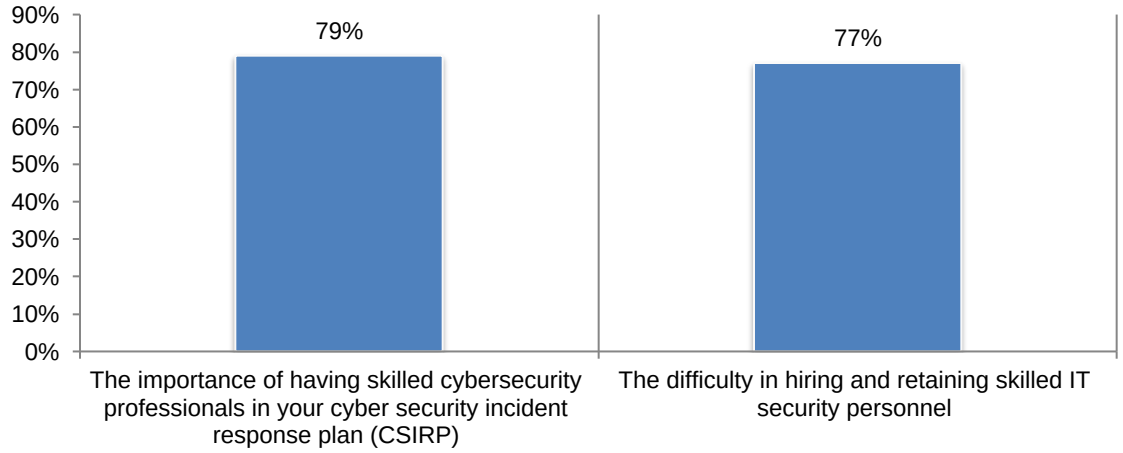
Cybersecurity technologies and skilled personnel are critical to a high level of cyber resilience. Lack of investment in new cybersecurity technologies, including artificial intelligence and machine learning, and the inability to hire and retain skilled personnel are the biggest barriers to cyber resilience, as shown in Figure 8.

Figure 8. What are the biggest barriers to cyber resilience?
Three choices allowed



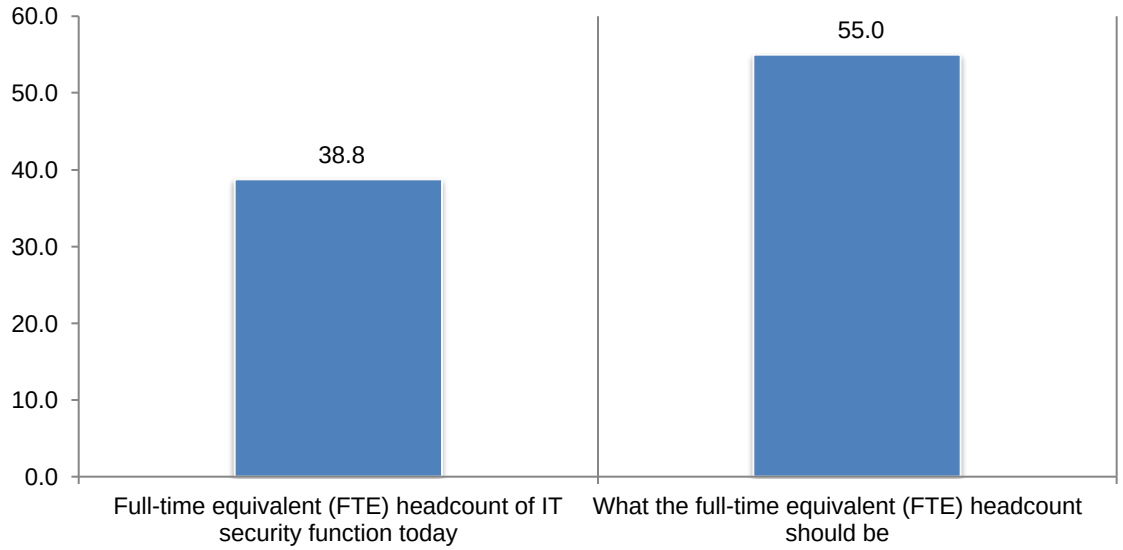
Hiring and retaining skilled IT security personnel is a serious hurdle to overcome to improving cyber resilience. Seventy-nine percent of respondents rate the importance of having skilled cybersecurity professionals in your cybersecurity response plan (CSIRP) as high or very high. However, 77 percent of respondents rate the difficulty in hiring and retaining skilled IT security personnel as very high, as shown in Figure 9.

Figure 9. The importance and difficulty in hiring skilled cybersecurity personnel
1 = low to 10 = high, 7+ responses reported



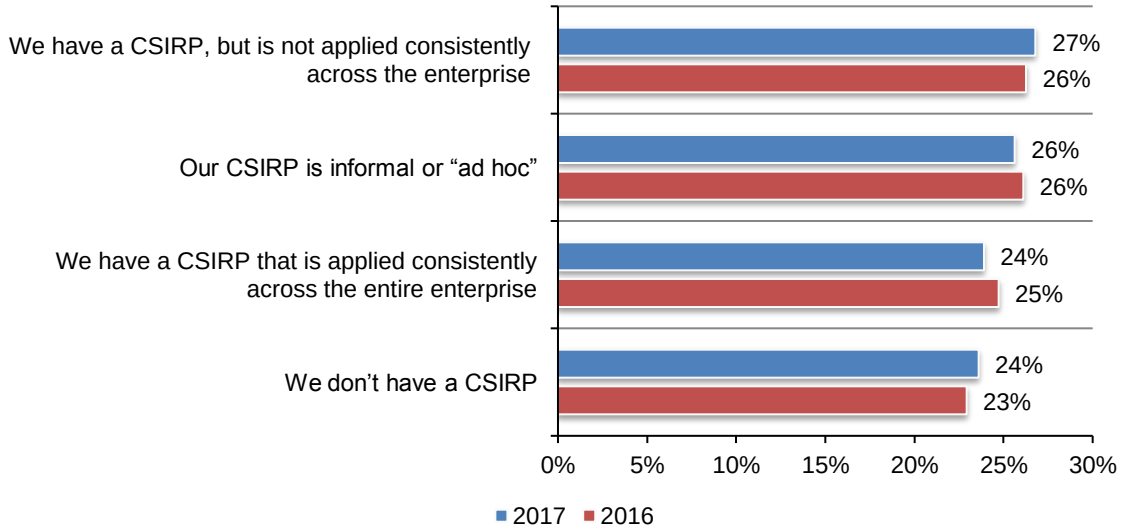
Staffing is inadequate. In fact, only 29 percent of respondents agree that in their organization, staffing for IT security is sufficient to achieve a high level of cyber resilience. As shown in Figure 10, the ideal average FTE should be 55 full-time security professionals.

Figure 10. Average full-time headcount today and what it should be
Extrapolated average



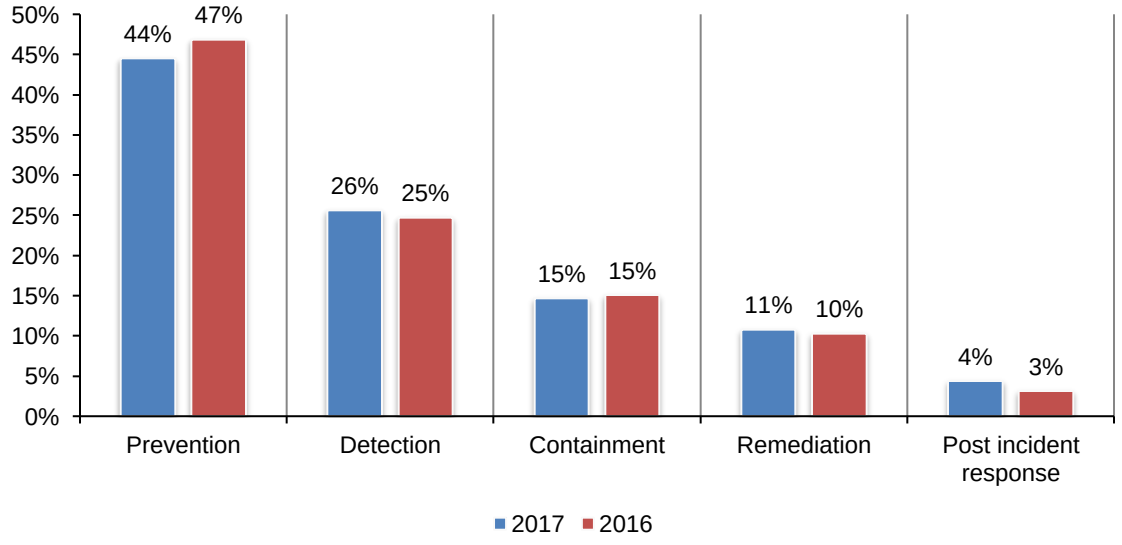
Incident response plans often do not exist or are "ad hoc." According to Figure 11**,** only 24 percent of respondents say they have a CSIRP that is applied consistently across the enterprise. If they do have a CSIRP 39 percent of respondents say there is no set time period for reviewing and updating the plan, and 34 percent of respondents say they review once each year.

Figure 11. What best describes your organization's cyber security incident response plan?



Prevention and detection CSRIP activities receive the most investment. As discussed previously, companies have significantly improved their ability to prevent and detect cyber attacks. These are the areas that receive the greatest amount of funding (44 percent and 26 percent, respectively).

Figure 12. Allocation of investment to five areas of a CSIRP

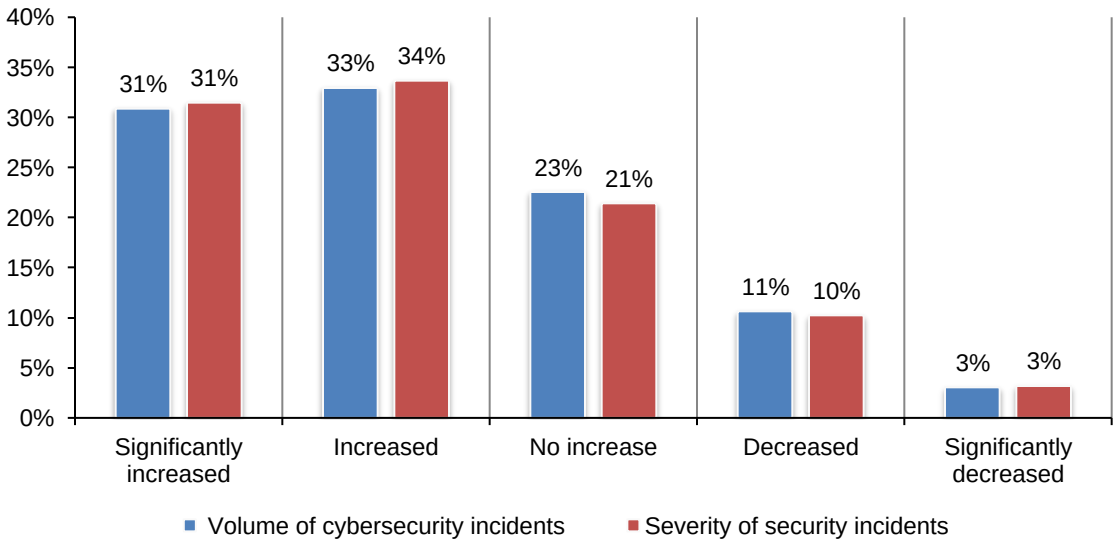


Funding decreases for cybersecurity and cyber resilience budgets. Only 31 percent of respondents say funding for IT security is sufficient to achieve a high level of cyber resilience. As shown in Table 1, the average budget for cyber resilience remains unchanged since last year at $3.4 million.

Table 1. Budget for cybersecurity & cyber resilience activities			
Extrapolated average (millions)	2017	2016	2015
Cybersecurity budget	$11.3	11.4	15.0
Percentage allocated to cyber resilience activities	30%	30%	26%
Total average budget allocated to cyber resilience	$3.4	$3.4	$3.9

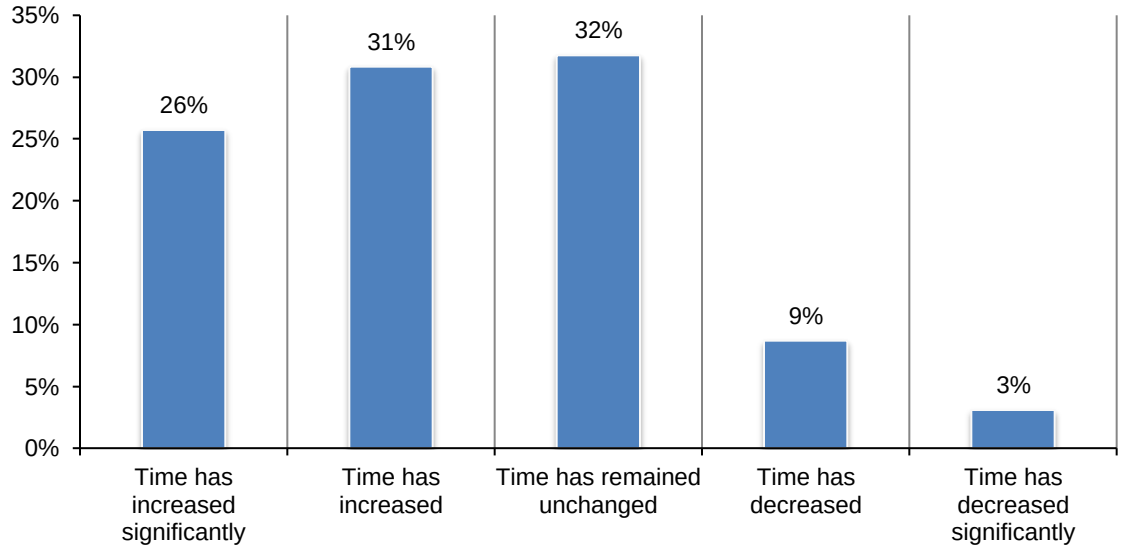
The severity and volume of cybersecurity incidents increases the time to resolve a security incident. As shown in Figure 13, 64 percent of respondents say the volume has increased (31 percent + 33 percent) and 65 percent (31 percent + 34 percent) say the severity has increased.

Figure 13. How has the volume and severity of security incidents changed in the past 12 months?



The increase in volume and severity has had a negative effect on the time to resolve a cyber incident has increased significantly. According to Figure 14, Fifty-seven percent of respondents say the time has increased significantly (26 percent) or increased (31 percent).

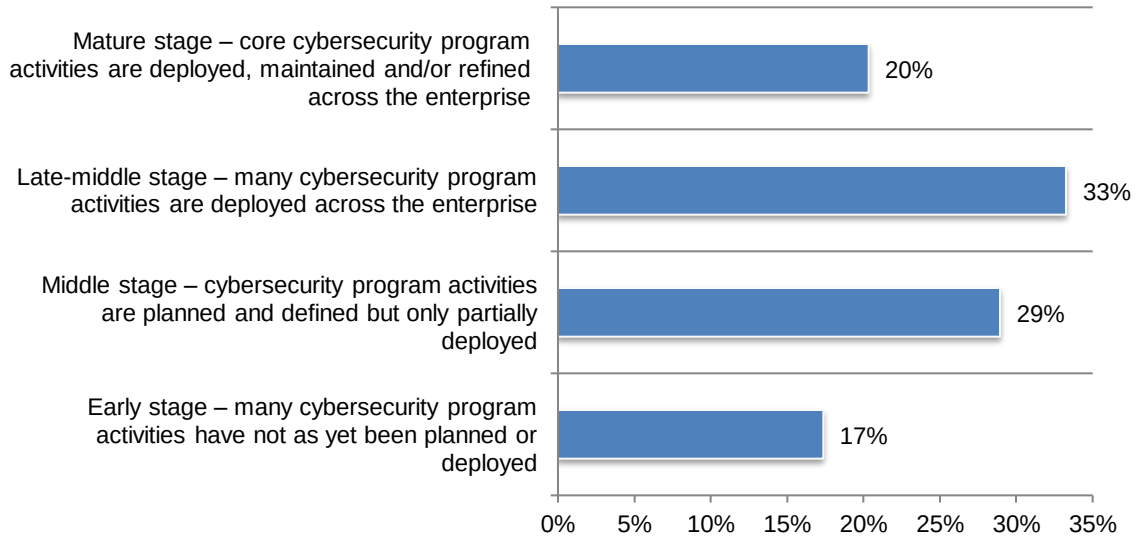
Figure 14. In the past 12 months, how has the time to detect, contain and respond to a cyber crime changed?



Technologies & governance practices to support cyber resilience

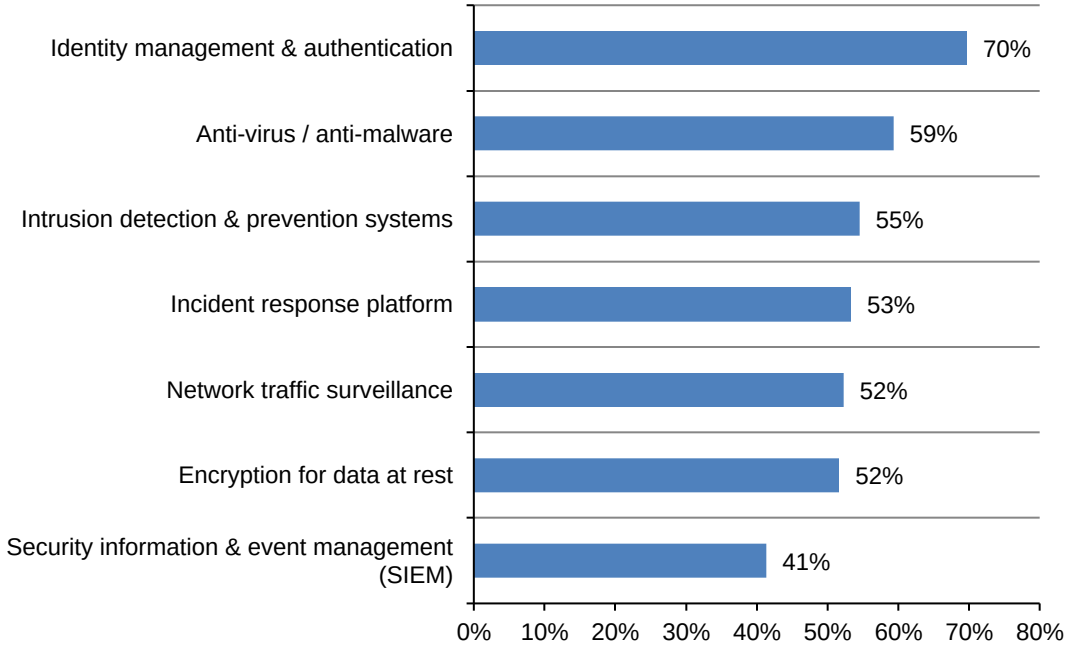
More than half of companies represented in this study have deployed many of their core cybersecurity program activities. As shown in Figure 15, 53 percent of respondents say the maturity of their cybersecurity program is late-middle or mature stage.

Figure 15. What best describes the maturity level of your organization's cybersecurity program or activities?



Identity management & authentication technologies are key to achieving a high level of cyber resilience. In addition to people and processes, the right technologies are essential for achieving cyber resilience. As shown in Figure 16, the seven most effective technologies for achieving cyber resilience are: identity management and authentication, anti-virus/anti-malware, intrusion detection and prevention systems, incident response platforms and network traffic surveillance.

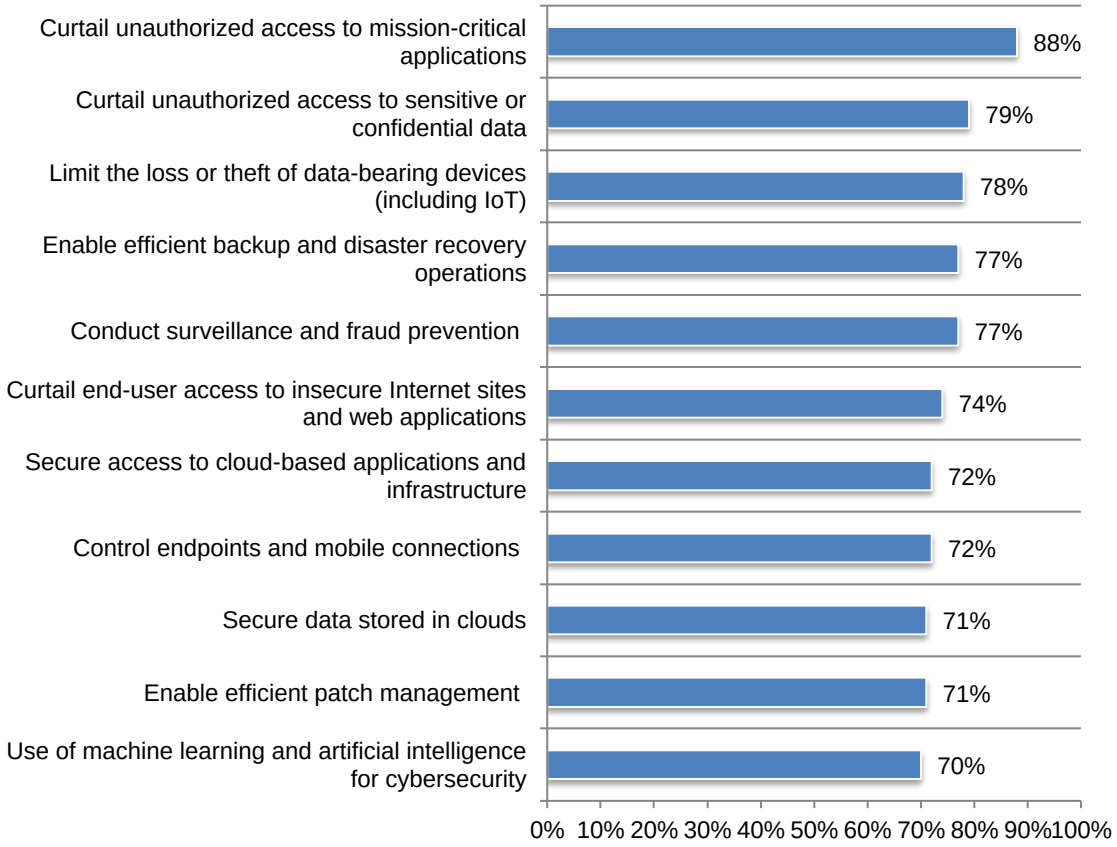
Figure 16. The seven most effective security technologies
Twenty-one technologies were listed in the survey instrument



Concerns about cyber attacks against mission-critical applications or sensitive data is driving the implementation of certain technologies. Curtailing unauthorized access to mission-critical applications and sensitive or confidential data are the most important cybersecurity activities (88 percent and 79 percent of respondents, respectively), as shown in Figure 17. Other top cybersecurity activities are those that limit the loss or theft of data-bearing devices (including IoT), efficient backup and disaster recovery operations and surveillance and fraud prevention (78 percent, 77 percent and 77 percent of respondents, respectively).

Figure 17. The top cybersecurity activities implemented or to be implemented in the next 12 months

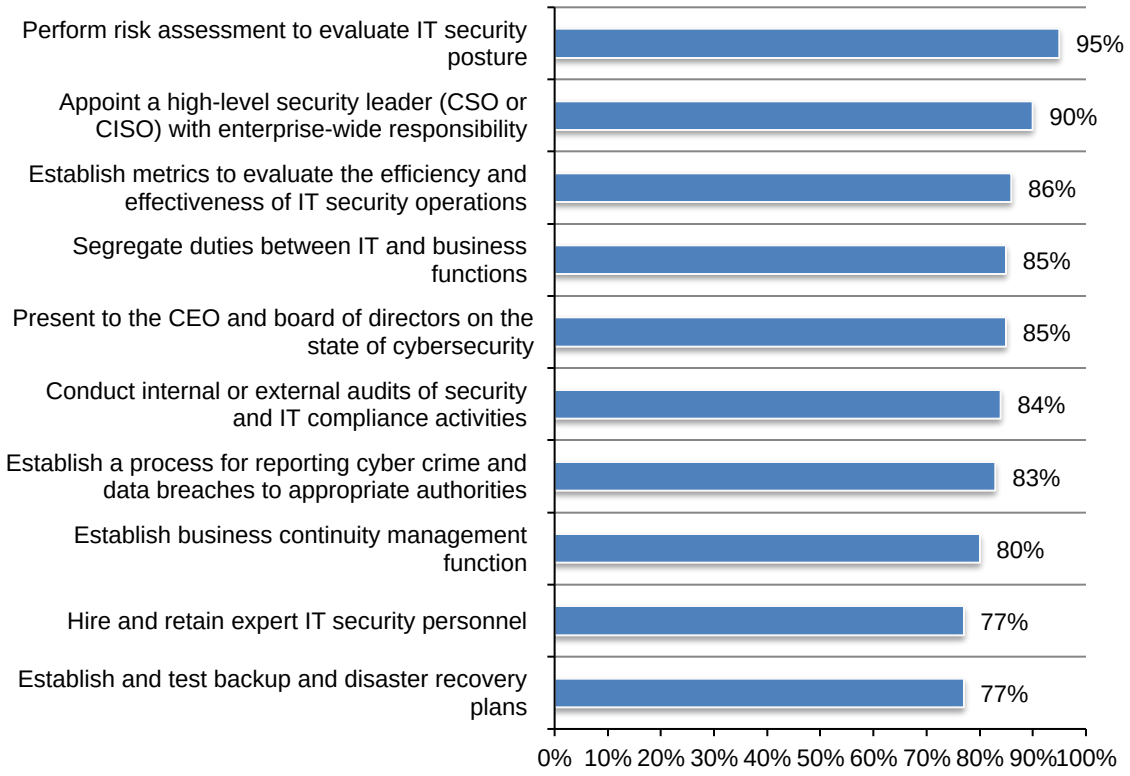
Implemented and plan to implement in the next 12 months responses combined



Risk assessments and CISOs with enterprise-wide responsibility are considered the most important governance practices to achieve cyber resilience. The most important governance activities are those that help organizations understand their security posture, which is considered important to cyber resilience. These are performing risk assessments to evaluate IT security posture (95 percent of respondents) and establish metrics to evaluate the efficiency and effectiveness of IT security operations (86 percent of respondents). Also critical to cyber resilience is the appointment of a high-level security leader with enterprise-wide responsibility.

Figure 18. The top cybersecurity governance practices implemented or to be implemented within the next 12 months

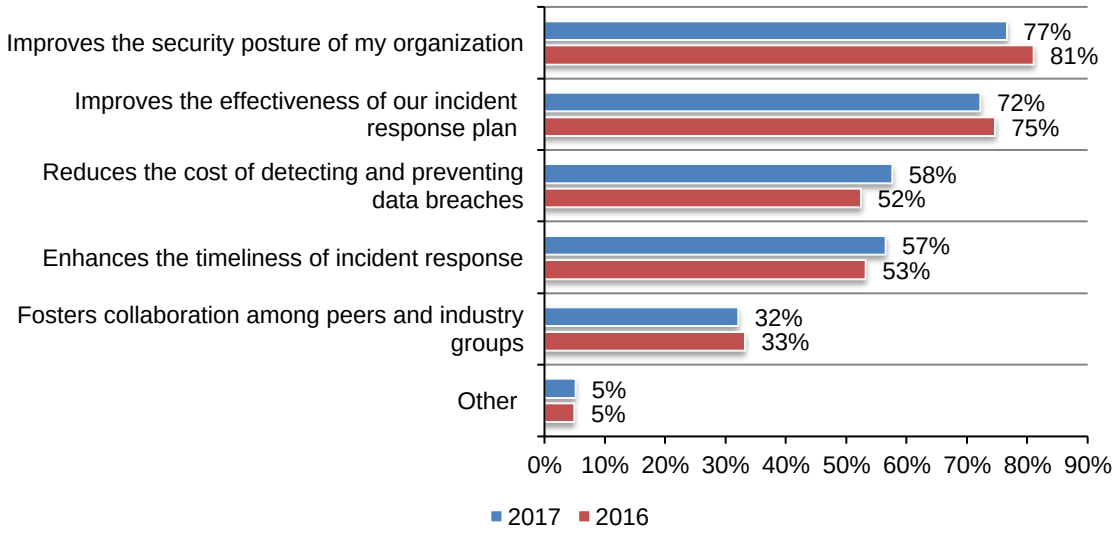
Implemented and plan to implement in the next 12 months responses combined



Having an incident response platform and sharing threat intelligence are considered key initiatives to improving cyber resilience. Fifty-three percent of respondents say their organizations participate in an initiative or program for sharing information with government and industry peers about data breaches and incident response.

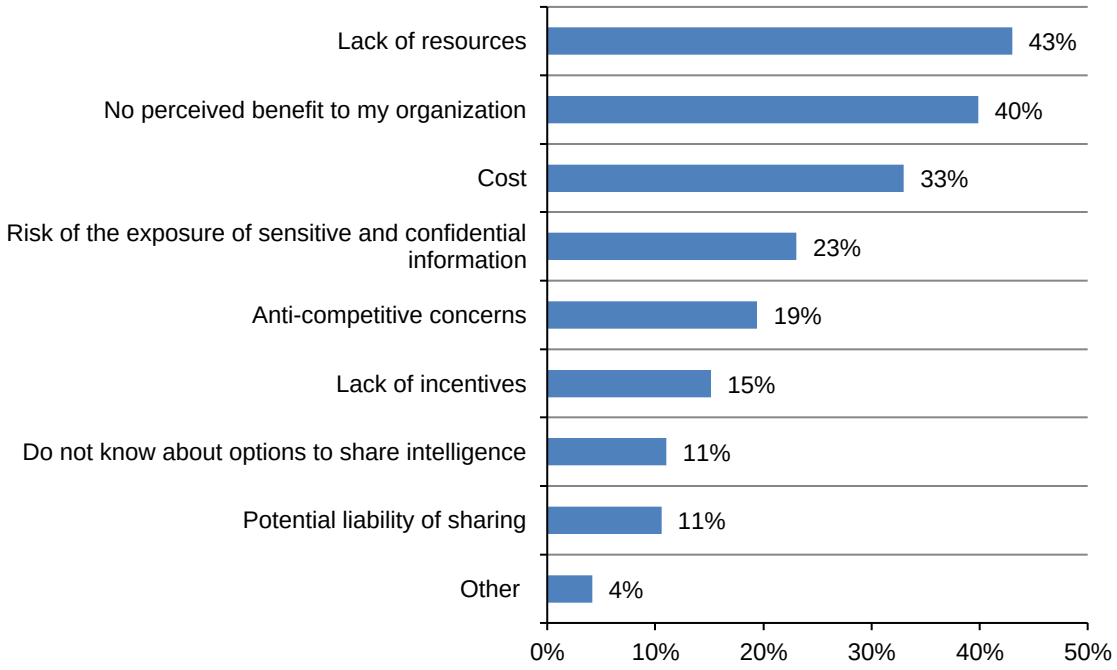
As shown in Figure 19, 77 percent of respondents say sharing intelligence improves the security posture of their organization, and 72 percent of respondents say it improves the effectiveness of their incident response plan. Fifty-seven percent of respondents say threat intelligence sharing enhances the timeliness of incident response.

Figure 19. Why does your organization share information about its data breach experience and incident response plans?
Three choices allowed



A lack of resources and no perceived benefits are reasons not to share. Why are some companies reluctant to share intelligence? According to respondents who don't share threat intelligence, it is because there is a lack of resources (42 percent), no perceived benefit (40 percent) and it costs too much (33 percent), as can be seen in Figure 20.

Figure 20. Why doesn't your organization participate in a threat-sharing program?
Two choices allowed



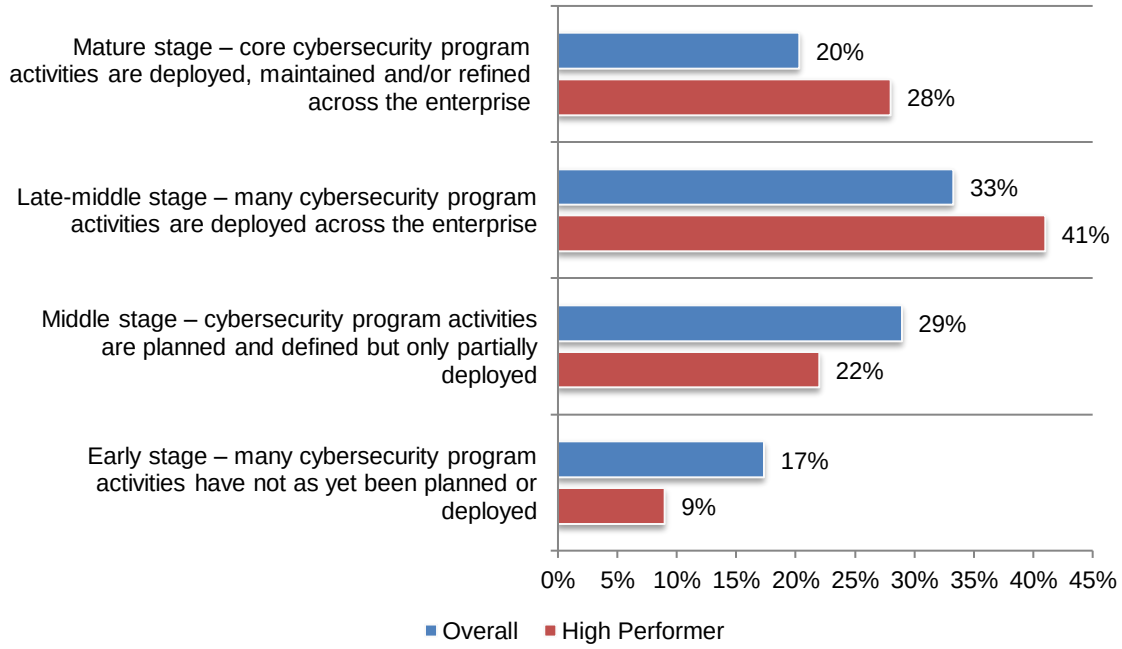
The characteristics of organizations with a high degree of cyber resilience

As part of this research, we identified certain organizations represented in this study that self-reported they have achieved a high level of cyber resilience and are better able to mitigate risks, vulnerabilities and attacks.

Of the 2,848 organizations represented in this study, 726 self-reported 9+ on a scale of 1 = low resilience to 10 = high resilience. Respondents from these organizations, referred to as high performers, are much more confident in the strength of their security posture as opposed to those who self-reported they have not achieved a state of high cyber resilience, referred to as average performers.

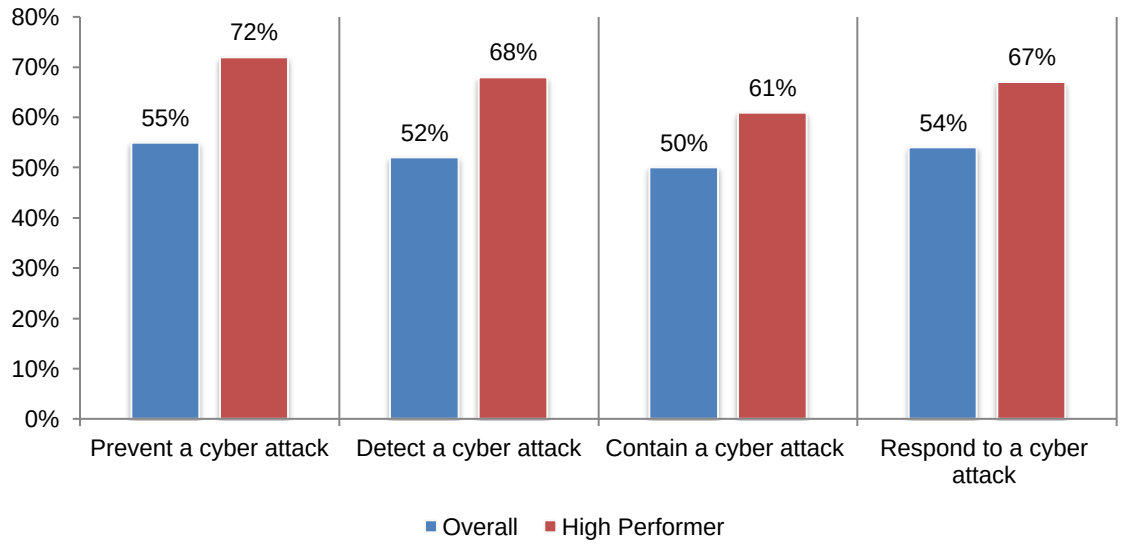
High performers have more mature cybersecurity programs and activities. According to Figure 21, 69 percent of high performing organizations have either late-middle stage (41 percent) or mature stage (28 percent) cybersecurity programs or activities as opposed to 53 percent of respondents in the overall sample.

Figure 21. What best describes the maturity level of your organization's cybersecurity program or activities?



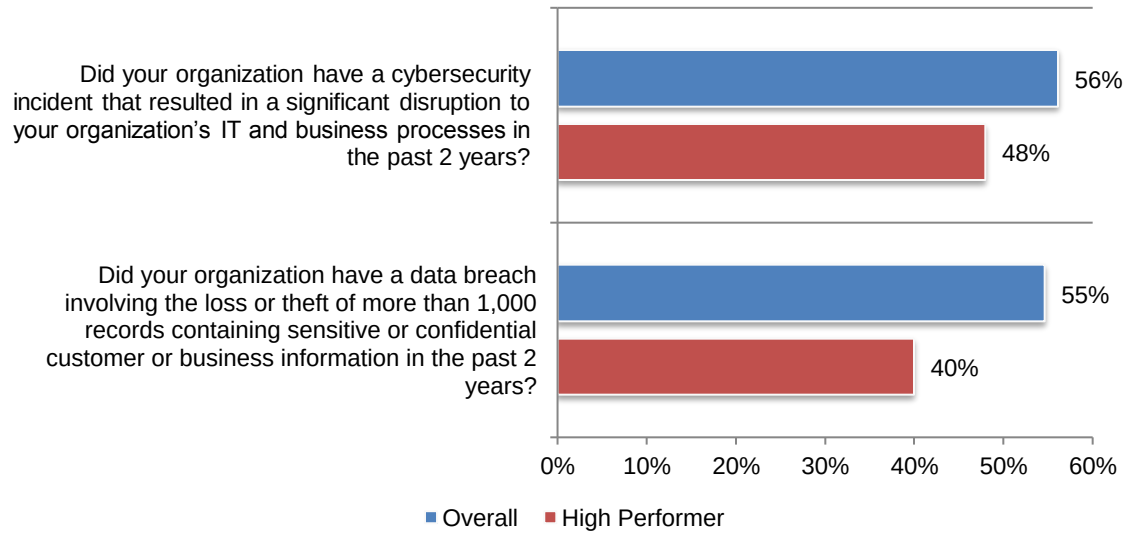
Highly cyber resilient organizations are significantly more confident in their ability to prevent, detect, contain and recover from a cyber attack. As shown in Figure 22, 72 percent of respondents in high performing organizations are highly confident in their ability to prevent a cyber attack, whereas 55 percent of respondents from the other more average organizations believe they have a high ability to prevent a cyber attack. Other differences in the detection, contain and respond are presented in this figure.

Figure 22. Organizations confident in preventing, detecting, containing and responding to a cyber attack
1 = low ability to 10 = high ability, 7+ responses reported



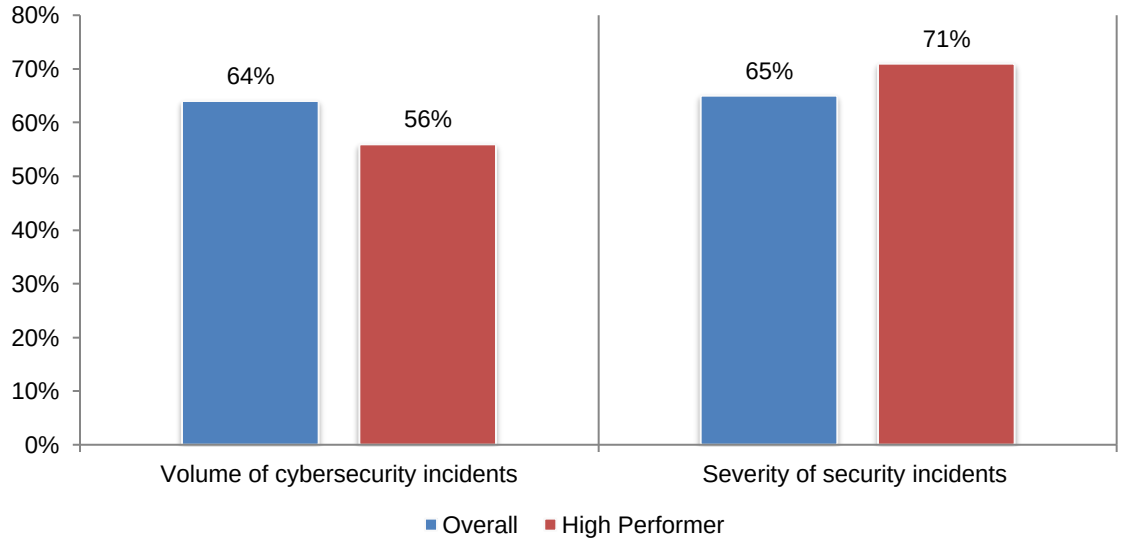
Highly cyber resilient organizations are far less likely to have a data breach and cyber security incident. According to Figure 23**,** 55 percent of respondents from average performing organizations experienced a data breach, while only 40 percent of respondents from high performer organizations reported a data breach. Similarly, less than half of high performing organizations (48 percent of respondents) report a cybersecurity incident vs. 56 percent of respondents in the other organizations.

Figure 23. Did your organization have a data breach or cybersecurity incident?
Yes responses reported



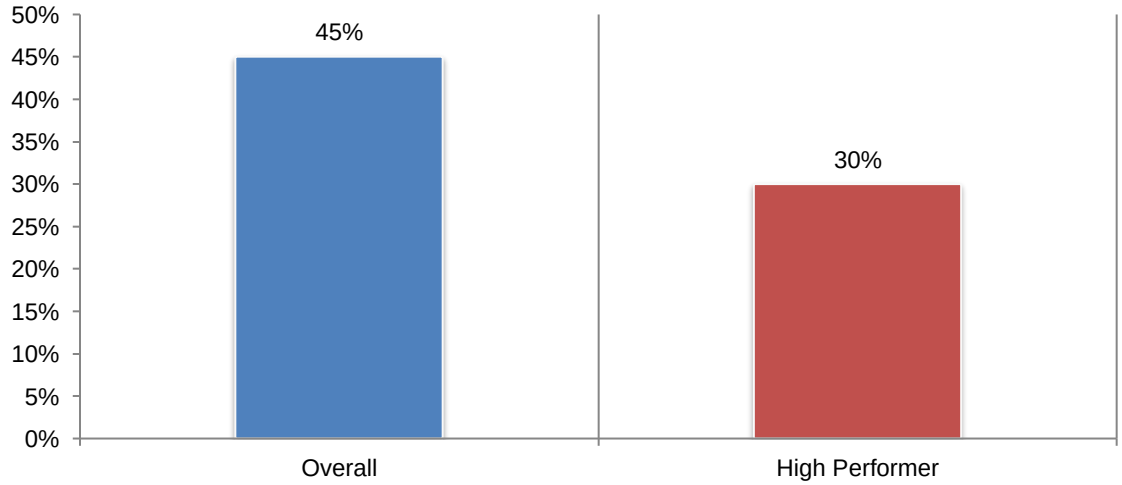
High performing organizations seem to have a better response than other organizations in dealing with the volume of cybersecurity incidents. Fifty-six percent of respondents in the high performing organizations believe the volume has significantly increased or increased vs. 64 percent of respondents in the average organizations. This is reversed in seeing an increase in the severity of cybersecurity incidents, as shown in Figure 24.

Figure 24. How has the volume and severity of cybersecurity incidents changed in the past 12 months?
Significantly increased and Increased responses combined



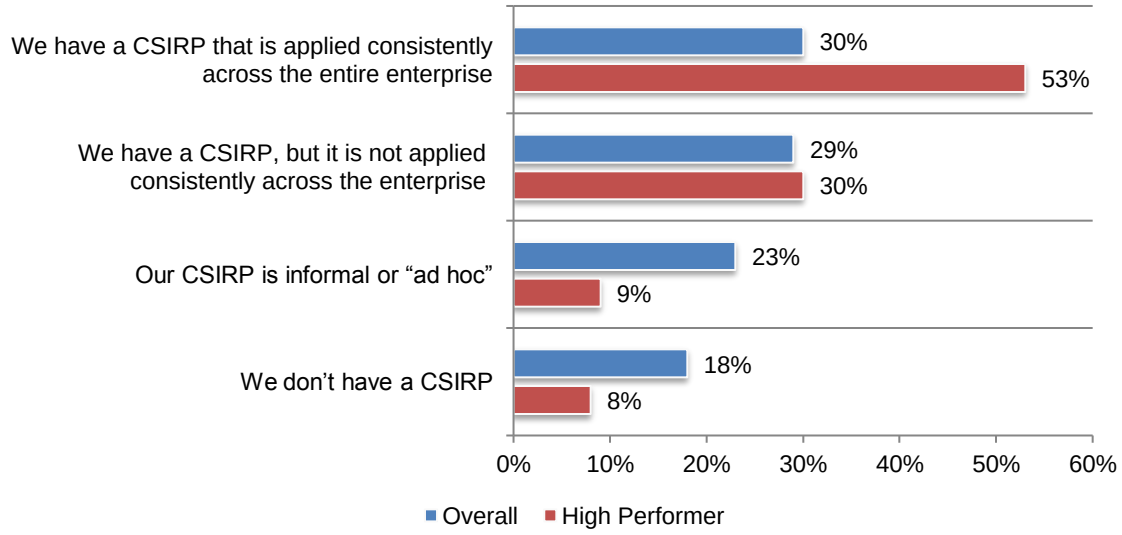
Respondents in high performing organizations are reporting fewer data breaches and cybersecurity incidents than other organizations. They also report fewer disruptions to business processes or IT operations.

Figure 25. As a result of data breaches and cyber crime incidents, how frequently do disruptions to business processes or IT services occur?
Very frequently and Frequently responses combined



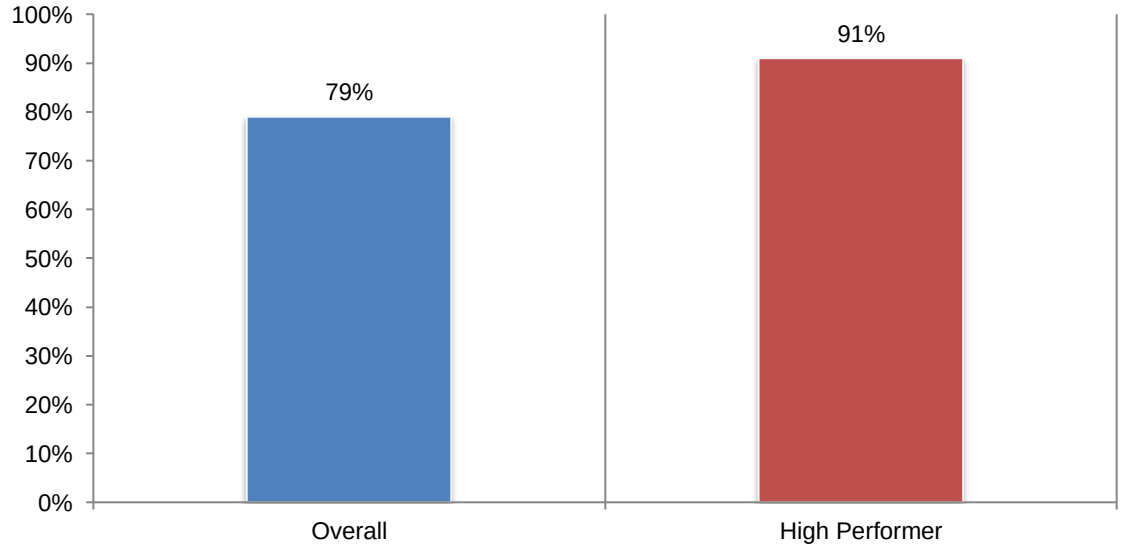
Highly cyber resilient organizations have enterprise-wide CSIRPs. As demonstrated in the data above, high performer organizations are much more confident in their ability to prevent, detect, contain and recover from a cyber attack. They are also more likely, as shown in Figure 26, to have a CSIRP that is applied consistently across the entire enterprise.

Figure 26. What best describes your organization's cybersecurity incident response plan (CSIRP)



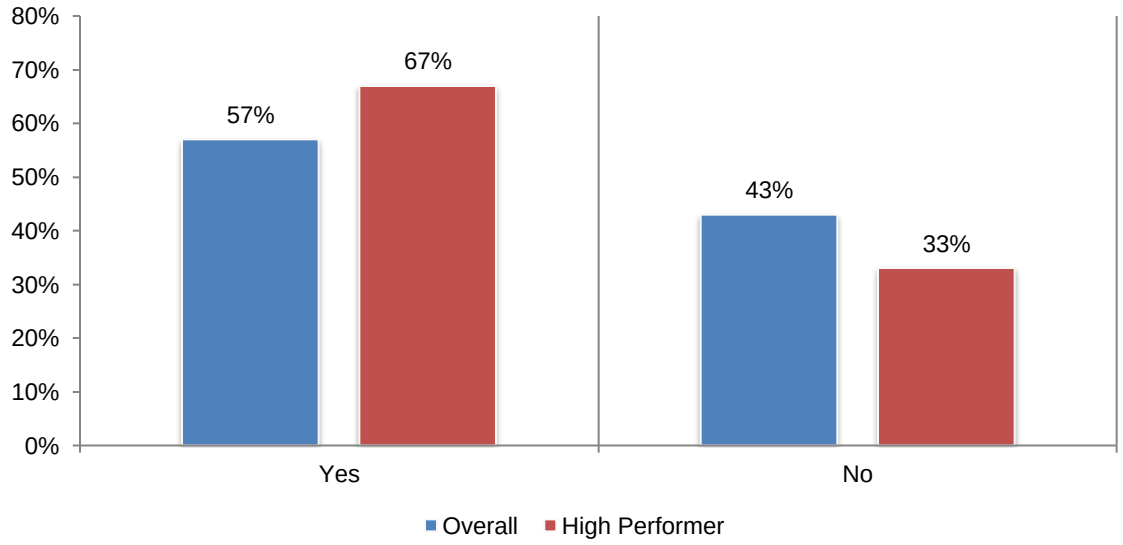
Moreover, almost all highly cyber resilient organizations expressed their belief in the importance of having skilled cybersecurity professionals in their CSIRP**,** as shown in Figure 27.

Figure 27. It is very important to have skilled cybersecurity professionals in their CSIRP
1 = low importance to 10 = high importance, 7+ responses reported



Highly cyber resilient organizations believe in sharing intelligence regarding data breaches. As shown in Figure 28, 67 percent of respondents in high performing organizations say their organizations share information regarding data breaches they experienced with government and industry peers.

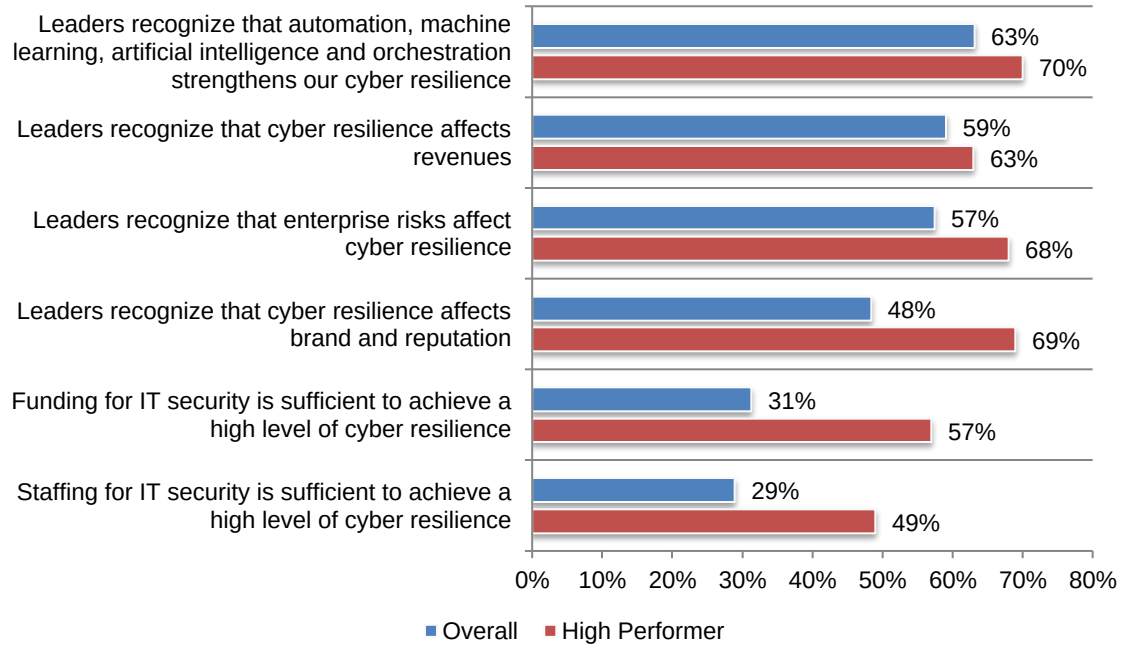
Figure 28. Does your organization share information about data breaches with government or industry peers?



Senior management in high performer organizations tend to place a higher value on cyber resilience. As shown in Figure 29, high performing organizations benefit from senior management that sees the relationship between cyber resilience, and growing revenues and maintaining brand and reputation.

Figure 29. Senior management's awareness about the positive impact of cyber resilience on the enterprise

Strongly agree and Agree responses combined

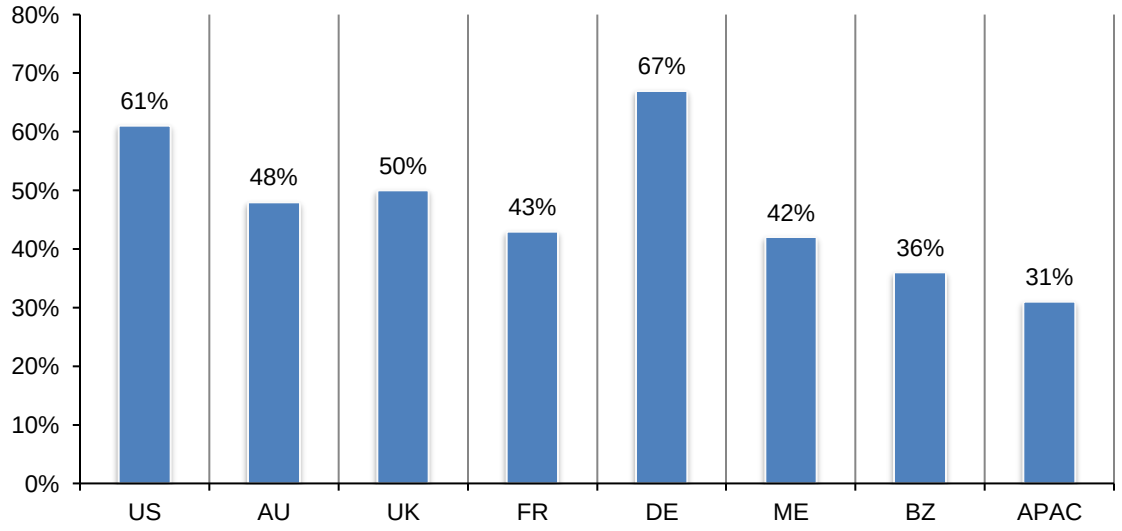


Country differences

In this section of the report we analyze differences in cyber resilience in the countries represented in this study. Countries include: US, Australia, UK, France, Germany, Middle East, Brazil and Asia Pac.

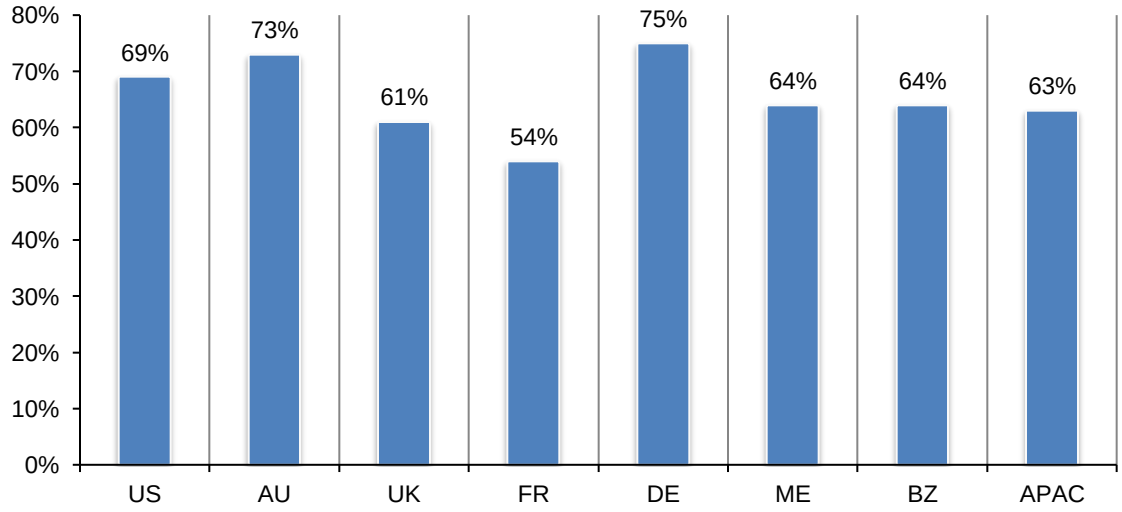
The most cyber resilient organizations are in Germany and the US. Respondents were asked to rank the level of their organizations' cyber resilience. As shown in Figure 30, German and US organizations are believed to be the most resilient (67 percent and 61 percent of respondents, respectively). Organizations in Brazil and Asia Pac are less confident in their ability to be cyber resilient.

Figure 30. How cyber resilient is your organization?
1 = low resilience to 10 = high resilience, 7+ responses reported



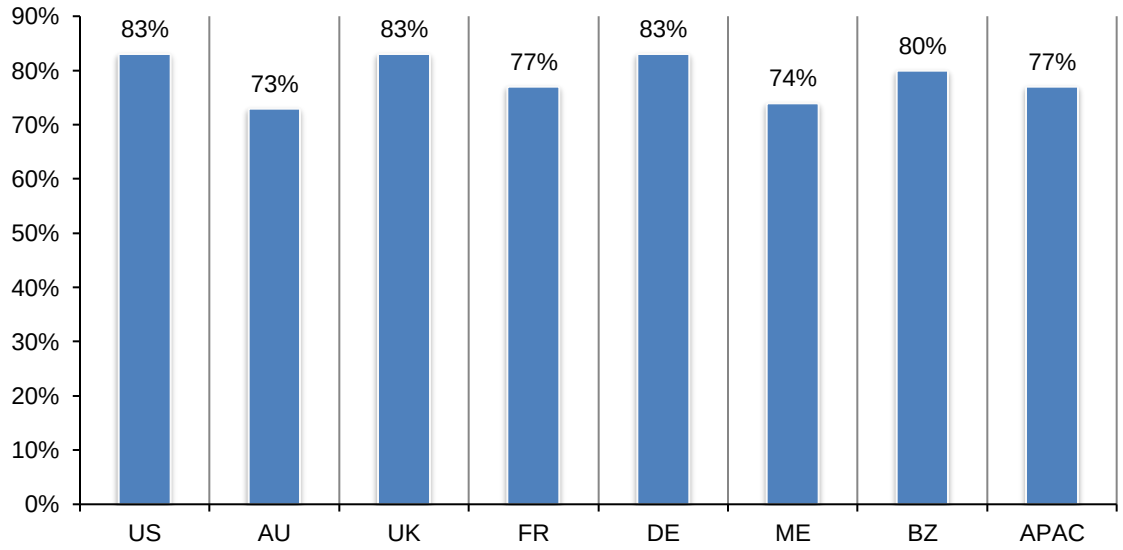
German and Australia are more likely to believe in the value of cyber resilience. Seventy-five percent of German respondents say cyber resilience is critical. Seventy-three percent of Australian respondents value cyber resilience, as shown in Figure 31. Respondents in France place the least value in cyber resilience.

Figure 31. Certain countries value cyber resilience more than others
1 = low value to 10 = high value, 7+ responses reported



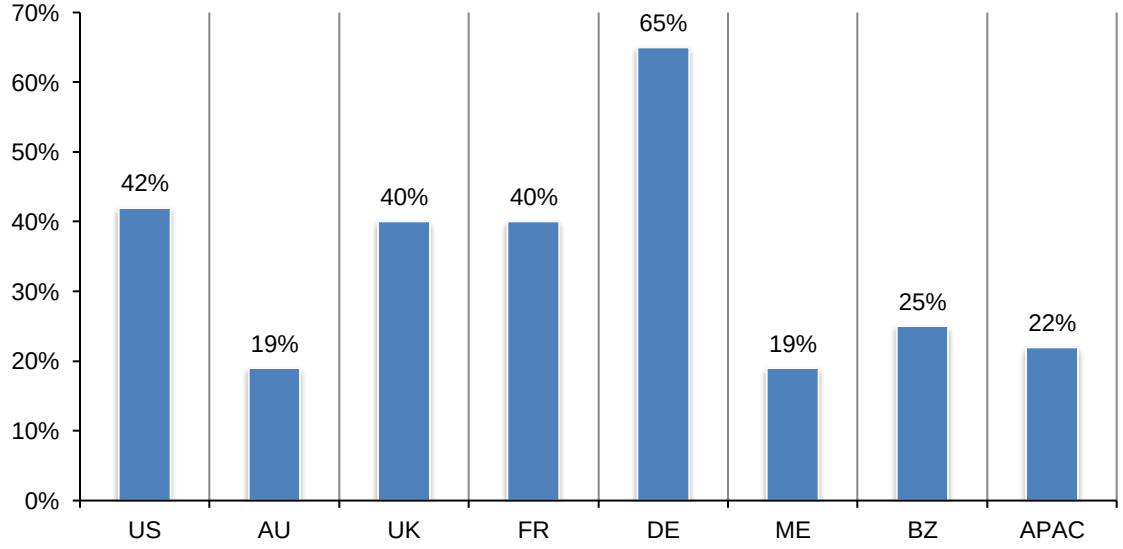
In every country, skilled cybersecurity professionals as part of the CSIRP is very important. In Germany, 83 percent of respondents say the inclusion of such professionals is very important—higher than the other countries represented in this study, as shown in Figure 32.

Figure 32. How important is having skilled cybersecurity professionals in a CSIRP?
1 = low important to 10 = high importance, 7+ responses reported



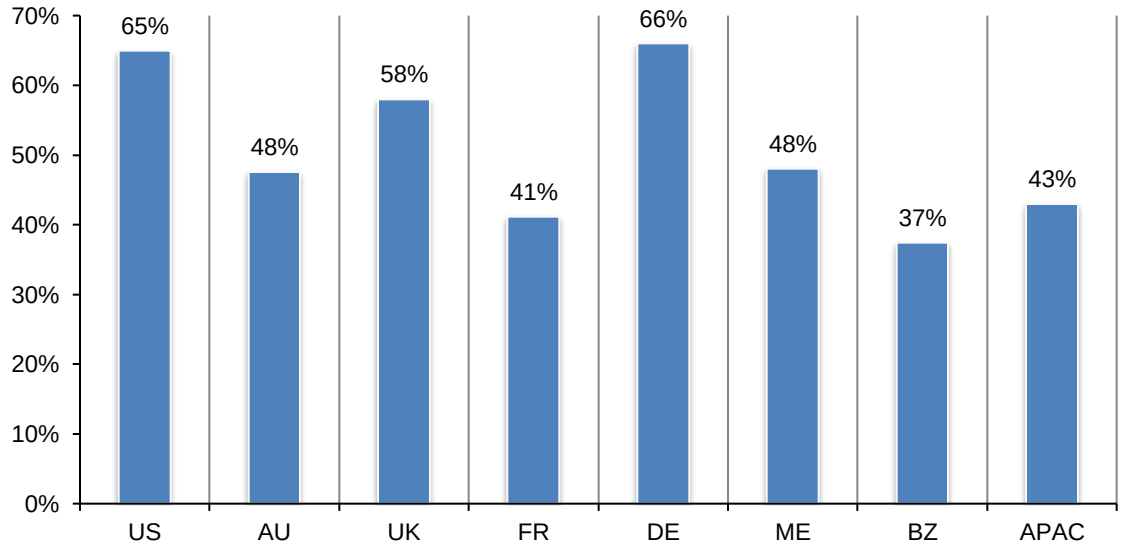
Most companies lack confidence in their ability to comply with the European Union's General Data Protection Regulation (GDPR), which is scheduled to go into effect May 2018. As shown in Figure 33, very few organizations represented in this study are confident in their ability to comply with this new regulation. German respondents expressed the most confidence (65 percent of respondents).

Figure 33. Confidence in organizations' ability to comply with the EU GDPR
1 = low ability to 10 = high ability, 7+ responses reported



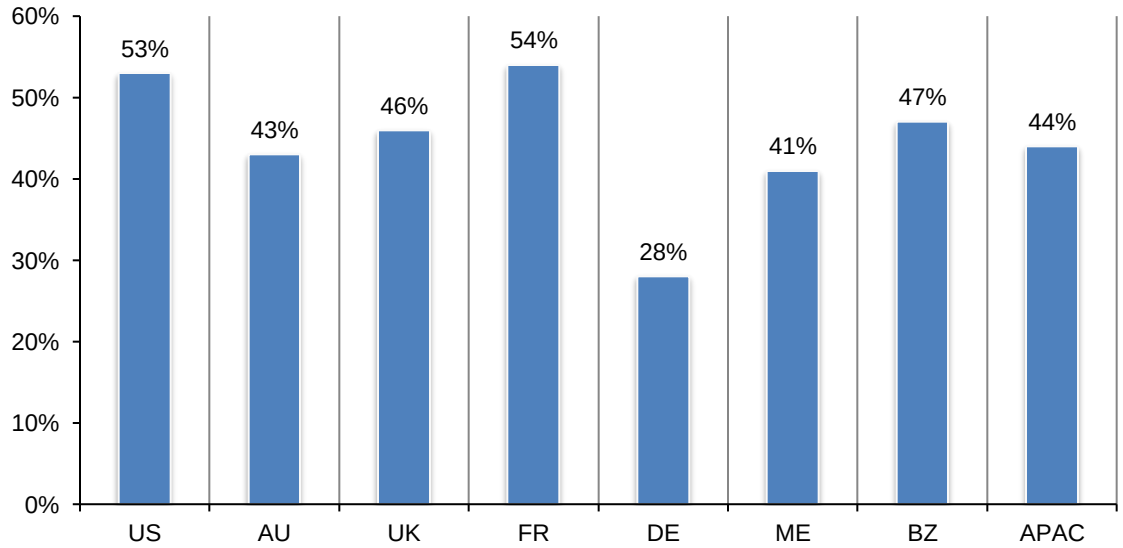
German and US organizations are more likely to participate in threat sharing. France and Asia Pac are least likely to participate, as shown in Figure 34.

Figure 34. Does your organization participate in threat sharing?
Yes responses reported



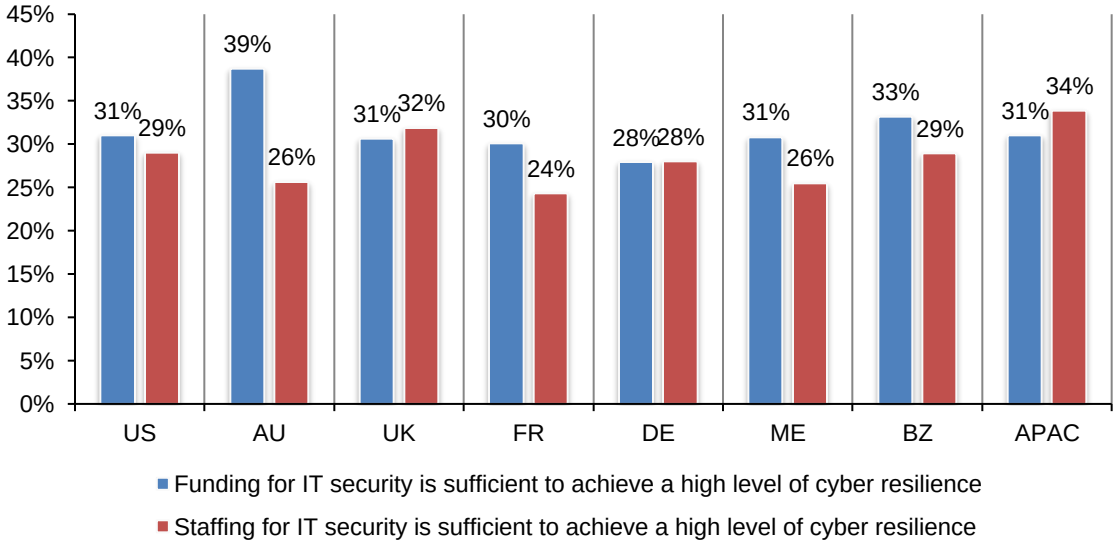
France and US experience the most business disruptions. According to Figure 35, 54 percent of respondents in France and 53 percent of respondents in the US say their organization experienced disruptions to business processes or IT services as a result of cybersecurity breaches. Germany has the least occurrence of business disruptions (28 percent of respondents).

Figure 35. How frequently do disruptions to business processes or IT services occur as a result of cybersecurity breaches?
Very frequently and Frequently responses combined



Globally, funding and staffing for cyber resilience activities are not adequate. As shown in Figure 36, most countries represented in this research do not believe they have the budget or the staff to improve their cyber resilience.

Figure 36. Perceptions regarding funding and staffing
Strongly agree and Agree responses combined



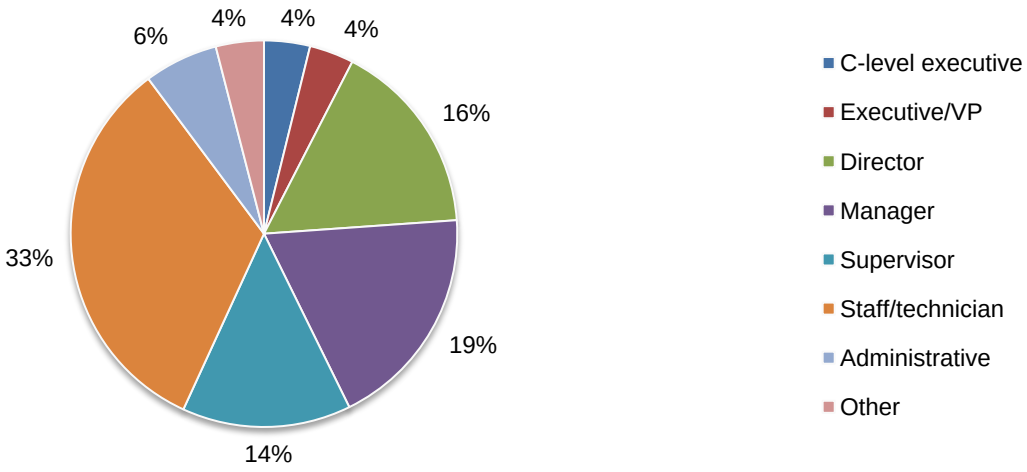
Part 4. Methods

The sampling frame is composed of 83,658 IT and IT security practitioners located in the United States, Australia, the United Kingdom, France, Germany, Mexico, Brazil and the Asia Pacific region. As shown in Table 2, 3,271 respondents completed the survey. Screening and failed reliability checks resulted in the removal of 423 surveys. The final sample consisted of 2,848 surveys, for an overall 3.4 percent response rate.

Table 2: Survey response	Total sampling frame	Final sample	Response rate
United States	17,040	573	3.4%
United Kingdom	11,625	422	3.6%
Asia-Pacific	12,339	404	3.3%
Germany	10,607	378	3.6%
Brazil	10,647	317	3.0%
France	9,050	300	3.3%
Australia	6,800	235	3.5%
Middle East	5,550	219	3.9%
Total	83,658	2,848	3.4%

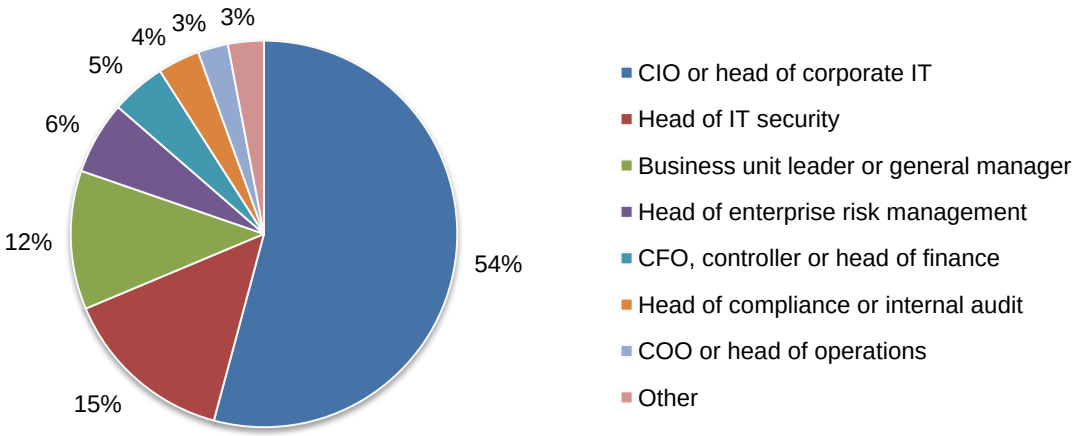
Pie Chart 1 reports respondents' organizational level within participating organizations. As can be seen, the majority of respondents (57 percent) are at or above the supervisory level.

Pie Chart 1. Distribution of respondents according to position level



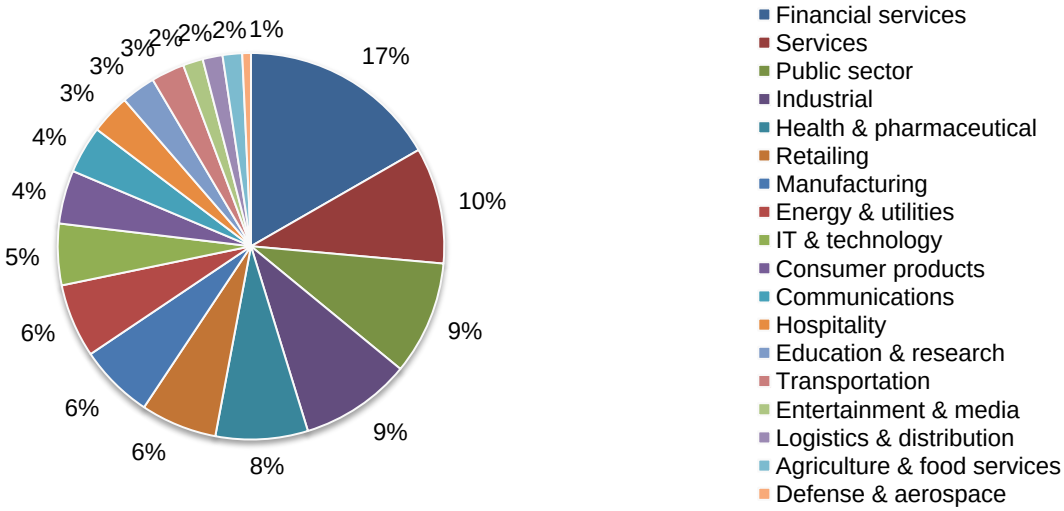
Pie Chart 2 reveals that 54 percent of respondents report directly to the CIO or head of corporate IT, 15 percent of respondents report to the head of IT security and 12 percent of respondents report to the business unit leader or general manager.

Pie Chart 2. Direct reporting channel or chain of command



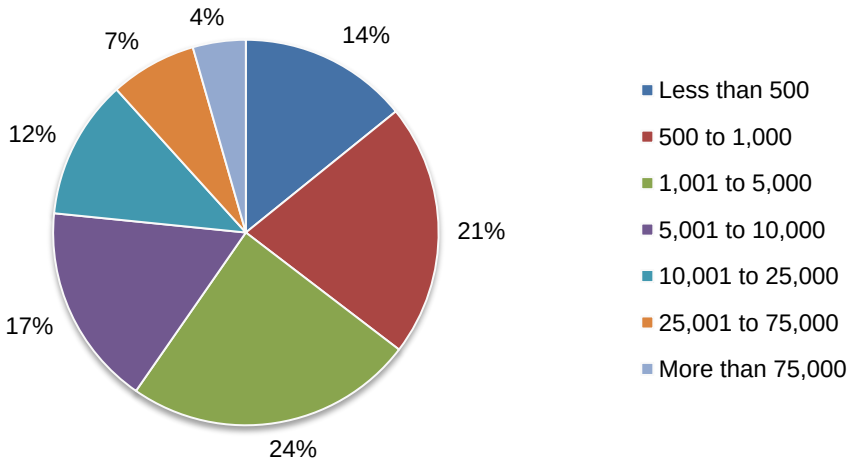
Pie Chart 3 reports the primary industry classification of respondents' organizations. This chart identifies financial services (17 percent) as the largest segment, followed by services (10 percent), public sector (9 percent) and industrial (9 percent).

Pie Chart 3. Primary industry classification



Pie Chart 4 reveals that 65 percent of respondents are from organizations with a worldwide headcount of more than 1,000 employees.

Pie Chart 4. Worldwide full-time headcount of the organization



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 are IT or IT security practitioners. 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 November 2017.

Survey response	2017	2016	2015
Total sampling frame	83,658	75,160	46,820
Total returns	3,271	2,796	1,745
Rejected or screened surveys	423	392	227
Final sample	2,848	2,404	1,518
Response rate	3.4%	3.2%	3.24%

Part 1. Screening

S1. What best describes your organizational role or area of focus?	2017	2016	2015
IT security operations	34%	34%	35%
IT operations	43%	45%	39%
CSIRT team	17%	16%	18%
Business continuity management	6%	6%	8%
None of the above (stop)	0%	0%	0%
Total	100%	100%	100%

S2. Please check all the activities that you see as part of your job or role.	2017	2016	2015
Managing budgets	46%	43%	49%
Evaluating vendors	46%	48%	47%
Setting priorities	39%	38%	33%
Securing systems	59%	61%	65%
Ensuring compliance	45%	45%	46%
Ensuring system availability	41%	41%	39%
None of the above (stop)	0%	0%	0%
Total	275%	277%	338%

Part 2. Background Questions

Q1a. Did your organization have a data breach involving the loss or theft of more than 1,000 records containing sensitive or confidential customer or business information in the past 2 years?	2017	2016
Yes	55%	53%
No	40%	42%
Unsure	5%	5%
Total	100%	100%

Q1b. If yes, how frequently did these incidents occur during the past 2 years?	2017	2016
Only once	44%	43%
2 to 3 times	40%	41%
4 to 5 times	10%	10%
More than 5 times	7%	6%
Total	100%	100%

Q2a. Did your organization have a cybersecurity incident that resulted in a significant disruption to your organization's IT and business processes in the past 2 years?	2017
Yes	56%
No	40%
Unsure	4%
Total	100%

Q2b. If yes, how frequently did these incidents occur during the past 2 years?	2017
Only once	19%
2 to 3 times	24%
4 to 5 times	35%
More than 5 times	22%
Total	100%

Q3a. How has the volume of cybersecurity incidents changed in the past 12 months?	2017
Significantly increased	31%
Increased	33%
No increase	23%
Decreased	11%
Significantly decreased	3%
Total	100%

Q3b. How has the severity of security incidents changed in the past 12 months?	2017
Significantly increased	31%
Increased	34%
No increase	21%
Decreased	10%
Significantly decreased	3%
Total	100%

Q4. As a result of data breaches and cyber crime incidents, how frequently do disruptions to business processes or IT services occur as a result of cybersecurity breaches?	2017	2016
Very frequently	18%	16%
Frequently	27%	28%
Somewhat frequently	29%	30%
Rarely	20%	20%
Never	6%	6%
Total	100%	100%

Q5. Using the following 10-point scale, please rate your organization's cyber resilience from 1 = low resilience to 10 = high resilience.	2017	2016	2015
1 or 2	10%	9%	10%
3 or 4	15%	17%	19%
5 or 6	27%	41%	36%
7 or 8	23%	22%	19%
9 or 10	25%	10%	16%
Total	100%	100%	100%
Extrapolated value	6.30	5.63	5.72

Q6. Using the following 10-point scale, please rate your organization's ability to **prevent** a cyber attack from 1 = low to 10 = high.	2017	2016	2015
1 or 2	9%	10%	11%
3 or 4	14%	15%	19%
5 or 6	22%	35%	32%
7 or 8	28%	27%	22%
9 or 10	27%	13%	16%
Total	100%	100%	100%
Extrapolated value	6.50	5.85	5.73

Q7. Using the following 10-point scale, please rate your organization's ability to quickly **detect** a cyber attack from 1 = low to 10 = high.	2017	2016	2015
1 or 2	8%	9%	10%
3 or 4	14%	13%	16%
5 or 6	26%	28%	27%
7 or 8	28%	28%	24%
9 or 10	24%	21%	23%
Total	100%	100%	100%
Extrapolated value	6.46	6.28	6.20

Q8. Using the following 10-point scale, please rate your organization's ability to **contain** a cyber attack from 1 = low to 10 = high.	2017	2016	2015
1 or 2	4%	3%	6%
3 or 4	18%	17%	17%
5 or 6	28%	27%	25%
7 or 8	32%	35%	28%
9 or 10	18%	18%	24%
Total	100%	100%	100%
Extrapolated value	6.32	6.44	6.46

Q9. Using the following 10-point scale, please rate your organization's ability to respond to a cyber attack from 1 = low to 10 = high.	2017
1 or 2	4%
3 or 4	14%
5 or 6	28%
7 or 8	31%
9 or 10	23%
Total	100%
Extrapolated value	6.57

Q10. Please rate the value of cyber resilience to your organization from 1 = low to 10 = high.	2017	2016
1 or 2	7%	9%
3 or 4	12%	13%
5 or 6	16%	28%
7 or 8	32%	29%
9 or 10	33%	22%
Total	100%	100%
Extrapolated value	6.95	6.36

Q11. Using the following 10-point scale, please rate the importance of having skilled cybersecurity professionals in your cyber security incident response plan (CSIRP) from 1 = low to 10 = high.	2017	2016
1 or 2	2%	2%
3 or 4	5%	5%
5 or 6	13%	14%
7 or 8	46%	47%
9 or 10	33%	32%
Total	100%	100%
Extrapolated value	7.57	7.53

Q12. Please rate the difficulty in hiring and retaining skilled IT security personnel from 1 = low to 10 = high.	2017
1 or 2	2%
3 or 4	5%
5 or 6	16%
7 or 8	44%
9 or 10	33%
Total	100%
Extrapolated value	7.49

Q13. Using the following 10-point scale, please rate your organization's ability to comply with the EU General Data Protection Regulation from 1 = low to 10 = high.	2017	2016
1 or 2	13%	17%
3 or 4	22%	32%
5 or 6	29%	30%
7 or 8	20%	15%
9 or 10	16%	7%
Total	100%	100%
Extrapolated value	5.58	4.74

Q14. Following are 7 factors considered important in achieving a high level of cyber resilience. Please rank order each factor from 1 = most important to 7 = least important.	2017	2016	2015
Agility	2.2	2.2	2.68
Preparedness	1.8	1.8	2.06
Planned redundancies	4.5	4.3	5.57
Strong security posture	2.9	3.0	2.81
Knowledgeable or expert staff	3.7	3.7	2.66
Ample resources	5.1	5.1	4.99
Leadership	4.4	4.4	3.21

Q15a. How has your organization's cyber resilience changed in the past 12 months?	2017	2016
Significantly improved	18%	9%
Improved	25%	18%
Somewhat improved	29%	25%
Declined	4%	4%
No improvement	25%	44%
Total	100%	100%

Q15b. If your organization has improved its cyber resilience, what caused the improvement? Please check your four top choices.	2017	2016
Implementation of new technology, including cyber automation tools such as artificial intelligence and machine learning	47%	
Elimination of silo and turf issues	39%	
Visibility into applications and data assets	57%	
Improved information governance practices	60%	
C-level buy-in and support for the cybersecurity function	23%	
Board-level reporting on the organization's cyber resilience	15%	
Training and certification for IT security staff	30%	54%
Training for end-users	29%	
Hiring skilled personnel	61%	
Engaging a managed security services provider	39%	42%
Total	400%	

Q16. In the past 12 months, how has the time to **detect, contain and respond to** a cyber crime incident changed?	2017
Time has increased significantly	26%
Time has increased	31%
Time has remained unchanged	32%
Time has decreased	9%
Time has decreased significantly	3%
Total	100%

Q17. What are the barriers to improving the detection, containment and response to a cyber crime incident? Please check your top three choices.	2017
Lack of investment in new cybersecurity technologies, including artificial intelligence and machine learning	60%
Silo and turf issues	24%
Lack of visibility into applications and data assets	46%
Lack of information governance practices	22%
Lack of C-level buy-in and support for the cybersecurity function	15%
Lack of board-level reporting on the organization's state of cyber resilience	17%
Lack of training and certification for IT security staff	28%
Lack of training for end-users	31%
Inability to hire and retain skilled personnel	56%
Total	300%

18a. Please check one statement that best describes your organization's cyber security incident response plan (CSIRP).	2017	2016	2015
We have a CSIRP that is applied consistently across the entire enterprise	24%	25%	18%
We have a CSIRP, but is not applied consistently across the enterprise	27%	26%	23%
Our CSIRP is informal or "ad hoc"	26%	26%	27%
We don't have a CSIRP	24%	23%	31%
Total	100%	100%	100%

Q18b. If you have a CSIRP, how often is it reviewed and tested?	2017	2016
Each quarter	7%	7%
Twice per year	7%	7%
Once each year	34%	34%
No set time period for reviewing and updating the plan	39%	37%
We have not reviewed or updated since the plan was put in place	14%	15%
Total	100%	100%

Q19a. Does your organization participate in an initiative or program for sharing information with government and industry peers about data breaches and incident response?	2017	2016
Yes	53%	53%
No	47%	47%
Total	100%	100%

Q19b. If your organization shares information about its data breach experience and incident response plans, what are the main reasons? Please select only three choices.	2017	2016
Improves the security posture of my organization	77%	81%
Improves the effectiveness of our incident response plan	72%	75%
Enhances the timeliness of incident response	57%	53%
Reduces the cost of detecting and preventing data breaches	58%	52%
Fosters collaboration among peers and industry groups	32%	33%
Other (please specify)	5%	5%
Total	300%	300%

Q19c. If no, why does your organization not participate in a threat-sharing program? Please select only two choices.	2017	2016
Cost	33%	33%
Potential liability of sharing	11%	10%
Risk of the exposure of sensitive and confidential information	23%	22%
Anti-competitive concerns	19%	21%
Lack of resources	43%	42%
Lack of incentives	15%	16%
No perceived benefit to my organization	40%	42%
Do not know about options to share intelligence	11%	11%
Other (please specify)	4%	4%
Total	200%	200%

Q20. If yes, which of the following security technologies have been the most effective in helping your organization become cyber resilient. Please select your top seven choices.	2017	2016
Web application firewalls (WAF)	13%	12%
Incident response platform	53%	58%
Next generation firewalls	15%	15%
Security information & event management (SIEM)	41%	41%
Cloud SIEM	25%	27%
Anti-virus / anti-malware	59%	53%
Intrusion detection & prevention systems	55%	58%
Network traffic surveillance	52%	52%
Identity management & authentication	70%	71%
Code review and debugging systems	17%	17%
Wireless security solutions	14%	14%
Data tokenization technology	20%	20%
Encryption for data in motion	37%	34%
Encryption for data at rest	52%	53%
Data loss prevention (DLP)	39%	37%
Virtual private networks (VPN)	24%	25%
Big data analytics for cybersecurity	29%	29%
DDoS solutions	18%	19%
Endpoint security solution	23%	23%
Governance solutions (GRC)	16%	16%
User Behavioral Analytics (UBA)	23%	22%
Other (please specify	5%	4%
Total	700%	700%

Strongly Agree and Agree response: Please express your opinion about each one of the following statements using the agreement scale.	2017	2016	2015
Q21a. My organization's leaders recognize that enterprise risks affect cyber resilience.	57%	48%	47%
Q21b. My organization's leaders recognize that cyber resilience affects revenues.	59%	47%	52%
Q21c. My organization's leaders recognize that cyber resilience affects brand and reputation.	48%	45%	43%
Q21d. In my organization, funding for IT security is sufficient to achieve a high level of cyber resilience	31%	33%	42%
Q21e. In my organization, staffing for IT security is sufficient to achieve a high level of cyber resilience	29%	33%	38%
Q21f. My organization's leaders recognize that automation, machine learning, artificial intelligence and orchestration strengthens our cyber resilience.	63%		

Q22. Who has overall responsibility for directing your organization's efforts to ensure a high level of cyber resilience? Please check one choice only.	2017	2016	2015
Business continuity manager	8%	8%	6%
Business unit leader	22%	22%	19%
Chief executive officer (CEO)	7%	7%	8%
Chief information officer (CIO)	23%	23%	19%
Chief technology officer (CTO)	6%	6%	6%
Chief risk officer (CRO)	7%	8%	3%
Chief information security officer (CISO)	14%	13%	9%
No one person has overall responsibility	11%	13%	12%
Other (please specify)	2%	0%	
Total	100%	100%	83%

Q23a. What is the full-time equivalent (FTE) headcount of your IT security function today?	2017
Less than 5	7%
5 to 10	10%
11 to 20	11%
21 to 30	13%
31 to 40	21%
41 to 50	16%
51 to 100	15%
More than 100	5%
Total	100%
Extrapolated value	38.8

Q23b. What should the full-time equivalent (FTE) headcount be to achieve cyber resilience?	2017
Less than 5	1%
5 to 10	2%
11 to 20	7%
21 to 30	11%
31 to 40	16%
41 to 50	26%
51 to 100	22%
More than 100	14%
Total	100%
Extrapolated value	55.0

Q24. How long has your organization's current CISO or security leader held their position?	2017
Currently, we don't have a CISO or security leader	23%
Less than 1 year	22%
1 to 3 years	28%
4 to 6 years	16%
7 to 10 years	9%
More than 10 years	2%
Total	100%

Q25. What best describes the maturity level of your organization's cybersecurity program or activities?	2017
Early stage – many cybersecurity program activities have not as yet been planned or deployed	17%
Middle stage – cybersecurity program activities are planned and defined but only partially deployed	29%
Late-middle stage – many cybersecurity program activities are deployed across the enterprise	33%
Mature stage – Core cybersecurity program activities are deployed, maintained and/or refined across the enterprise	20%
Total	100%

Q26. Following are cybersecurity activities considered important by many organizations. Please rate each activity using the following scale: 1 = implemented, 2 = plan to implement in the next 12 months, 3 = plan to implement in more than 12 months, 4 = no plan to implement	1	2	3	4	Total
Capture information about attackers (honey pot)	0.21	0.28	0.19	0.32	1.00
Conduct surveillance and fraud prevention	0.60	0.17	0.14	0.09	1.00
Control endpoints and mobile connections	0.53	0.19	0.12	0.16	1.00
Control over insecure mobile devices including BYOD	0.42	0.19	0.11	0.28	1.00
Curtail end-user access to insecure Internet sites and web applications	0.55	0.19	0.08	0.18	1.00
Curtail unauthorized access to sensitive or confidential data	0.73	0.06	0.09	0.12	1.00
Curtail unauthorized access to mission-critical applications	0.69	0.19	0.02	0.10	1.00
Curtail unauthorized sharing of sensitive or confidential data	0.71	0.07	0.02	0.20	1.00
Curtail botnets and distributed denial of service attacks	0.44	0.15	0.15	0.26	1.00
Effort to reduce footprint of sensitive or confidential data	0.56	0.04	0.18	0.22	1.00
Enable adaptive perimeter controls	0.22	0.13	0.28	0.37	1.00
Enable efficient backup and disaster recovery operations	0.72	0.05	0.01	0.22	1.00
Enable efficient patch management	0.52	0.19	0.13	0.16	1.00
Enable multifactor authentication	0.45	0.10	0.18	0.27	1.00
Enable signal sign-on	0.46	0.12	0.17	0.25	1.00
Establish metrics or capability maturity model for management reporting	0.36	0.23	0.15	0.26	1.00
Limit access to insecure networks (e.g., public WiFi)	0.47	0.06	0.29	0.18	1.00
Limit the loss or theft of data-bearing devices (including IoT)	0.21	0.57	0.04	0.18	1.00
Pinpoint and monitor anomalies in network traffic	0.37	0.22	0.16	0.25	1.00
Pinpoint and monitor suspicious user behaviour (e.g., UBA)	0.50	0.05	0.06	0.39	1.00
Prioritize threats, vulnerabilities and attacks	0.43	0.23	0.25	0.09	1.00
Provide advance warning about threats and attackers	0.44	0.16	0.05	0.35	1.00
Provide intelligence about the threat landscape	0.29	0.11	0.12	0.48	1.00
Secure access to cloud-based applications and infrastructure	0.50	0.22	0.04	0.24	1.00
Secure data stored in clouds	0.50	0.21	0.06	0.23	1.00
Use of machine learning and artificial intelligence for cybersecurity	0.31	0.39	0.15	0.15	1.00

Q27. Following are cybersecurity governance practices considered important by many organizations. Please rate each activity using the following scale: 1 = implemented, 2 = plan to implement in the next 12 months, 3 = plan to implement in more than 12 months, 4 = no plan to implement.	1	2	3	4	Total
Hire and retain expert IT security personnel	0.64	0.13	0.14	0.09	1.00
Provide clearly defined IT security policies	0.72	0.15	0.05	0.08	1.00
Establish and test backup and disaster recovery plans	0.69	0.08	-	0.23	1.00
Establish business continuity management function	0.56	0.24	0.09	0.11	1.00
Establish and test incident response management plan	0.56	0.10	0.05	0.29	1.00
Perform background checks of system users	0.33	0.28	0.06	0.33	1.00
Conduct specialized training for IT security personnel	0.59	0.12	0.08	0.21	1.00
Conduct training and awareness activities for the organization's users	0.57	0.27	0.11	0.05	1.00
Monitor business partners, vendors and other third parties	0.56	0.18	0.12	0.14	1.00
Conduct Internal or external audits of security and IT compliance practices	0.63	0.21	0.02	0.14	1.00
Segregate duties between IT and business functions	0.70	0.15	0.04	0.11	1.00
Perform risk assessment to evaluate IT security posture	0.77	0.18	-	0.05	1.00
Adhere to standardized security requirements (ISO, NIST, others)	0.42	0.07	0.20	0.31	1.00
Appoint a high-level security leader (CSO or CISO) with no more than 3 levels below the CEO and enterprise-wide responsibility	0.69	0.21	0.06	0.04	1.00
Appoint a high-level leader (CPO) accountable for information protection and privacy	0.44	0.06	0.32	0.18	1.00
Establish a direct crisis communication channel to the CEO and board of directors	0.46	0.03	0.22	0.29	1.00
Establish a security program charter approved by executive management	0.62	0.13	0.18	0.07	1.00
Present to the CEO and board of directors on the state of cybersecurity	0.44	0.41	0.06	0.09	1.00
Establish a process for reporting cyber crime and data breach to appropriate authorities	0.53	0.30	0.17	-	1.00
Purchase of cyber liability insurances	0.40	0.24	0.13	0.23	1.00
Establish metrics to evaluate the efficiency and effectiveness of IT security operations	0.52	0.34	0.07	0.07	1.00
Fosters collaboration among peers and industry groups	0.29	0.15	0.18	0.38	1.00
Other (please specify)	0.32	0.27	0.01	0.40	1.00

Q28. What factors justify the funding of your organization's IT security? Please select two choices.	2017	2016	2015
System or application downtime	61%	62%	64%
Information loss or theft	47%	48%	37%
Performance degradation	10%	9%	9%
Productivity loss	9%	9%	8%
Revenue decline	8%	7%	6%
Reputation damage	18%	20%	18%
Customer defection	8%	8%	11%
Compliance/regulatory failure	36%	36%	44%
Other (please specify)	1%	1%	1%
Total	200%	200%	200%

Q29. Approximately, what is the dollar range that best describes your organization's current **cyber security budget**?	2017	2016	2015
< $1 million	6%	5%	0%
$1 to 5 million	18%	16%	10%
$6 to $10 million	28%	29%	29%
$11 to $15 million	23%	25%	32%
$16 to $20 million	15%	15%	10%
$21 to $25 million	7%	6%	8%
$26 to $50 million	1%	2%	6%
> $50 million	1%	1%	4%
Total	100%	100%	100%
Extrapolated value ($millions)	11.3	11.4	$15.0

Q30. Approximately, what percentage of the current **cyber security budget** will go to cyber resilience-related activities?	2017	2016	2015
< 2%	0%	0%	1%
2% to 5%	2%	2%	1%
6% to 10%	8%	7%	6%
11% to 20%	12%	13%	25%
21% to 30%	34%	35%	34%
31% to 40%	22%	22%	20%
41% to 50%	10%	10%	9%
51% to 60%	8%	6%	3%
61% to 70%	4%	5%	2%
71% to 80%	1%	0%	0%
81% to 90%	0%	0%	0%
91 to 100%	0%	0%	0%
Total	100%	100%	100%
Extrapolated value (percentage)	30%	30%	26%

Q31. The following table lists five areas of a CSRIP in your organization. Please allocate 100 points to denote the level of investment in each area.	2017	2016
Prevention	44	47
Detection	26	25
Containment	15	15
Remediation	11	10
Post incident response	4	3
Total	100	100

Organizational and respondent characteristics

D1. What best describes the position level within the organization?	2017	2016	2015
C-level executive	4%	4%	2%
Executive/VP	4%	3%	5%
Director	16%	16%	15%
Manager	19%	20%	19%
Supervisor	14%	14%	17%
Staff/technician	33%	34%	33%
Administrative	6%	5%	4%
Consultant/contractor	2%	2%	3%
Other (please specify)	2%	1%	1%
Total	100%	100%	100%

D2. What best describes your reporting channel or chain of command?	2017	2016
CEO/executive committee	2%	3%
COO or head of operations	3%	3%
CFO, controller or head of finance	5%	4%
CIO or head of corporate IT	54%	54%
Business unit leader or general manager	12%	12%
Head of compliance or internal audit	4%	3%
Head of enterprise risk management	6%	7%
Head of IT security	15%	14%
Other (please specify)	1%	2%
Total	100%	100%

D3. What best describes your organization's primary industry classification?	2017	2016	2015
Agriculture & food services	2%	2%	1%
Communications	4%	4%	3%
Consumer products	4%	5%	5%
Defense & aerospace	1%	1%	1%
Education & research	3%	2%	2%
Energy & utilities	6%	6%	5%
Entertainment & media	2%	1%	2%
Financial services	17%	17%	16%
Health & pharmaceutical	8%	8%	10%
Hospitality	3%	3%	2%
Industrial	9%	10%	9%
IT & technology	5%	4%	6%
Logistics & distribution	2%	1%	0%
Manufacturing	6%	7%	7%
Public sector	9%	10%	11%
Retailing	6%	7%	8%
Services	10%	9%	8%
Transportation	3%	3%	3%
Total	100%	100%	99%

D4. What range best describes the full-time headcount of your global organization?	2017	2016	2015
Less than 500	15%	14%	14%
500 to 1,000	21%	21%	20%
1,001 to 5,000	26%	24%	24%
5,001 to 10,000	17%	17%	20%
10,001 to 25,000	11%	12%	10%
25,001 to 75,000	6%	7%	7%
More than 75,000	4%	4%	5%
Total	100%	100%	100%

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

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.