The Fourth Annual Study on

The Cyber Resilient Organization

Independently conducted by the Ponemon Institute

Sponsored by IBM Security

Publication Date: April 2019

The 2019 Study on the Cyber Resilient Organization

Ponemon Institute, April 2019

Part 1. Introduction

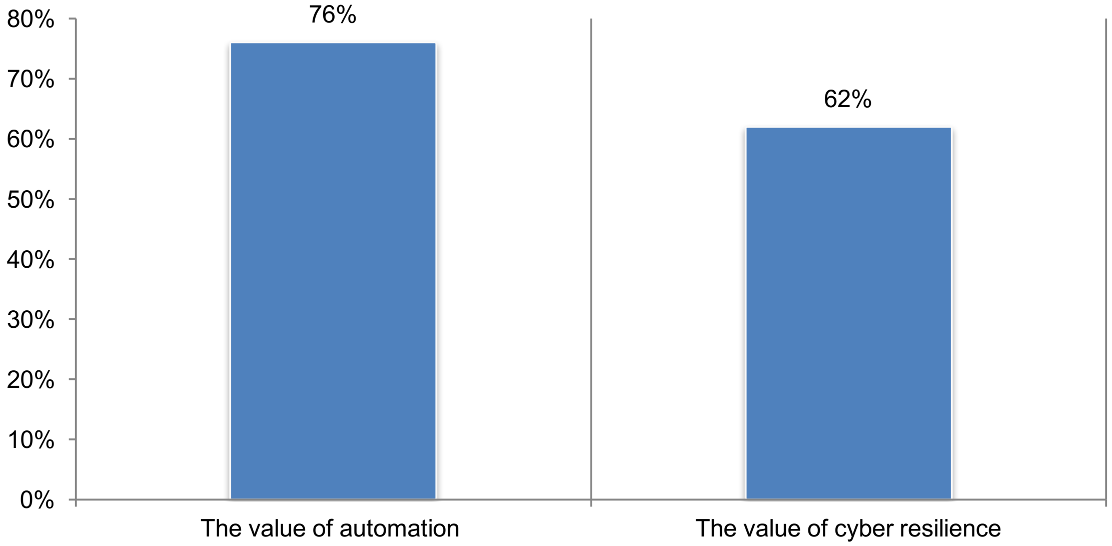
The Ponemon Institute and IBM Resilient are pleased to release the findings of the fourth annual study on the importance of cyber resilience[1] to ensure a strong security posture. For the first time, we feature the importance of automation to cyber resilience. In the context of this research, automation refers to enabling security technologies that augment or replace human intervention in the identification and containment of cyber exploits or breaches. Such technologies depend upon artificial intelligence, machine learning, analytics and orchestration.

Other topics covered in this report are:

- The impact of the skills gap on the ability to be more cyber resilient
- How complexity can be the enemy of cyber resilience
- Lessons learned from organizations that have achieved a high level of cyber resilience
- The importance of including the privacy function in cyber resilience strategies.

Cyber resilience and automation go hand in hand. When asked to rate the value of automation and cyber resilience to their security posture on a scale of 1 = low value to 10 = high value, 62 percent rate the value of cyber resilience as very high and an even higher percentage of respondents (76 percent) find automation very valuable. Moreover, according to the research, 60 percent of respondents say their organizations' leaders recognize that investments in automation, machine learning, artificial intelligence and orchestration strengthen their cyber resilience.

Figure 2. The value of cyber resilience and automation to your organization
From 1 = low to 10 = high, 7+ responses presented



[1] We define cyber resilience as the alignment of prevention, detection and response capabilities to manage, mitigate and move on from cyberattacks. This refers to an enterprise's capacity to maintain its core purpose and integrity in the face of cyberattacks. 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.

How automation supports and improves cyber resilience

In this section, we compare the findings of the 23 percent of respondents who self-reported their organizations use automation extensively (high automation) vs. 77 percent of respondents who use automation moderately, insignificantly or not at all (overall sample). Following are six benefits when automation is used extensively in the organization.

1. High automation organizations are better able to prevent security incidents and disruption to IT and business processes**.** Measures used to determine improvements in cyber resilience are cyberattacks prevented and a reduction in the time to identify and contain the incident.

2. High automation organizations rate their cyber resilience much higher than the overall sample and also rate their ability to prevent, detect, respond to and contain a cyberattack as much higher.

3. Automation increases the importance of having skilled cybersecurity professionals such as security analysts, forensic analysts, developers and SecDevOps. Eighty-six percent of respondents in high automation organizations are more likely to recognize the importance of having cybersecurity professionals in their cybersecurity incident response plan (CSIRP) and are not as likely to have difficulty in hiring these professionals.

4. High automation organizations are maximizing the benefits of threat intelligence sharing and advanced technologies. In every case, respondents in organizations that are extensive users of automation are more likely to believe threat intelligence and sharing, DevOps and secure SDLC, analytics and artificial intelligence are most effective in achieving cyber resilience.

5. Automation can reduce complexity in the IT infrastructure. High automation organizations are more likely to say their organizations have the right number of security solutions and technologies. This can be accomplished by aligning in-house expertise to tools so that investments are leveraged properly. Respondents in the overall sample are more likely to have too many security solutions and technologies.

6. High automation organizations recognize the value of the privacy function in achieving cyber resilience. Most respondents in this research recognize that the privacy role is becoming increasingly important, especially due to the EU's GDPR and the California Consumer Privacy Act. Moreover, high automation organizations are more likely than the overall sample to recognize the importance of aligning the privacy and cybersecurity roles in their organizations (71 percent vs. 62 percent).

Lessons learned from high performing organizations

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

Of the 3,655 organizations represented in this study, 960 respondents (26 percent of the total sample) 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 compared to those who self-reported they have not achieved a high state of high cyber resilience. They are referred to as average performers. Following are seven benefits from achieving a highly effective cyber resilience security posture.

1. High performers are significantly more confident in their ability to prevent, detect, contain and recover from a cyberattack. Of respondents in high performing organizations, 71 percent of respondents in high performing organizations are very confident in their ability to prevent a cyberattack, whereas slightly more than half (53 percent of respondents) from the other organizations believe they have a high ability to prevent a cyberattack.

2. High performers are far more likely to have a CSIRP that is applied consistently across the entire enterprise, which makes this group far more likely to prevent, detect, contain and respond to a cyberattack. Only 5 percent of high performers do not have a CSIRP. In contrast, 24 percent of organizations in the overall sample do not have a CSIRP.

3. Communication with senior leaders about the state of cyber resilience occurs more frequently in high performing organizations. More than half of respondents (51 percent) vs. 40 percent in the overall sample communicate the effectiveness of cyber resilience to the prevention, detection, containment and response of cyberattacks to the C-suite and board of directors.

4. Senior management in high performing organizations are more likely to understand the correlation between cyber resilience and their reputation in the marketplace. Perhaps because of frequent communication with the C-suite. As a result, high performing organizations are more likely to have adequate funding and staffing to achieve cyber resilience.

5. Senior management's awareness about the relationship between cyber resilience and reputation seems to result in greater support for investment in automation, machine learning, AI and orchestration to achieve a higher level of cyber resilience. In fact, 82 percent of respondents in high performing organizations use automation significantly or moderately. In the overall sample of organizations, 71 percent of respondents say their organizations use automation significantly or moderately.

6. High performers are more likely to value automation in achieving a high level of cyber resilience. When asked to rate the value of automation, 90 percent of respondents in high performing organizations say automation is highly valuable to achieving cyber resilience. However, 75 percent of respondents in the overall sample say they place a high value on automation.

7. High performers are more likely to have streamlined their IT infrastructure and reduced complexity. More than half of respondents (53 percent) vs. only 30 percent of respondents in the overall sample say their organizations have the right number of security solutions and technologies to be cyber resilient. The average number of separate security solutions and technologies in high performing organizations is 39 vs. 45 in the overall sample.

Part 2. Key Findings

Ponemon Institute surveyed 3,655 IT and IT security professionals in the following countries: Australia, Brazil, Canada, Germany, France, India, Japan, the Middle East (UAE/Saudi Arabia), Southeast Asian countries (ASEAN), the United Kingdom and the United States. 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:

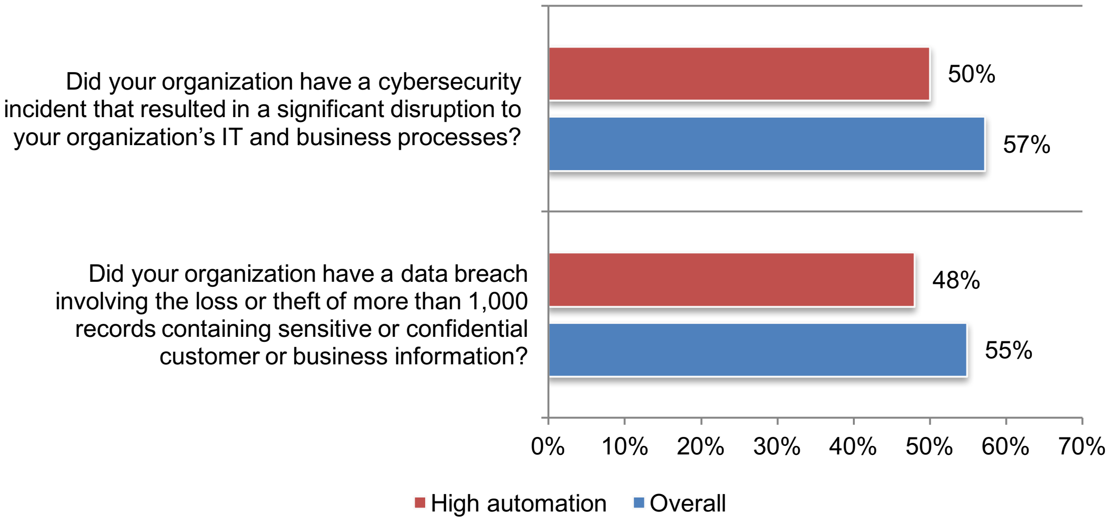
1. The extensive use of automation and its impact on cyber resilience
2. Collaboration between privacy and cybersecurity to improve cyber resilience
3. Steps taken to achieve cyber resilience
4. The characteristics of organizations with a high degree of cyber resilience

2.1 The extensive use of automation and its impact on cyber resilience

For the first time in our research on cyber resilience, we include the impact of automation on cyber resilience. In this section, we compare the findings of the 23 percent of respondents who self-reported their organizations use automation extensively (high automation) vs. the 77 percent of respondents who use automation moderately, insignificantly or not at all (overall sample).

Automation reduces the likelihood of a data breach and cybersecurity incident. According to Figure 2, 57 percent of respondents in organizations that **do not** use automation extensively vs. 50 percent in the high automation sample experienced a cybersecurity incident that resulted in a significant disruption to their organizations' IT and business processes. Similarly, less than half of organizations that use automation extensively (48 percent) had a data breach vs. the 55 percent who did in the overall sample.

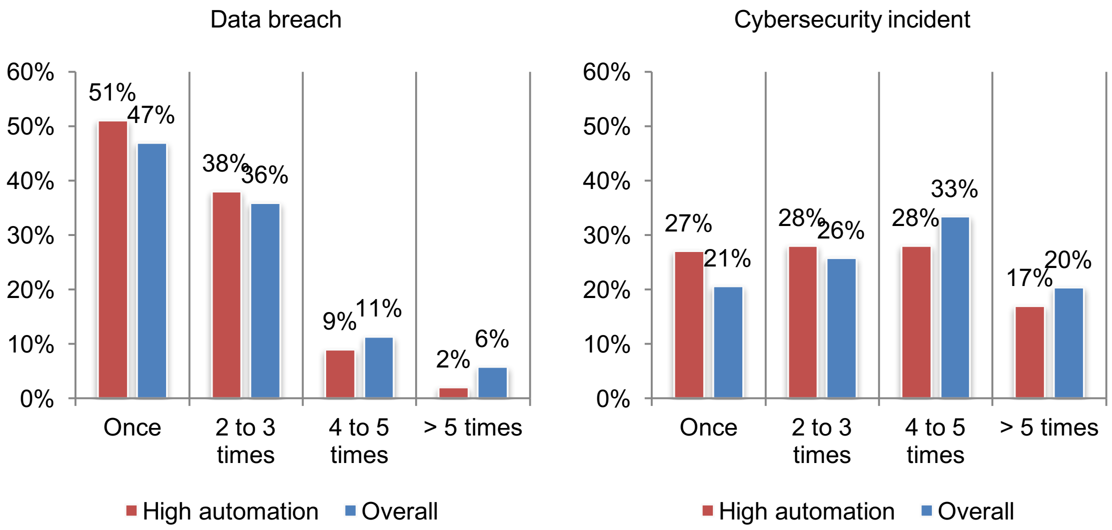
Figure 2. Did your organization have a data breach or cybersecurity incident in the past two years?
Yes responses presented



Automation reduces the frequency of data breaches and cybersecurity incidents. Companies that extensively use automation are more likely to prevent frequent occurrences of these incidents, as shown in Figure 3. Specifically, 53 percent of organizations in the overall sample had more than one data breach, while less than half (49 percent) in the high automation organizations had more than one.

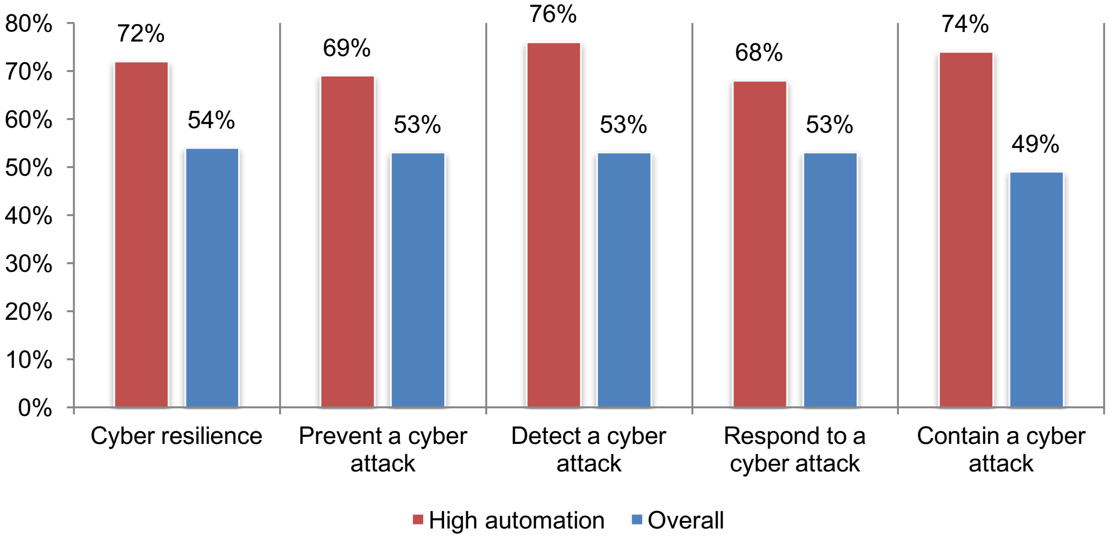
Similarly, 73 percent of respondents in high automation organizations had more than one cybersecurity incident in the past two years, but 79 percent of respondents in the overall sample had more than one cybersecurity incident.

Figure 3. If yes, how frequently did these incidents occur?



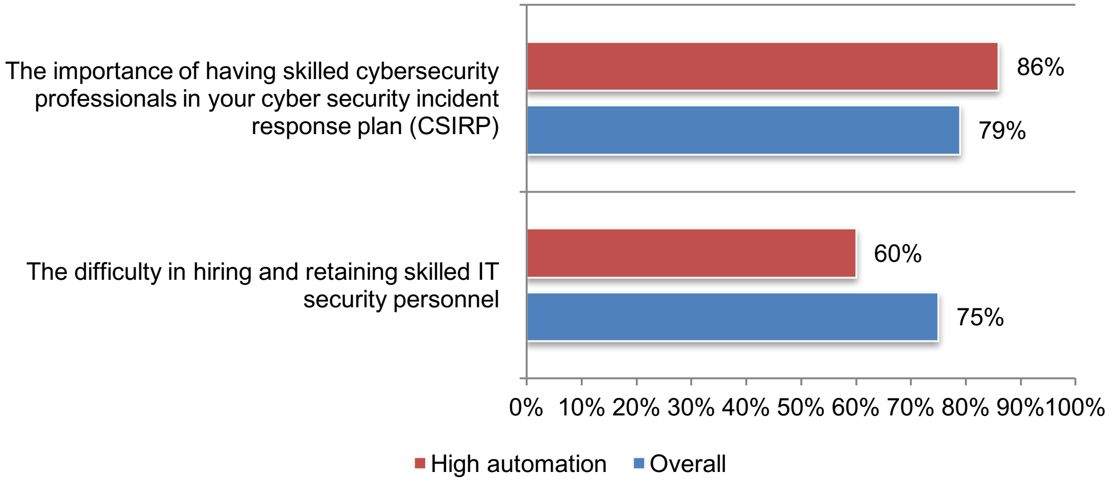
Companies can achieve significant improvements in their cyber resilience with automation. Respondents were asked to rate their organizations' cyber resilience on a scale of 1 = low to 10 = high. According to Figure 4, 72 percent of respondents with the extensive use of automation say their organizations have achieved a high level of cyber resilience, while 54 percent in the overall sample report they have high cyber resilience. Organizations with the extensive use of cyber resilience also rate their ability to prevent, detect, respond and contain a cyberattack as much higher than the overall sample of respondents.

Figure 4. Automation improves cyber resilience and the ability to prevent, detect, contain and respond to a cyberattack
From 1 = low to 10 = high, 7+ responses presented



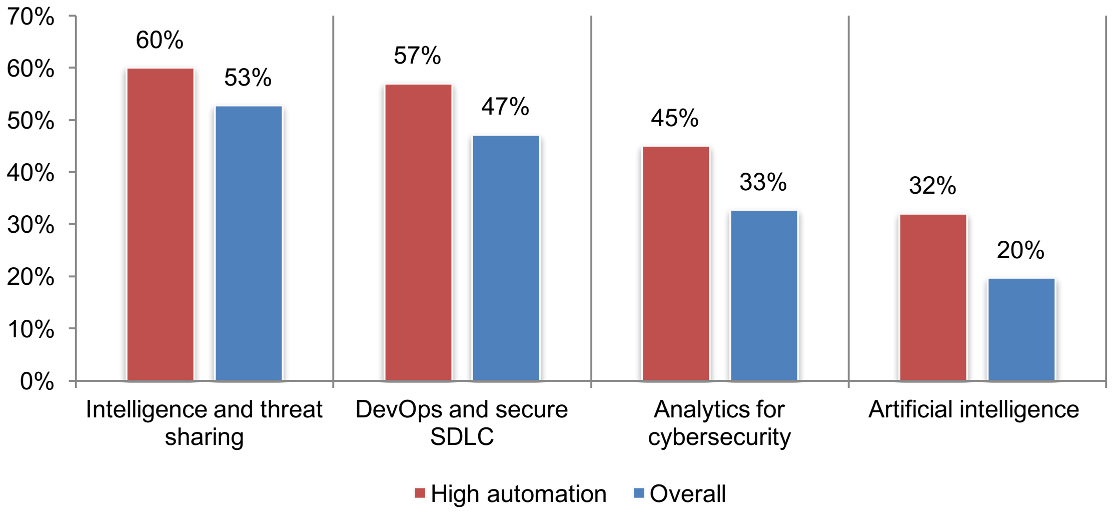
Automation increases awareness of the importance of having skilled cybersecurity professionals. As shown in Figure 5, 86 percent of respondents in organizations with the extensive use of automation are more likely to recognize the importance of having cybersecurity professionals in their CSIRP and are not as likely to have difficulty in hiring these professionals.

Figure 5. The importance of having skilled cybersecurity professionals and the difficulty in hiring them
From 1 = low to 10 = high, 7+ responses presented



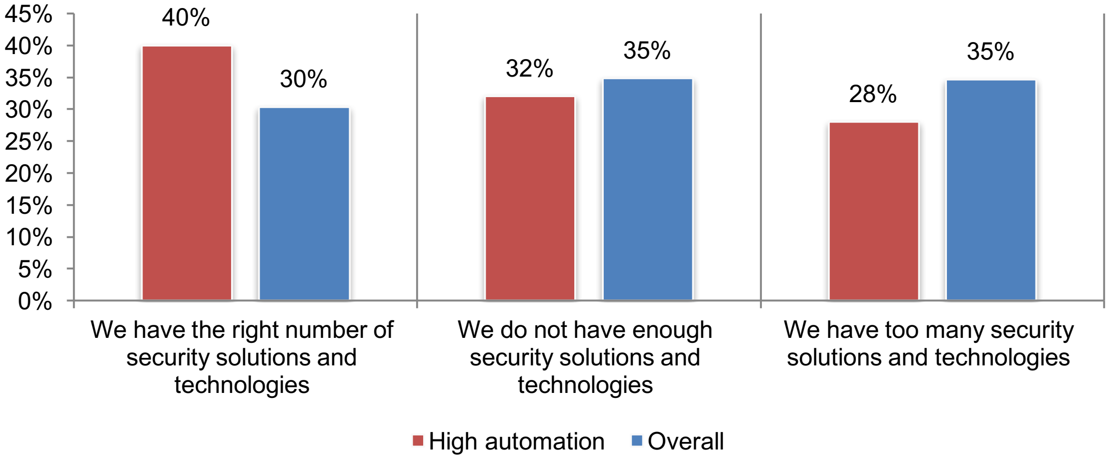
Organizations with the extensive use of automation are maximizing the benefits of threat sharing and advanced technologies. Figure 6 presents the differences between organizations in highly automated organizations and the overall sample of respondents. In every case, respondents in organizations that extensively use automation are more likely to believe intelligence and threat sharing, DevOps and secure SDLC, analytics and artificial intelligence are the most effective in being able to achieve cyber resilience. Threat sharing and the use of advanced technologies enable organizations to better understand the cybersecurity risks they face, and, as a result, the organizations are better able to prevent, detect, contain and respond to attacks.

Figure 6. What security technologies are most effective in the ability to achieve cyber resilience?
More than one response permitted



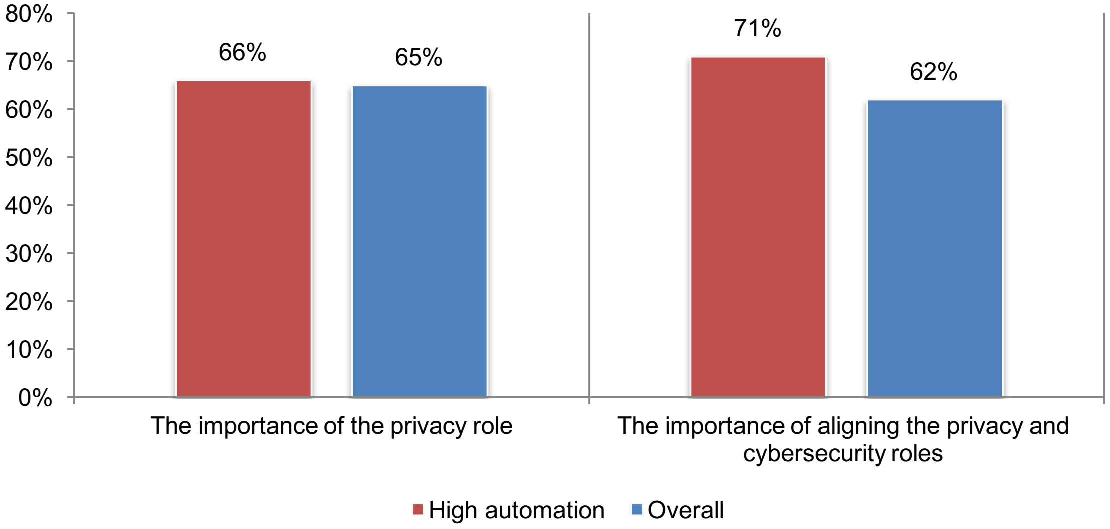
Automation can reduce complexity in the IT infrastructure. Respondents were asked to indicate if their organizations had the right number of security solutions and technologies or if there were too many which can lead to complexity. According to Figure 7, 40 percent of respondents in organizations that extensively use automation are more likely to say their organizations have the right number of security solutions and technologies. Respondents in the overall sample are more likely to have too many security solutions and technologies.

Figure 7. What best describes your organization's use of separate security technologies?



Organizations recognize the importance of the privacy function in achieving cyber resilience. According to Figure 8, most respondents believe that the privacy role is becoming increasingly important, especially due to the EU's GDPR and the California Consumer Privacy Act. However, respondents in organizations that extensively use automation are more likely than the overall sample to recognize the importance of aligning the privacy and cybersecurity roles in their organizations (71 percent vs. 62 percent).

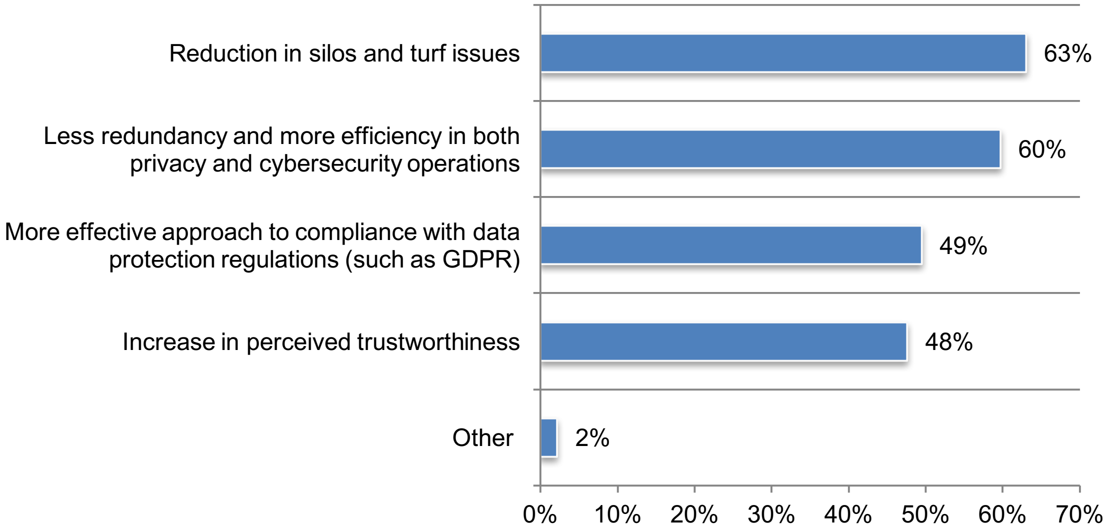
Figure 8. The importance of privacy and aligning privacy and cybersecurity roles to achieving cyber resilience within your organization
Essential and Very important responses combined



2.2 Collaboration between privacy and cybersecurity to improve cyber resilience

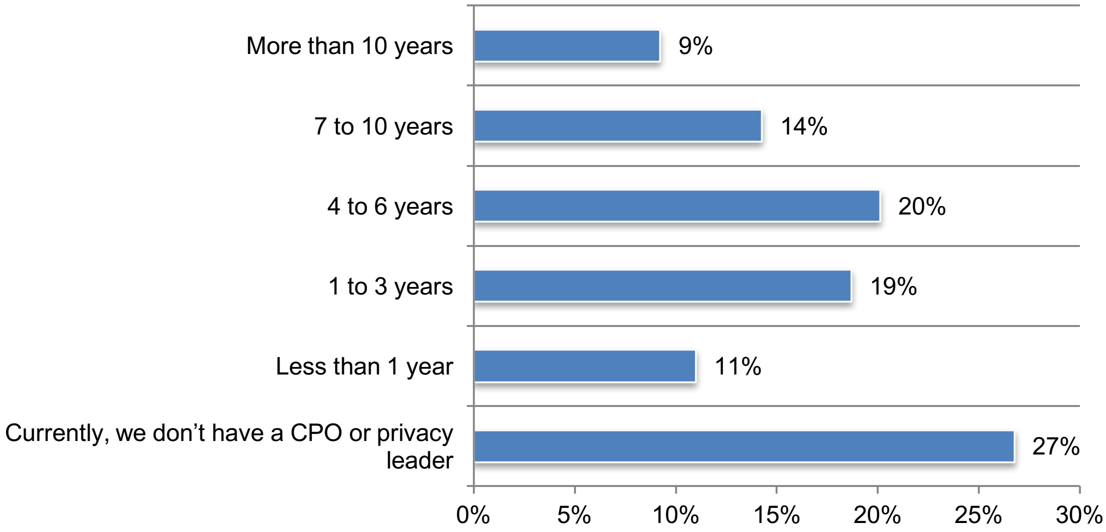
Alignment between privacy and cybersecurity reduces turf issues and increases efficiency. As previously discussed, most respondents (62 percent) recognize the importance of the privacy role and the alignment of privacy and cybersecurity roles in achieving cyber resilience. As shown in Figure 9, of these respondents, 63 percent say such alignment reduces silo and turf issues followed by less redundancy and more efficiency in both privacy and cybersecurity operations.

Figure 9. If alignment is essential or very important, why?
More than one response permitted



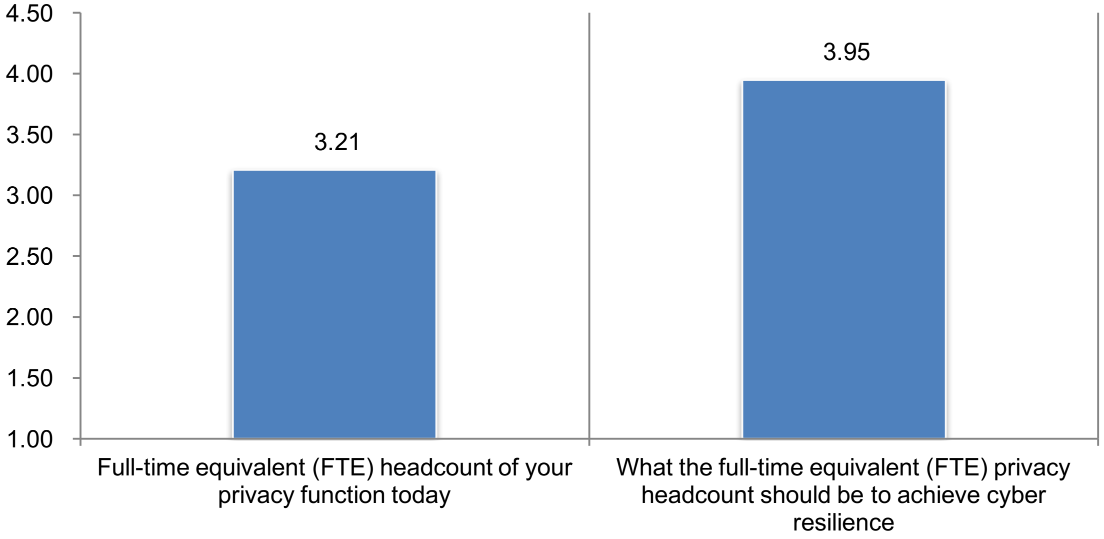
Most organizations have a privacy leader. The good news is that most organizations have a chief privacy officer (73 percent of respondents), as shown in Figure 10. However, only 23 percent of respondents say they have been in that position for a significant length of time (more than 7 years).

Figure 10. How long has your organization's current CPO or privacy leader held their position?



Privacy functions are slightly understaffed. With the many data protection regulations organizations must comply with, a fully staffed privacy function is essential. According to Figure 11, the average headcount in the privacy function is about 3, but ideally, it should be a headcount of 4. Because of new regulations, such as the EU's GDPR and the California Privacy Act, there is a need to increase staff to help achieve compliance. Only slightly more than half of respondents (54 percent) say their organizations have achieved full compliance with GDPR.

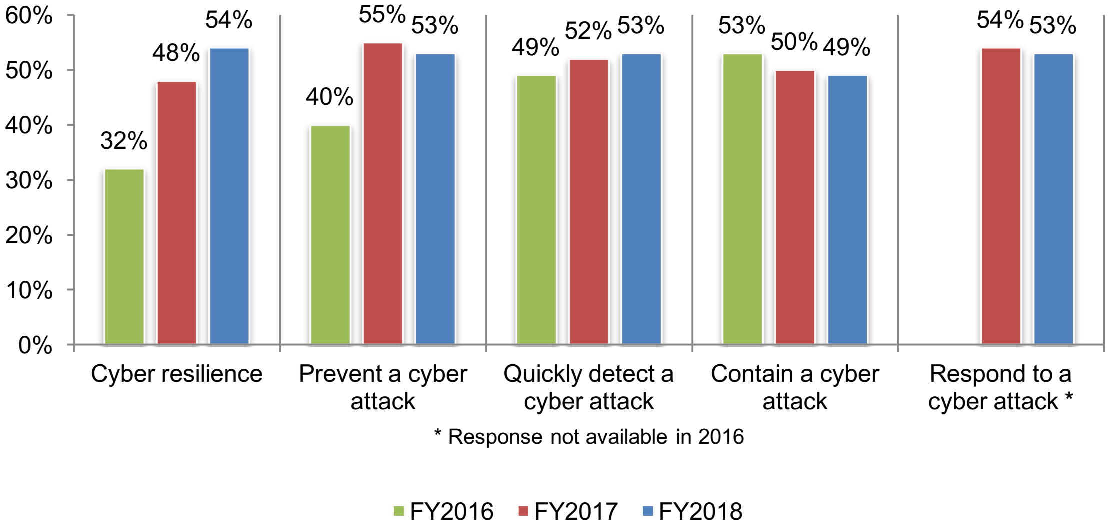
Figure 11. Average full-time headcount of the organization's privacy function today and what it should be
Extrapolated values presented



2.3 Steps taken to achieve cyber resilience

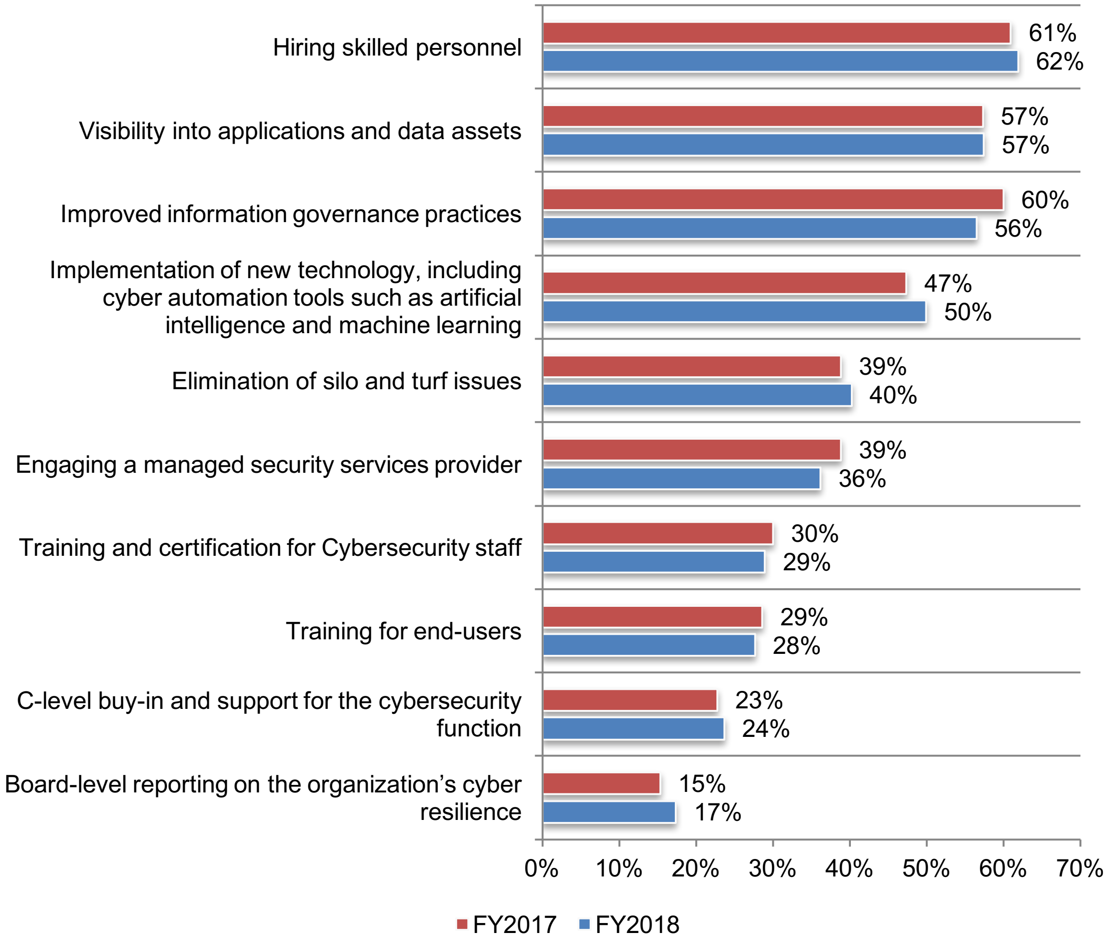
Cyber resilience reaches a new high. Figure 12 shows the trends in cyber resilience and the ability to prevent, detect, contain and respond to a cyberattack. When asked to rate their cyber resilience on a scale of 1 = low cyber resilience to 10 = high cyber resilience, 54 percent of respondents say cyber resilience is very high, a significant increase from last year's study. The majority of respondents rate their ability to prevent (53 percent), detect (53 percent), contain (49 percent) and respond (53 percent) to a cyberattack as very high.

Figure 12. Cyber resilience and the ability to prevent, detect, contain and respond to a cyberattack
1 = low ability to 10 = high ability, 7+ responses reported



To improve cyber resilience, organizations focus on people, process and technologies. Forty-four percent of respondents say their organizations' cyber resilience has significantly improved or has improved in the past 12 months. These respondents cite a variety of steps taken to becoming more cyber resilient. The most important (62 percent of respondents) say they added skilled personnel, and 57 percent of respondents say their organizations' technologies enabled greater visibility into applications and data assets. Fifty-six percent of respondents say their organizations' governance practices improved.

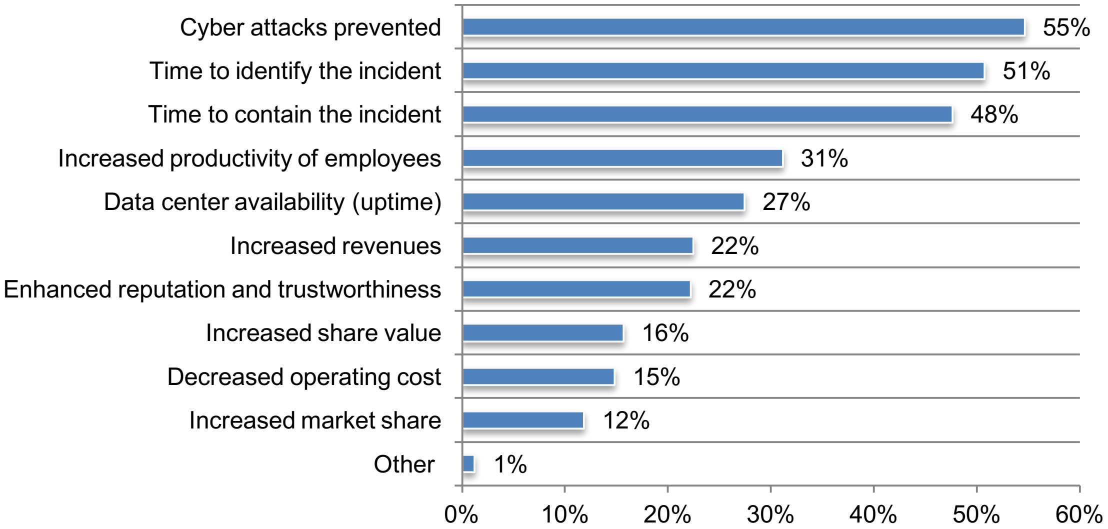
Figure 13. Steps taken to significantly improve cyber resilience



The prevention of cyberattacks is mostly used to measure improvements in cyber resilience. Forty-four percent of respondents say their organizations' cyber resilience significantly improved or improved over the past 12 months and specific metrics are used to understand the reasons for improvement.

According to Figure 14, 55 percent of respondents say improvements are tracked by the number of cyberattacks prevented. This is followed by time to identify the incident and time to contain the incident (51 percent and 48 percent of respondents, respectively).

Figure 14. How does your organization measure your improvements?
More than one response permitted



Funding for cyber resilience activities is predicted to remain stagnant. More resources are needed to fund cyber resilience activities. Only 33 percent of respondents say funding for IT security is sufficient to achieve a high level of cyber resilience.

Respondents were asked what their organizations' 2019 budget will be for cyber security and cyber resilience. As shown in Table 1, the average budget for cyber resilience will hardly increase from $3.4 to $3.6 million.

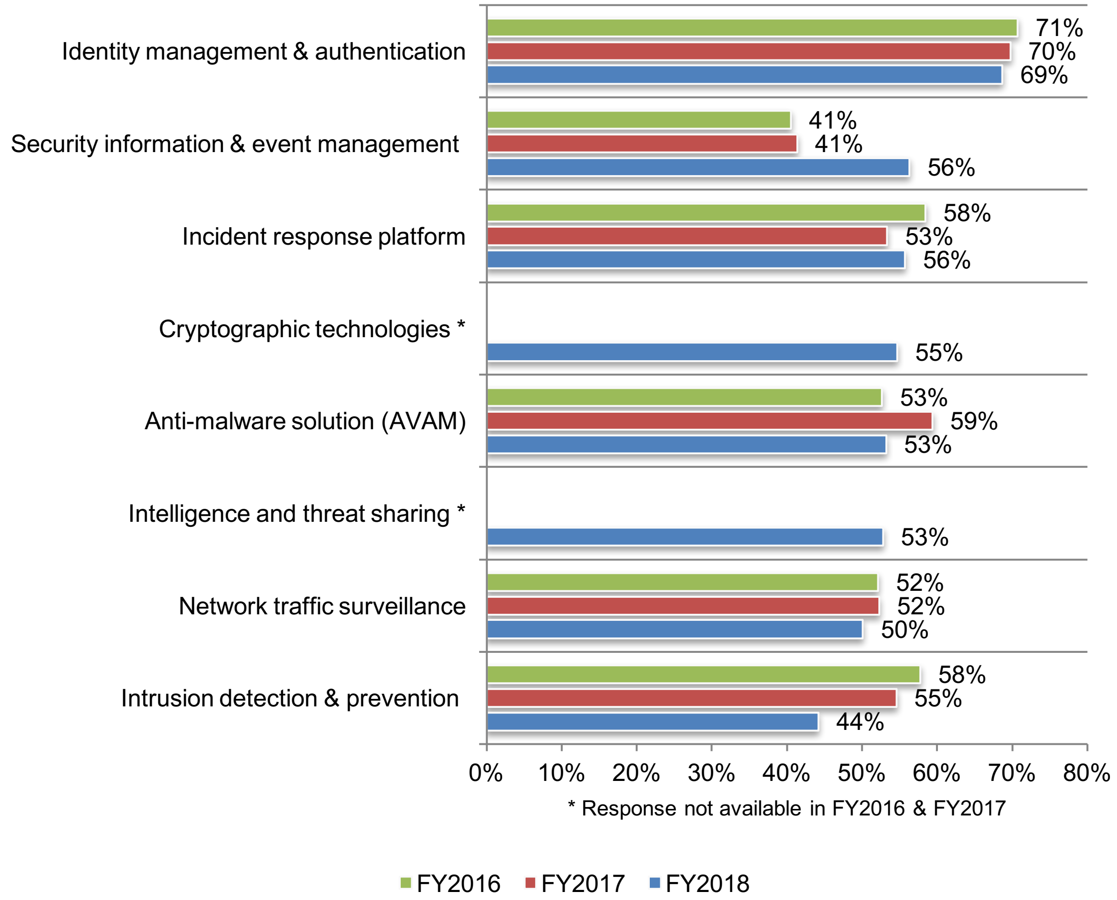
Table 1. Budget for cybersecurity and cyber resilience activities

Extrapolated average (millions)	2019	2017	2016
Cybersecurity budget	$11.6	$11.3	$11.4
Percentage allocated to cyber resilience activities	31%	30%	30%
Total average budget allocated to cyber resilience	$3.6	$3.4	$3.4

Identity management and 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.

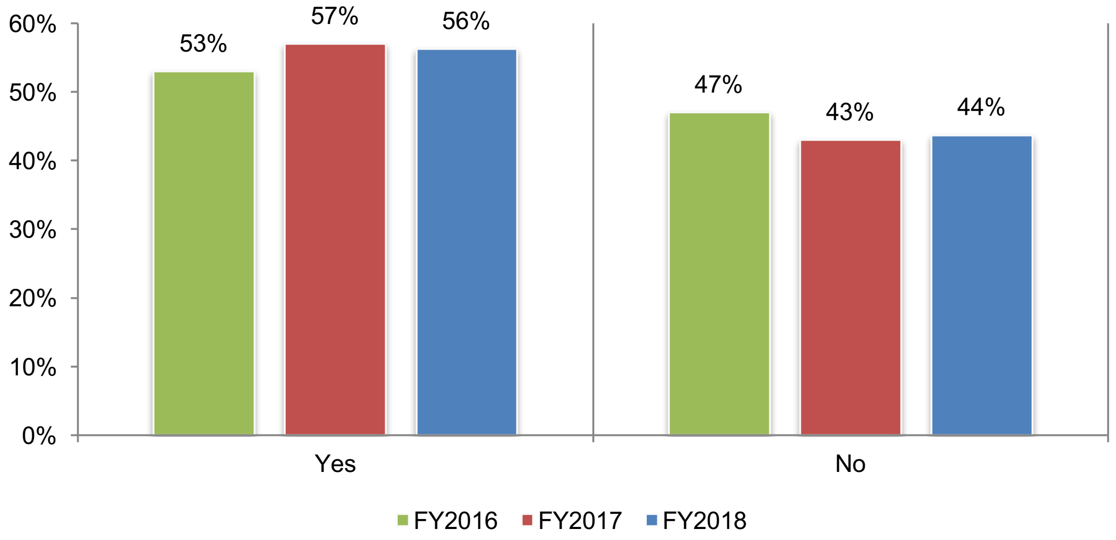
As shown in Figure 15, IAM continues to be considered the most effective technology for cyber resilience (69 percent of respondents). The effectiveness of security information and event management (SIEM) has increased significantly from 41 percent to 56 percent of respondents. Incident response platforms are considered the third most effective technology. For the first time, we included cryptographic technologies and intelligence and threat sharing. Fifty-five percent and 53 percent of respondents respectively say these technologies are effective, respectively.

Figure 15. The eight most effective security technologies
Twenty-two technologies were listed in the survey instrument



Sharing threat intelligence improves cyber resilience. As shown in Figure 16, 56 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.

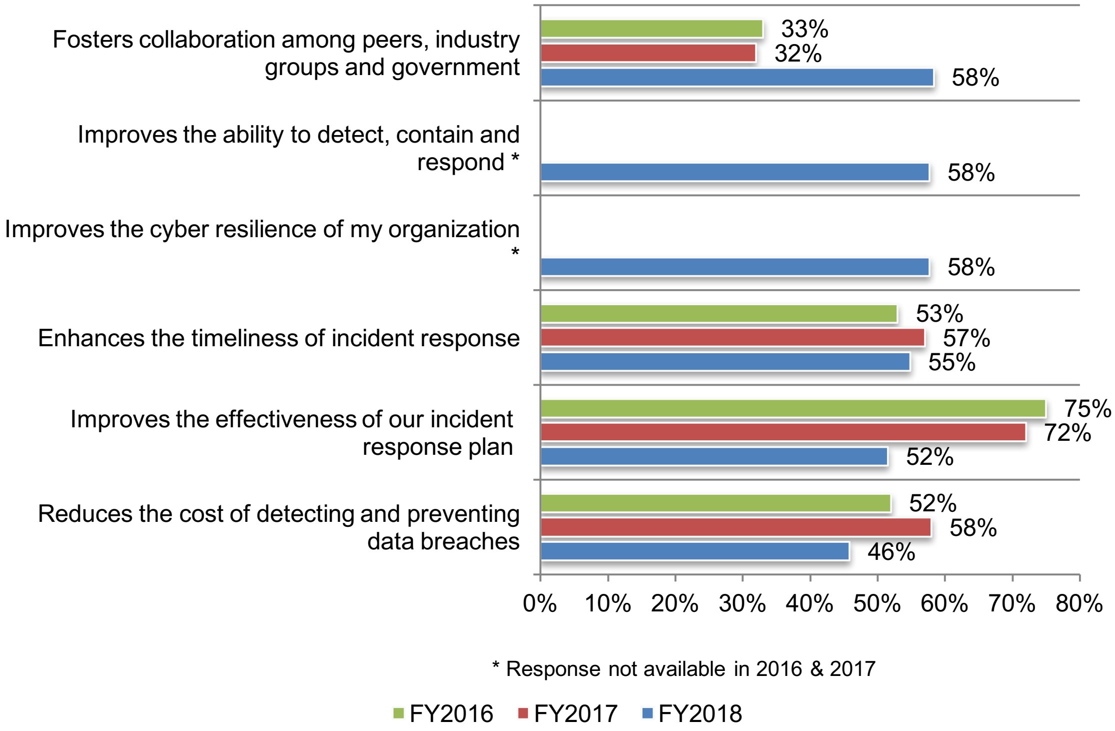
Figure 16. Does your organization participate in an initiative or program for sharing information with government and/or industry peers about cyber threats and vulnerabilities?



In this year's research, there have been significant changes in why organizations are participating in threat intelligence. As shown in Figure 17, more respondents (58 percent) say their organizations benefit from collaboration among peers, industry groups and the government; this is an increase from 32 percent of respondents in 2017. For the first time, we asked if threat intelligence sharing improves cyber resilience and the ability to detect, contain and respond to security incidents. A significant percentage of respondents (58 percent) say these are important reasons to share threat intelligence.

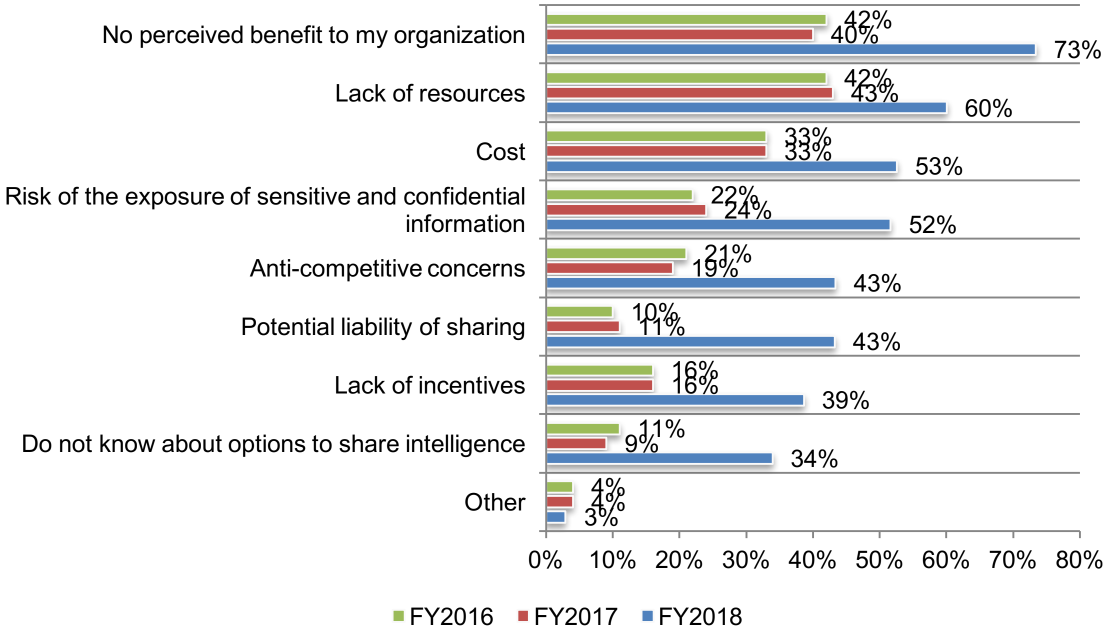
Two benefits have declined significantly. These are threat intelligence sharing improves the effectiveness of the incident response plan and reduces the cost of detecting and preventing data breaches. A possible reason for the decline is that organizations believe improvements in incident response plans and the ability to reduce the cost of detecting and preventing data breaches are best achieved using their in-house expertise.

Figure 17. Why does your organization share information about its data breach experience and incident response plans?
Three choices allowed



If they don't share, it is mostly due to not understanding the benefits. Forty-four percent of respondents say their organizations do not share threat intelligence. According to Figure 18, 73 percent of these respondents, an increase from 40 percent of respondents, believe there is no perceived benefit to their organization. Lack of resources, cost and risk of the exposure of sensitive and confidential information (60 percent, 53 percent and 52 percent of respondents, respectively) are other reasons for not participating in a threat-sharing program.

Figure 18. Why doesn't your organization participate in a threat-sharing program?
Four responses permitted



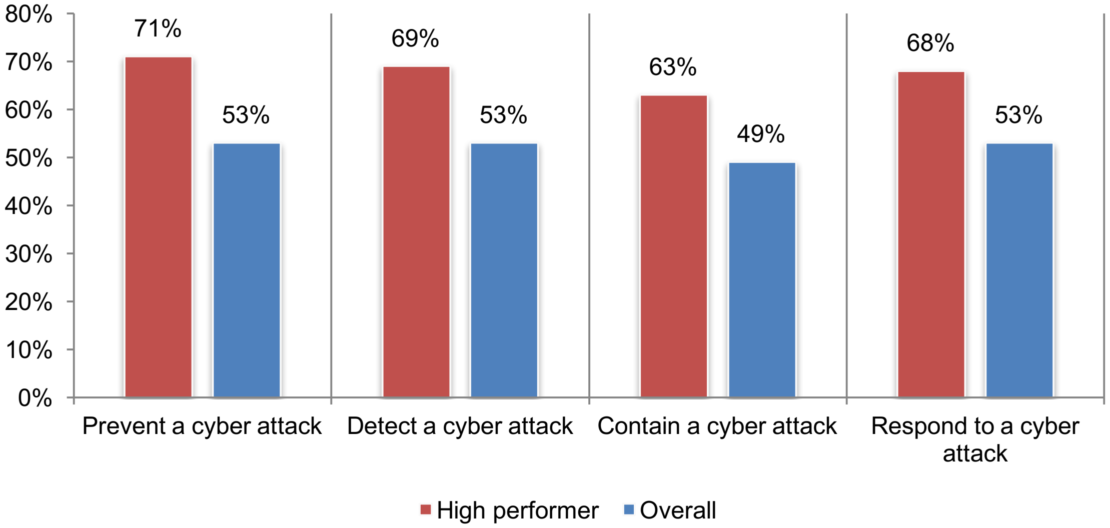
2.4 The characteristics of organizations with a high degree of cyber resilience

As part of this research, we identified organizations represented in this study that self-reported having achieved a high level of cyber resilience and are better able to mitigate risks, vulnerabilities and attacks. We refer to these organizations as high performers. In this section, we analyze how these organizations are able to achieve a higher cyber resilience security posture.

Of the 3,655 organizations represented in this study, 960 respondents (26 percent of the total sample) self-reported 9+ on a scale of 1 = low resilience to 10 = high resilience. Respondents from these organizations are much more confident in the strength of their security posture compared to those who self-reported they have not achieved a state of high cyber resilience. They are referred to as average performers.

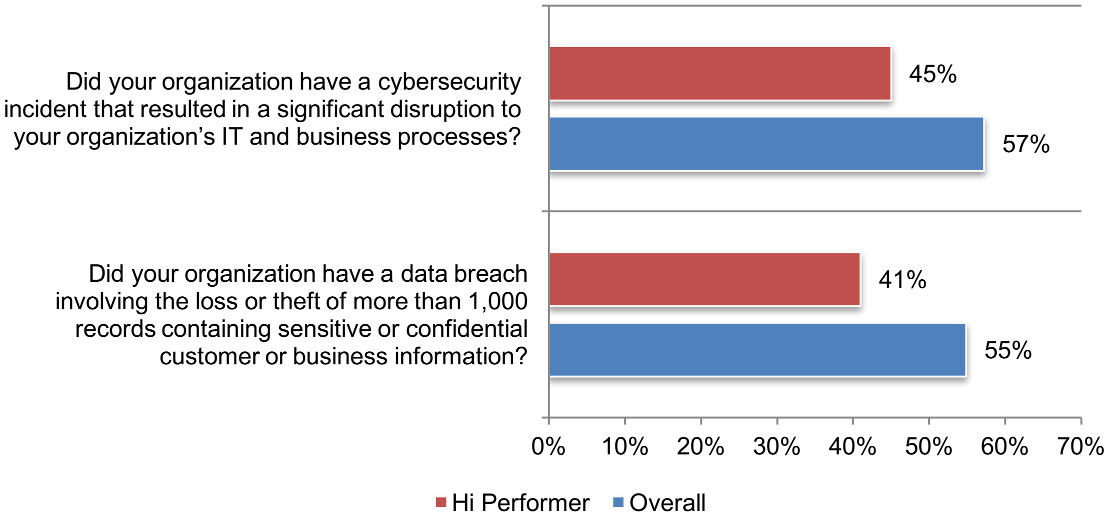
High performers are significantly more confident in their ability to prevent, detect, contain and recover from a cyberattack. As shown in Figure 19, 71 percent of respondents in high performing organizations are highly confident in their ability to prevent a cyberattack, whereas 53 percent of respondents from the other organizations believe they have a high ability to prevent a cyberattack. Other differences in the ability to detect, contain and respond are presented in this figure.

Figure 19. Organizations confident in preventing, detecting, containing and responding to a cyberattack
1 = low ability to 10 = high ability, 7+ responses reported



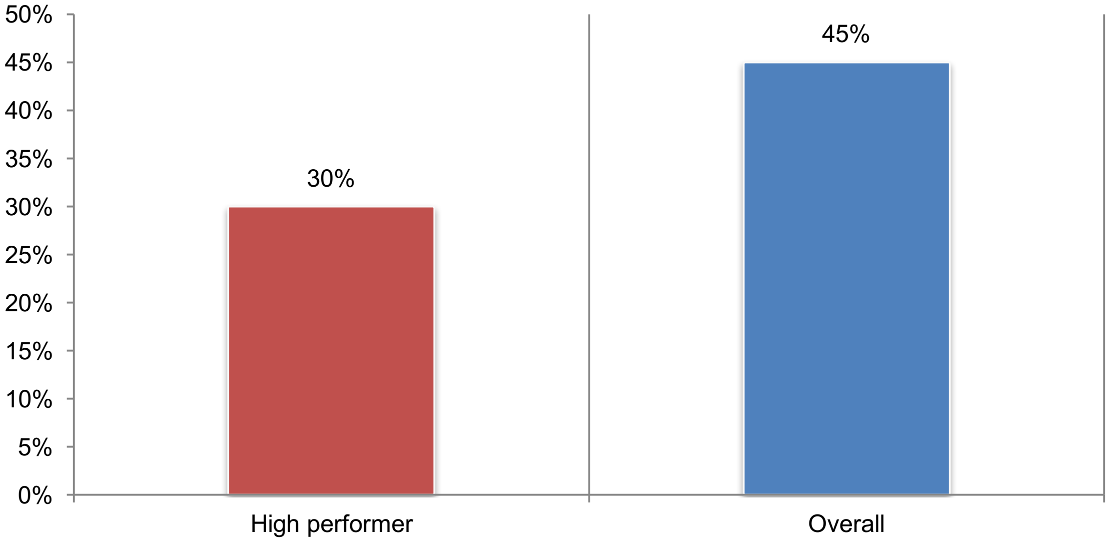
High performers have fewer data breaches and business disruptions. Respondents in high performing organizations are reporting fewer data breaches and cybersecurity incidents than other organizations. As shown in Figure 20, 57 percent of respondents in the overall sample say their organization had a cybersecurity incident that resulted in a significant disruption to their organization's IT and business processes versus 45 percent of respondents in the high performer samples. Similarly, 55 percent of respondents in the overall sample say their organizations had a data breach involving the loss or theft of more than 1,000 records containing sensitive or confidential customer or business information versus 41 percent of respondents in high performing organizations.

Figure 20. Did your organization have a data breach or cybersecurity incident?
Yes responses presented



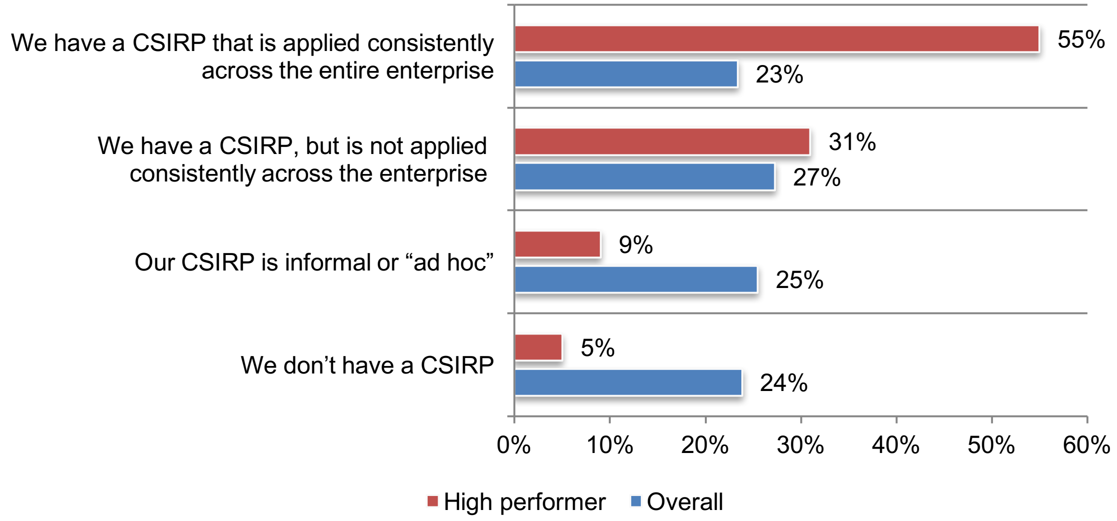
As shown in Figure 21, high performers also report fewer disruptions to business processes or IT operations (30 percent vs. 45 percent of respondents).

Figure 21. As a result of data breaches and cybercrime incidents, how frequently do disruptions to business processes or IT services occur?
Very frequently and Frequently responses combined



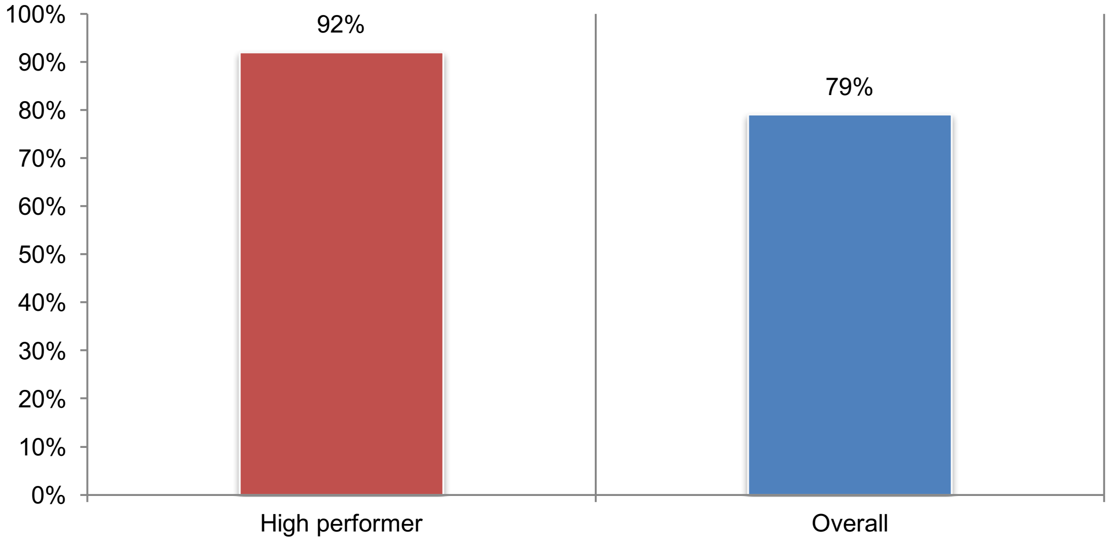
High performers have enterprise-wide CSIRPs. As shown in Figure 22, high performing organizations are far more likely to have a CSIRP that is applied consistently across the entire enterprise (55 percent of respondents vs. 23 percent of respondents), which makes this group far more likely to prevent, detect, contain and respond to a cyberattack.

Figure 22. What best describes your organization's cybersecurity incident response plan (CSIRP)?



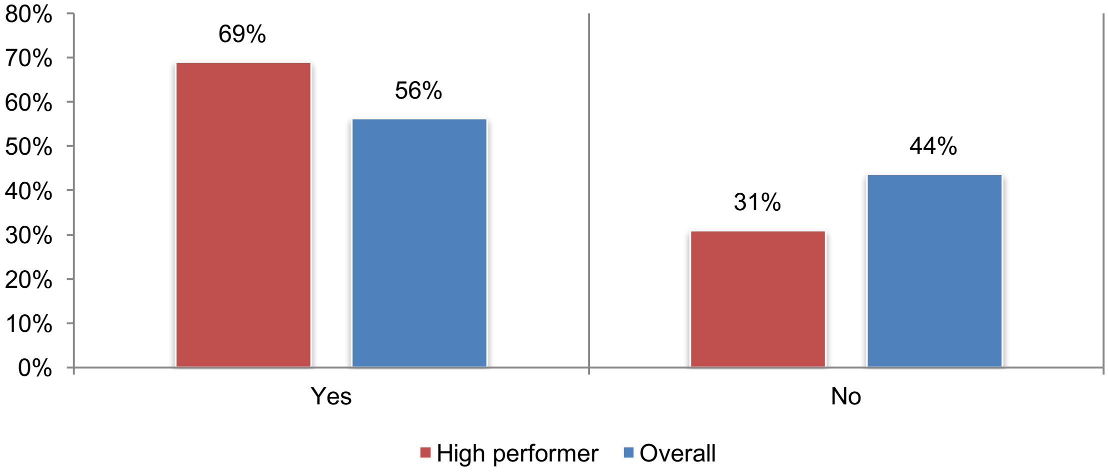
Moreover, 92 percent of respondents in high performers vs. 79 percent in the overall sample believe in the importance of having skilled cybersecurity professionals in their CSIRP, as shown in Figure 23.

Figure 23. It is very important to have skilled cybersecurity professionals in a CSIRP
1 = low importance to 10 = high importance, 7+ responses reported



High performers believe in sharing intelligence regarding data breaches and cyber exploits. As shown in Figure 24, 69 percent of respondents in high performing organizations say their organizations share information regarding data breaches they experienced with government and industry peers.

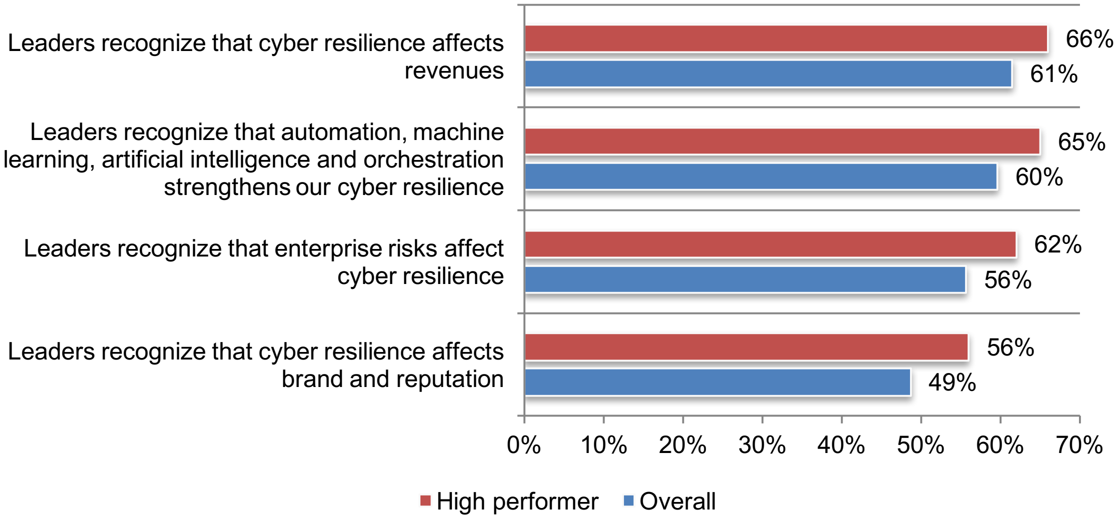
Figure 24. Does your organization share information about data breaches with government or industry peers?



Senior management in high performers understands the correlation between cyber resilience and reputation. As shown in Figure 25, high performing organizations benefit from a supportive senior leadership. Specifically, 66 percent of respondents say leaders recognize that cyber resilience affects revenues, and 56 percent of respondents say cyber resilience impacts brand and reputation.

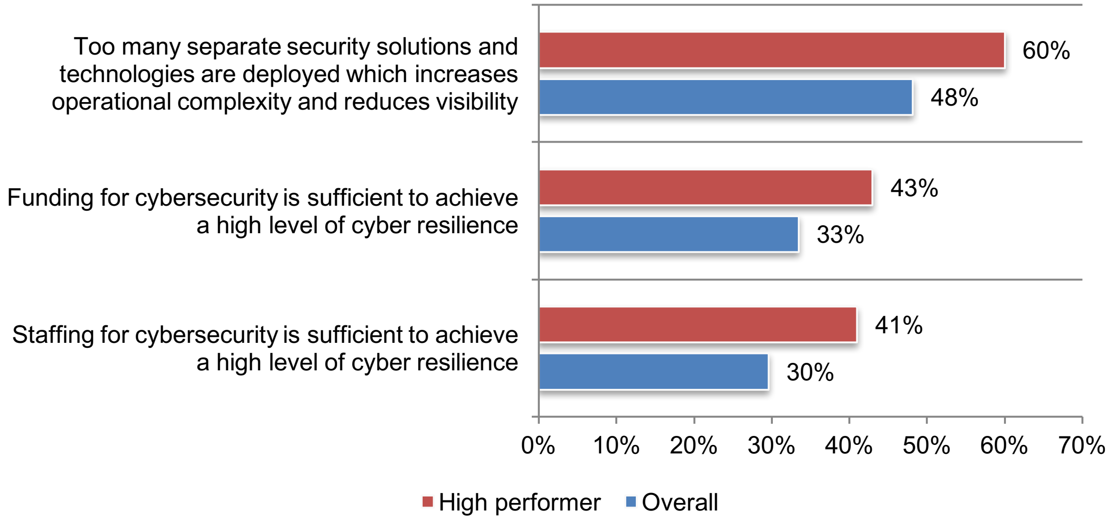
Awareness of the importance of cyber resilience results in leaders understanding that automation, machine learning, AI and orchestration strengthens cyber resilience. As a result, respondents in high performing organizations are more likely to have adequate funding and staffing with which to achieve cyber resilience.

Figure 25. Senior management's awareness about the positive impact of cyber resilience on the enterprise
Strongly agree and Agree responses combined



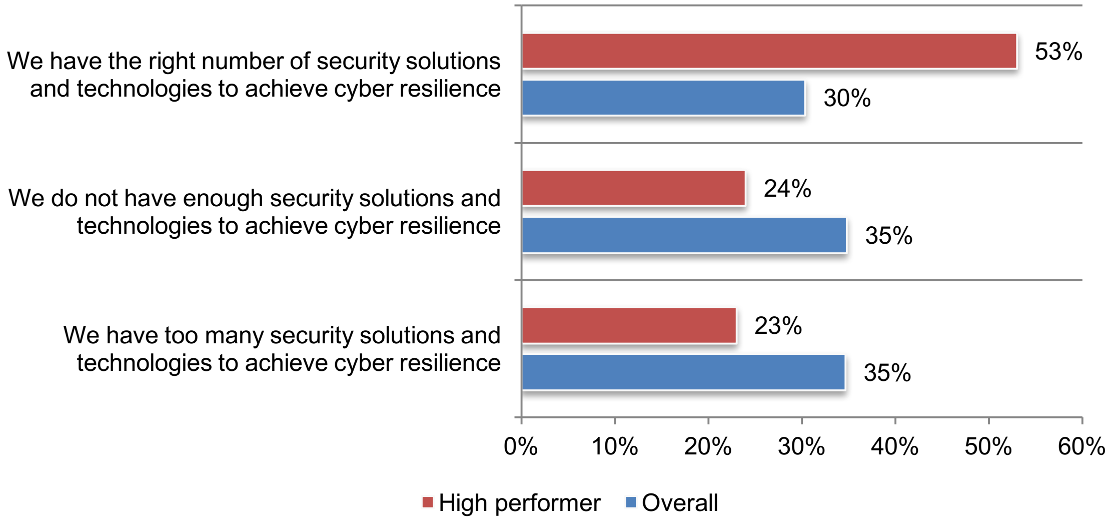
High performers believe complexity in the IT infrastructure reduces visibility and, as a result, cyber resilience. As shown in Figure 26, 60 percent of high performers vs. 48 percent of the overall sample believe too many separate security solutions and technologies increase operational complexity and reduce visibility. These high performers are also able to have more funding and staff.

Figure 26. Differences in the ability to achieve a high level of cyber resilience
Strongly agree and Agree responses combined



High performers are more likely to reduce complexity in their IT infrastructures. According to Figure 27, more than half of respondents in high performing organizations (53 percent) vs. only 30 percent of respondents in the overall sample say their organizations have the right number of security solutions and technologies to achieve cyber resiliency. Specifically, high performers have an average of 39 solutions vs. an average of 45 solutions in the overall sample. The right number of security solutions can be based upon the ability to meet the goals of the security program with the necessary in-house expertise to leverage investments in technologies.

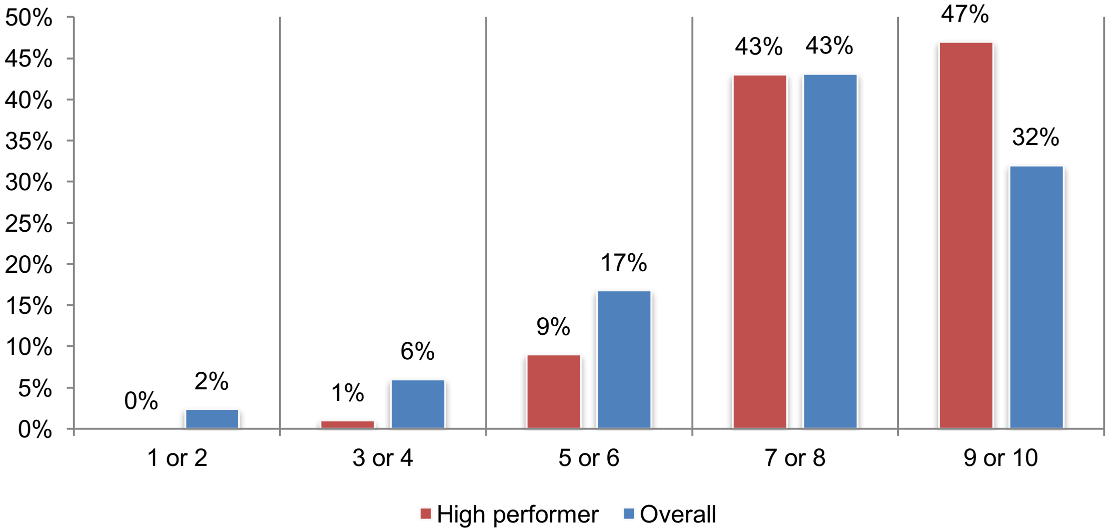
Figure 27. What one statement best describes the number of separate security technologies deployed by your organization



High performers are more likely to value automation in achieving a high level of cyber resilience. When asked to rate the value of automation on a scale of 1 = low value to 10 = high value, 90 percent of respondents say automation is highly valuable to achieving cyber resilience (7+ responses on the 10-point scale), while 75 percent of the overall sample say they place a high value on automation, according to Figure 28.

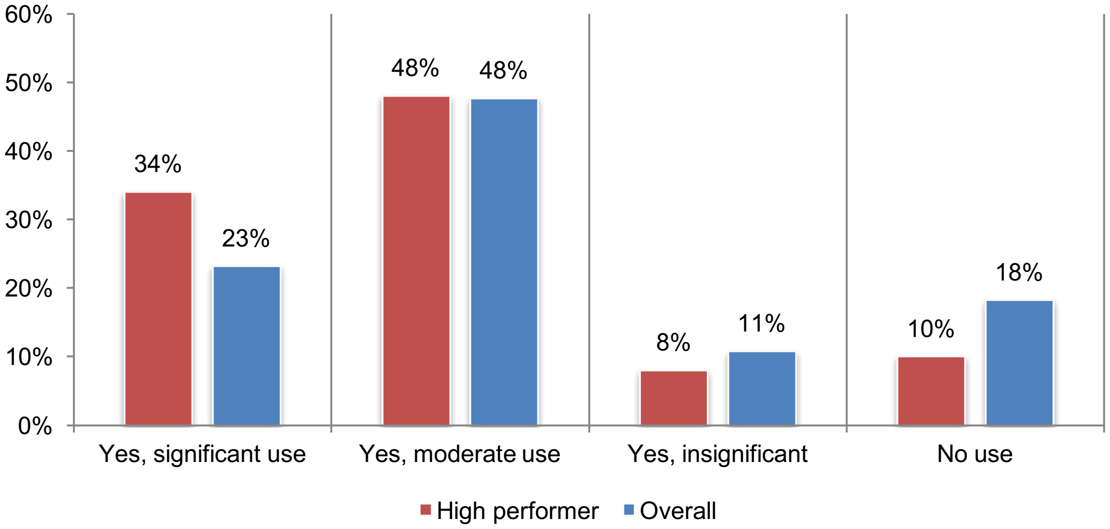
Figure 28. Please rate the value of automation on achieving a high level of cyber resilience

On a scale From 1 = low value to 10 = high value



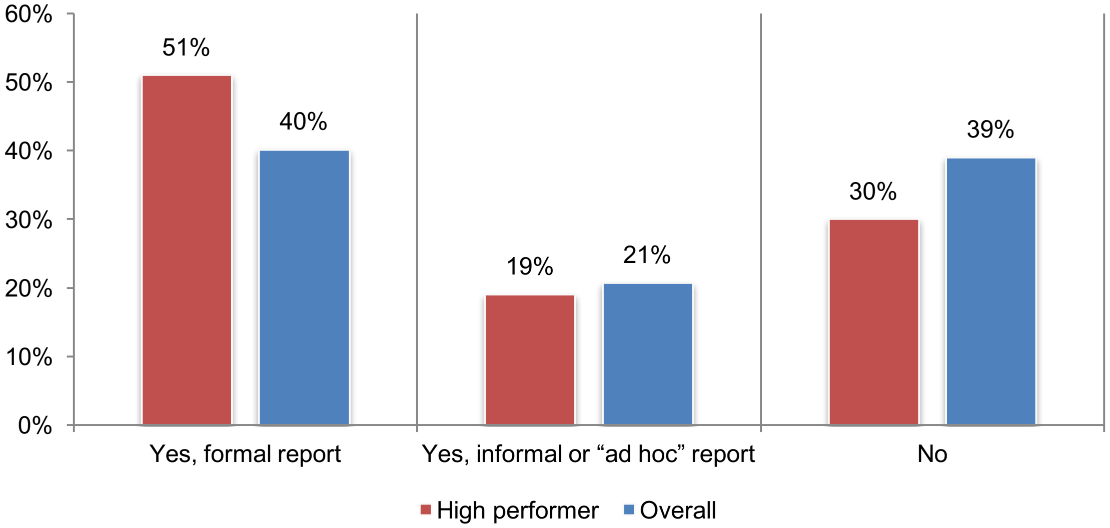
Because high performers are more likely to perceive the value of automation, they are more likely to use automation extensively. As shown in Figure 29, 82 percent of high performer organizations are using automation significantly or moderately. Seventy-one percent of respondents in the overall sample have this level of usage.

Figure 29. What best describes your organization's use of automation? Include both artificial intelligence and machine learning as part of automation.



Communication with senior leaders about the state of cyber resilience occurs more frequently in high performers. According to Figure 30 more than half of respondents (51 percent) vs. 40 percent in the overall sample communicate the effectiveness of cyber resilience to the prevention, detection, containment and response of cyberattacks to the C-suite and board of directors.

Figure 30. Does your organization report the state of cyber resilience to C-level executives and/or the board of directors?



Conclusion and Recommendations

Since first conducting this research in 2015, the cyber resilience of companies has steadily improved. To understand the reasons for improvement and what recommendations can be made to continue the improvement, we conducted a special analysis of those organizations that are extensively using automation throughout the enterprise and organizations that self-reported they have achieved a high level of cyber resilience.

The following are recommendations for achieving a high level of cyber resilience.

- When asked why their organizations’ cyber resilience security posture improved, the two top reasons are hiring skilled IT security professionals and investing in technologies and processes to improve visibility into applications and data assets. As shown in this research, automation increases the importance of having the necessary in-house expertise.

- Invest in automation to reduce complexity and streamline the IT infrastructure. Having too many unnecessary security solutions and technologies can reduce cyber resilience.

- The key metrics to use in assessing improvements in cyber resilience are the ability to prevent cyberattacks, reduce the time to identify and contain the incident. These measurements should be reported to the C-suite on a regular basis to demonstrate the importance of being cyber resilient and to increase funding of activities to achieve a stronger security posture.

- Deploy a CSIRP extensively throughout the enterprise to increase the likelihood of preventing an attack as well as reducing the time to detect, contain and respond to an attack.

- Align the privacy and cybersecurity functions to reduce silo and turf issues and increase the efficiency of complying with the numerous data protection regulations and respond to data breaches and other security incidents.

- The privacy function should be considered a valuable and integral part of cyber resilient strategies. Organizations in this research are struggling to achieve full compliance with the EU's GDPR. Privacy and cybersecurity should work closely to achieve full compliance and ensure ongoing compliance with all relevant data protection regulations.

- Participation in threat intelligence sharing improves cyber resilience. The most important reasons to share threat intelligence include fostering of collaboration among peers, industry groups and the government; improving the ability to detect, contain and respond to an attack; and enhancing the timeliness of incident response.

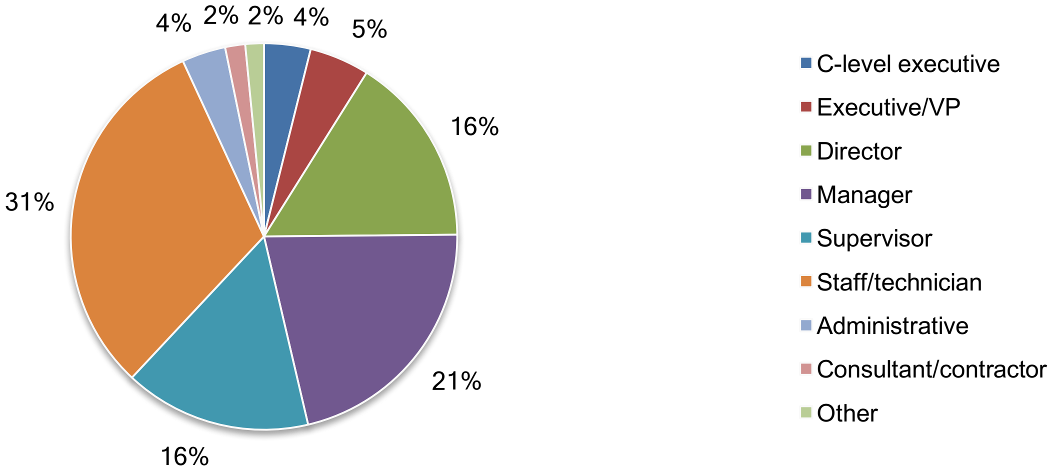
Part 3. Methods

The sampling frame is composed of 104,922 IT and IT security practitioners located in the United States, India, Germany, Japan, Brazil, the United Kingdom, France, Australia, Canada, the Middle East, and Southeast Asian countries (ASEAN). As shown in Table 2, 3,655 respondents completed the survey. Screening and failed reliability checks resulted in the removal of 559 surveys. The final sample consisted of 3,655 surveys, for an overall 3.5 percent response rate.

Table 2: Survey response	Total sampling frame	Final sample	Response rate
United States	16,990	602	3.5%
India	12,300	414	3.4%
Germany	11,007	384	3.5%
Japan	10,803	393	3.6%
Brazil	10,765	326	3.0%
United Kingdom	10,500	422	4.0%
France	9,578	298	3.1%
Australia	6,653	226	3.4%
Canada	6,010	207	3.4%
Middle East	5,436	215	4.0%
Southeast Asia	4,880	168	3.4%
Total	104,922	3,655	3.5%

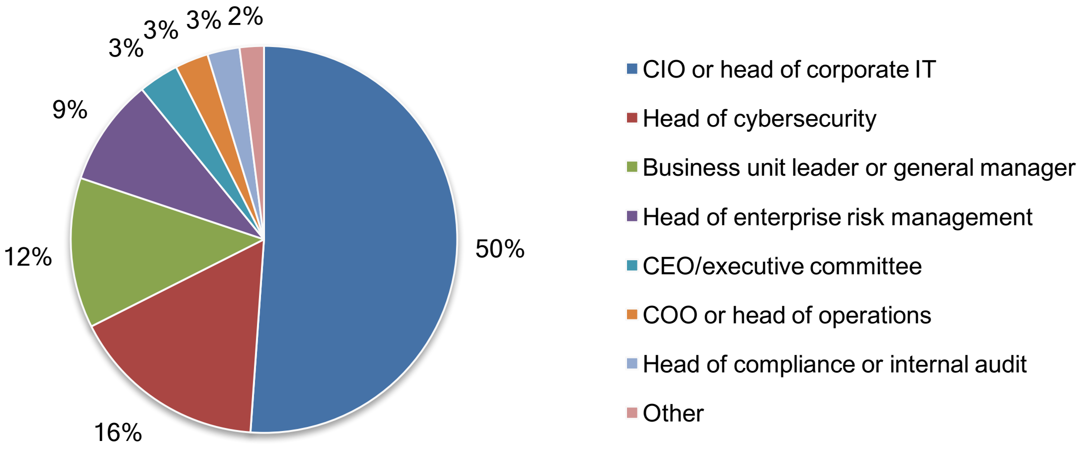
Pie Chart 1 reports respondents' organizational level within participating organizations. As shown, the majority of respondents (62 percent) are at or above the supervisory level, and 31 percent of respondents described their position as staff/technician.

Pie Chart 1. Distribution of respondents according to position level



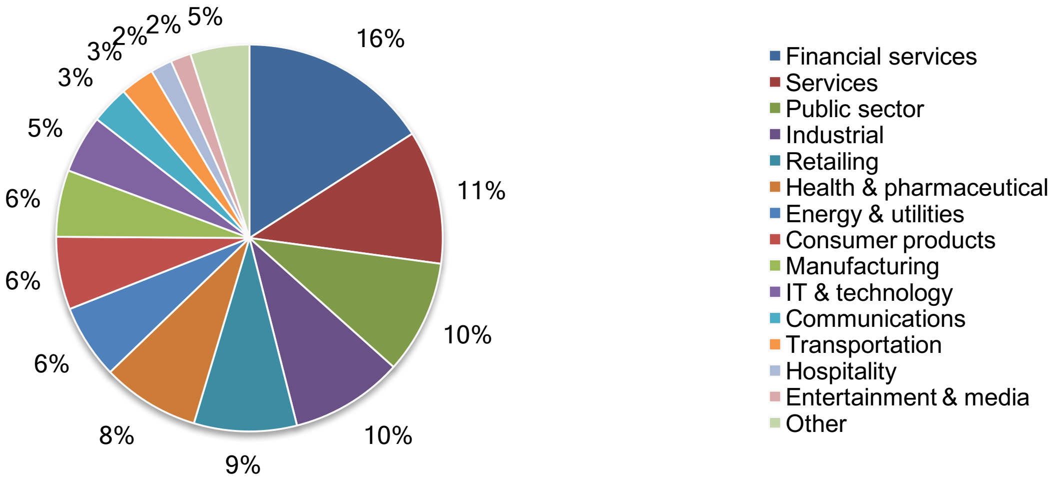
As shown in Pie Chart 2, 50 percent of respondents report to the CIO or head of corporate IT, 16 percent of respondents report to the head of cybersecurity, 12 percent of respondents report to the business unit leader or general manager and 9 percent of respondents indicated they report to the head of enterprise risk management.

Pie Chart 2. Direct reporting channel or chain of command



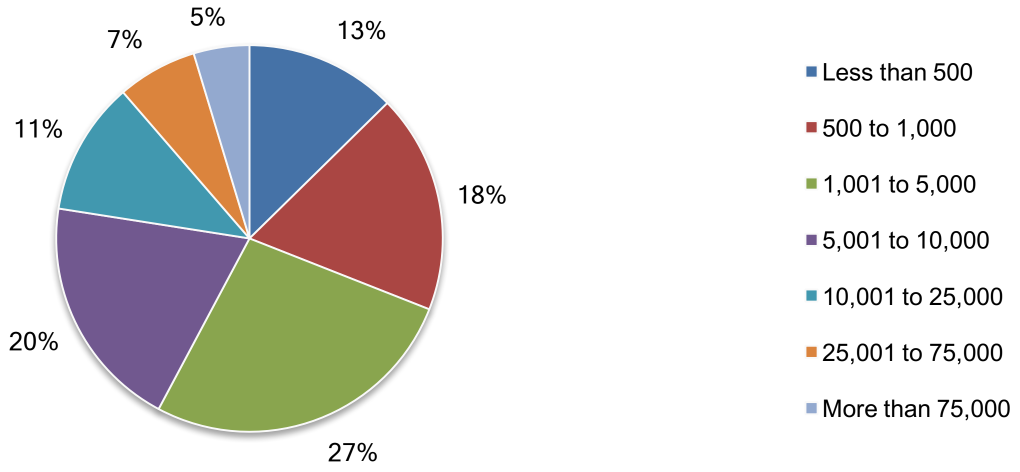
Pie Chart 3 shows the primary industry classification of respondents' organizations. This chart identifies financial services (16 percent of respondents) as the largest segment, followed by services (11 percent of respondents), the public sector (10 percent of respondents) and industrial sector (10 percent of respondents).

Pie Chart 3. Primary industry classification



Pie Chart 4 reveals that 70 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 December 2018

Survey response	FY2018	FY2017	FY2016
Total sampling frame	104,922	83,658	75,160
Total returns	4,214	3,271	2,796
Rejected or screened surveys	559	423	392
Final sample	3,655	2,848	2,404
Response rate	3.5%	3.4%	3.2%

Part 1. Screening

S1. What best describes your organizational role or area of focus?	FY2018	FY2017	FY2016
Cybersecurity operations	23%	34%	34%
IT operations	18%	43%	45%
SOC team	21%		
CSIRT team	16%	17%	16%
DevOps team	16%		
Business continuity management	6%	6%	6%
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.	FY2018	FY2017	FY2016
Managing budgets	43%	46%	43%
Evaluating vendors	45%	46%	48%
Setting priorities	37%	39%	38%
Securing systems	56%	59%	61%
Ensuring compliance	42%	45%	45%
Ensuring system availability	39%	41%	41%
None of the above (stop)	0%	0%	0%
Total	262%	275%	277%

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?	FY2018	FY2017	FY2016
Yes	55%	55%	53%
No	41%	40%	42%
Unsure	5%	5%	5%
Total	100%	100%	100%

Q1b. If yes, how frequently did these incidents occur during the past 2 years?	FY2018	FY2017	FY2016
Only once	47%	44%	43%
2 to 3 times	36%	40%	41%
4 to 5 times	11%	10%	10%
More than 5 times	6%	7%	6%
Total	100%	100%	100%

Q1c. If yes, did any of these data breaches require notification?	FY2018	FY2017
Yes	27%	22%
No	66%	71%
Unsure	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?	FY2018	FY2017
Yes	57%	56%
No	38%	40%
Unsure	4%	4%
Total	100%	100%

Q2b. If yes, how frequently did these incidents occur during the past 2 years?	FY2018	FY2017
Only once	21%	19%
2 to 3 times	26%	24%
4 to 5 times	33%	35%
More than 5 times	20%	22%
Total	100%	100%

Q3a. How has the volume of cybersecurity incidents changed in the past 12 months?	FY2018	FY2017
Significantly increased	30%	31%
Increased	31%	33%
No increase	24%	23%
Decreased	11%	11%
Significantly decreased	3%	3%
Total	100%	100%

Q3b. How has the severity of security incidents changed in the past 12 months?	FY2018	FY2017
Significantly increased	33%	31%
Increased	32%	34%
No increase	22%	21%
Decreased	9%	10%
Significantly decreased	3%	3%
Total	100%	100%

Q3c. [If you selected significant increase or increase] How is severity measured? Please check your two top choices.	FY2018
Damage to IT infrastructure	31%
Leakage of high value information assets	56%
Time to identify the incident	37%
Time to contain the incident	29%
Data center downtime	44%
Diminished productivity of employees	51%
Cost of consultants and attorneys	21%
Decline in reputation and trustworthiness	19%
Regulatory fines	12%
Other (please specify)	0%
Total	300%

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?	FY2018	FY2017	FY2016
Very frequently	19%	18%	16%
Frequently	26%	27%	28%
Somewhat frequently	27%	29%	30%
Rarely	21%	20%	20%
Never	6%	6%	6%
Total	100%	100%	100%

Q5. Using the following 10-point scale, please rate your organization’s **cyber resilience** from 1 = low resilience to 10 = high resilience.	FY2018	FY2017	FY2016
1 or 2	8%	10%	9%
3 or 4	14%	15%	17%
5 or 6	24%	27%	41%
7 or 8	28%	23%	22%
9 or 10	26%	25%	10%
Total	100%	100%	100%
Extrapolated value	6.52	6.30	5.63

Q6. Using the following 10-point scale, please rate your organization’s ability to **preven**t a cyber attack from 1 = low to 10 = high.	FY2018	FY2017	FY2016
1 or 2	9%	9%	10%
3 or 4	14%	14%	15%
5 or 6	23%	22%	35%
7 or 8	27%	28%	27%
9 or 10	26%	27%	13%
Total	100%	100%	100%
Extrapolated value	6.46	6.50	5.85

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.	FY2018	FY2017	FY2016
1 or 2	8%	8%	9%
3 or 4	14%	14%	13%
5 or 6	25%	26%	28%
7 or 8	30%	28%	28%
9 or 10	23%	24%	21%
Total	100%	100%	100%
Extrapolated value	6.46	6.46	6.28

Q8. Using the following 10-point scale, please rate your organization's ability to **contain** a cyber attack from 1 = low to 10 = high.	FY2018	FY2017	FY2016
1 or 2	5%	4%	3%
3 or 4	17%	18%	17%
5 or 6	30%	28%	27%
7 or 8	29%	32%	35%
9 or 10	20%	18%	18%
Total	100%	100%	100%
Extrapolated value	6.34	6.32	6.44

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.	FY2018	FY2017
1 or 2	5%	4%
3 or 4	14%	14%
5 or 6	27%	28%
7 or 8	30%	31%
9 or 10	23%	23%
Total	100%	100%
Extrapolated value	6.52	6.57

Q10. Using the following 10-point scale, please rate the value of cyber resilience to your organization from 1 = low to 10 = high.	FY2018	FY2017	FY2016
1 or 2	8%	7%	9%
3 or 4	12%	12%	13%
5 or 6	18%	16%	28%
7 or 8	31%	32%	29%
9 or 10	31%	33%	22%
Total	100%	100%	100%
Extrapolated value	6.82	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.	FY2018	FY2017	FY2016
1 or 2	2%	2%	2%
3 or 4	5%	5%	5%
5 or 6	13%	13%	14%
7 or 8	45%	46%	47%
9 or 10	34%	33%	32%
Total	100%	100%	100%
Extrapolated value	7.54	7.57	7.53

Q12. Please rate the difficulty in hiring and retaining skilled cybersecurity personnel from 1 = low to 10 = high.	FY2018	FY2017
1 or 2	2%	2%
3 or 4	6%	5%
5 or 6	17%	16%
7 or 8	41%	44%
9 or 10	34%	33%
Total	100%	100%
Extrapolated value	7.45	7.49

Q13. Please rate the value of automation to achieving a high level of cyber resilience from 1 = low to 10 = high.	FY2018
1 or 2	2%
3 or 4	6%
5 or 6	17%
7 or 8	43%
9 or 10	33%
Total	101%
Extrapolated value	7.53

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.	FY2018	FY2017	FY2016
Agility	2.0	2.2	2.2
Preparedness	1.9	1.8	1.8
Planned redundancies	4.3	4.5	4.3
Strong security posture	3.0	2.9	3.0
Knowledgeable or expert staff	3.8	3.7	3.7
Ample resources	5.4	5.1	5.1
Leadership	4.5	4.4	4.4

Q15a. How has your organization’s cyber resilience changed in the past 12 months?	FY2018	FY2017	FY2016
Significantly improved	20%	18%	9%
Improved	24%	25%	18%
Somewhat improved	27%	29%	25%
Declined	4%	4%	4%
No improvement	25%	25%	44%
Total	100%	100%	100%

Q15b. [If you selected significantly improved or improved] How is improvement measured? Please check your top three top choices.	FY2018
Cyber attacks prevented	55%
Time to identify the incident	51%
Time to contain the incident	48%
Data center availability (uptime)	27%
Increased productivity of employees	31%
Decreased operating cost	15%
Increased revenues	22%
Increased market share	12%
Increased share value	16%
Enhanced reputation and trustworthiness	22%
Other (please specify)	1%
Total	300%

Q15c. If your organization has improved its cyber resilience, what caused the improvement? Please check your four top choices.	FY2018	FY2017
Implementation of new technology, including cyber automation tools such as artificial intelligence and machine learning	50%	47%
Elimination of silo and turf issues	40%	39%
Visibility into applications and data assets	57%	57%
Improved information governance practices	56%	60%
C-level buy-in and support for the cybersecurity function	24%	23%
Board-level reporting on the organization’s cyber resilience	17%	15%
Training and certification for Cybersecurity staff	29%	30%
Training for end-users	28%	29%
Hiring skilled personnel	62%	61%
Engaging a managed security services provider	36%	39%
Total	400%	400%

Q16a. Does your organization report on the state of cyber resilience to C-level executives and/or the board?	FY2018
Yes, formal report	40%
Yes, informal or “ad hoc” report	21%
No	39%
Total	100%

Q16b. If yes, what metrics are used to report on the state of cyber resilience? Please select all that apply.	FY2018
Cyber attacks prevented	59%
Time to identify the incident	57%
Time to contain the incident	50%
Data center availability (uptime)	34%
Increased productivity of employees	33%
Decreased operating cost	25%
Increased revenues	24%
Increased market share	12%
Increased share value	16%
Enhanced reputation and trustworthiness	24%
Other (please specify)	2%
Total	336%

Q17. In the past 12 months, how has the time to **detect, contain and respond to** a cyber crime incident changed?	FY2018	FY2017
Time has increased significantly	26%	26%
Time has increased	30%	31%
Time has remained unchanged	31%	32%
Time has decreased	9%	9%
Time has decreased significantly	3%	3%
Total	100%	100%

18a. Please check one statement that best describes your organization's cybersecurity incident response plan (CSIRP).	FY2018	FY2017	FY2016
We have a CSIRP that is applied consistently across the entire enterprise	23%	24%	25%
We have a CSIRP, but is not applied consistently across the enterprise	27%	27%	26%
Our CSIRP is informal or "ad hoc"	25%	26%	26%
We don't have a CSIRP	24%	24%	23%
Total	100%	100%	100%

Q18b. If you have a CSIRP, how often is it reviewed and tested?	FY2018	FY2017	FY2016
Each quarter	6%	7%	7%
Twice per year	6%	7%	7%
Once each year	34%	34%	34%
No set time period for reviewing and updating the plan	42%	39%	37%
We have not reviewed or updated since the plan was put in place	12%	14%	15%
Total	100%	100%	100%

Q19a. Does your organization participate in an initiative or program for sharing information with government and/or industry peers about cyber threats and vulnerabilities?	FY2018	FY2017	FY2016
Yes	56%	57%	53%
No	44%	43%	47%
Total	100%	100%	100%

Q19b. If your organization shares information about cyber threats and vulnerabilities, what are the main reasons? Please select all that apply.	FY2018	FY2017	FY2016
Improves the cyber resilience of my organization	58%		
Improves the ability to detect, contain and respond	58%		
Improves the effectiveness of our incident response plan	52%	72%	75%
Enhances the timeliness of incident response	55%	57%	53%
Reduces the cost of detecting and preventing data breaches	46%	58%	52%
Fosters collaboration among peers, industry groups and government	58%	32%	33%
Total	326%	219%	213%

Q19c. If no, why does your organization not participate in a threat-sharing program? Please select four top choices.	FY2018	FY2017	FY2016
Cost	53%	33%	33%
Potential liability of sharing	43%	11%	10%
Risk of the exposure of sensitive and confidential information	52%	24%	22%
Anti-competitive concerns	43%	19%	21%
Lack of resources	60%	43%	42%
Lack of incentives	39%	16%	16%
No perceived benefit to my organization	73%	40%	42%
Do not know about options to share intelligence	34%	9%	11%
Other (please specify)	3%	4%	4%
Total	400%	200%	200%

Q20. Which of the following security technologies have been the most effective in helping your organization achieve cyber resilience. Please select your top eight (8) choices.	FY2018	FY2017	FY2016
Analytics for cybersecurity	33%	29%	29%
Anti-DDoS solutions	44%		
Anti-malware solution (AVAM)	53%	59%	53%
Artificial intelligence (AI)	20%		
Cryptographic technologies	55%		
Data loss prevention (DLP)	35%	39%	37%
DevOps & secure SDLC	47%		
Endpoint security solution	22%	23%	23%
Governance & risk management solutions (GRC)	19%	16%	16%
Identity management & authentication	69%	70%	71%
Incident response platform	56%	53%	58%
Intelligence and threat sharing	53%		
Intrusion detection & prevention (IDS/IPS)	44%	55%	58%
Machine learning	23%		
Network traffic surveillance	50%	52%	52%
Next generation firewalls	15%	15%	15%
Security information & event management (SIEM)	56%	41%	41%
Smart bots	21%		
User Behavioral Analytics (UBA)	25%	23%	22%
Virtual private networks (VPN)	26%	24%	25%
Web application firewalls (WAF)	15%	13%	12%
Wireless security solutions	14%	14%	14%
Other (please specify)	5%	5%	4%
Total	800%	700%	700%

Q21. Approximately, how many separate security solutions and technologies does your organization deploy today?	FY2018
Less than 10	5%
10 to 20	11%
21 to 30	24%
31 to 50	32%
51 to 100	22%
100+	6%
Total	100%
Extrapolated value	44.6

Q22a. What best describes your organization's use of automation? Please include both artificial intelligence and machine learning as part of automation.	FY2018
Yes, significant use	23%
Yes, moderate use	48%
Yes, insignificant	11%
No use	18%
Total	100%

Q22b. If your organization's use of automation is significant or moderate, why? Please select all that apply.	FY2018
To improve operational efficiency	64%
To reduce costs	49%
To support our IT security team	64%
To maintain competitive advantage	35%
To reduce security risks	50%
Other (please specify)	2%
Total	264%

Q23. What one statement best describes your opinion regarding the number of separate security technologies deployed by your organization?	FY2018
We have too many security solutions and technologies to achieve cyber resilience	35%
We do not have enough security solutions and technologies to achieve cyber resilience	35%
We have the right number of security solutions and technologies to achieve cyber resilience	30%
Total	100%

Part 3. Attribution: Please express your opinion about each one of the following statements using the scale below each item.			
Strongly Agree and Agree response: Please express your opinion about each one of the following statements using the agreement scale.	FY2018	FY'2017	FY2016
Q24a. My organization's leaders recognize that enterprise risks affect cyber resilience.	56%	57%	48%
Q24b. My organization's leaders recognize that cyber resilience affects revenues.	61%	59%	47%
Q24c. My organization's leaders recognize that cyber resilience affects brand and reputation.	49%	48%	45%
Q24d. In my organization, funding for Cybersecurity is sufficient to achieve a high level of cyber resilience.	33%	31%	33%
Q24e. In my organization, staffing for Cybersecurity is sufficient to achieve a high level of cyber resilience.	30%	29%	33%
Q24f. My organization's leaders recognize that automation, machine learning, artificial intelligence and orchestration strengthens our cyber resilience.	60%	63%	
Q24g. My organization deploys too many separate security solutions and technologies, which increases operational complexity and reduces visibility.	48%		
Q24h. In my organization, a strong privacy posture is important to achieving cyber resilience.	60%		
Q24i. In my organization, complying with data protection regulations such as the EU's GDPR and California's new privacy law is important to achieving cyber resilience.	54%		

Q25. Who has overall responsibility for directing your organization's efforts to ensure cyber resilience? Please check one choice only.	FY2018	FY2017	FY2016
Business continuity manager	9%	8%	8%
Business unit leader	23%	22%	22%
Chief executive officer (CEO)	7%	7%	7%
Chief information officer (CIO)	22%	23%	23%
Chief technology officer (CTO)	6%	6%	6%
Chief risk officer (CRO)	2%	7%	8%
Chief information security officer (CISO)	15%	14%	13%
Chief privacy officer (CPO)	1%		
No one person has overall responsibility	14%	11%	13%
Other (please specify)	1%	2%	0%
Total	100%	100%	100%

Q26. How important is the privacy role to achieving cyber resilience within your organization?	FY2018
Essential	35%
Very important	30%
Important	19%
Somewhat important	11%
Not important	5%
Total	100%

Q27a. How important is **aligning** the privacy and cybersecurity roles to achieving cyber resilience within your organization?	FY2018
Essential	31%
Very important	31%
Important	22%
Somewhat important	10%
Not important	5%
Total	100%

Q27b. if alignment is essential or very important, why?	FY2018
More effective approach to compliance with data protection regulations (such as GDPR)	49%
Less redundancy and more efficiency in both privacy and cybersecurity operations	60%
Increase in perceived trustworthiness	48%
Reduction in silos and turf issues	63%
Other (please specify)	2%
Total	222%

Q28a. Has your organization achieved full compliance with the EU's General Data Protection Regulation (GDPR)?	FY2018
Yes	54%
No	41%
Unsure	5%
Total	100%

Q28b. If yes, how important is the alignment between the privacy and cybersecurity roles to achieving compliance with GDPR?	FY2018
Essential	31%
Very important	32%
Important	23%
Somewhat important	10%
Not important	4%
Total	100%

Q29a. What is the full-time equivalent (FTE) headcount of your IT **cybersecurity** function today?	FY2018	FY2017
Less than 5	6%	7%
5 to 10	8%	10%
11 to 20	12%	11%
21 to 30	15%	13%
31 to 40	21%	21%
41 to 50	17%	16%
51 to 100	14%	15%
More than 100	7%	5%
Total	100%	100%
Extrapolated value	39.73	38.8

Q29b. What should the full-time equivalent (FTE) **cybersecurity** headcount be to achieve cyber resilience?	FY2018	FY2017
Less than 5	1%	1%
5 to 10	1%	2%
11 to 20	7%	7%
21 to 30	12%	11%
31 to 40	18%	16%
41 to 50	25%	26%
51 to 100	20%	22%
More than 100	15%	14%
Total	100%	100%
Extrapolated value	55.46	55.0

Q30. How long has your organization's current CISO or **cybersecurity** leader held their position?	FY2018	FY2017
Currently, we don't have a CISO or security leader	22%	23%
Less than 1 year	21%	22%
1 to 3 years	27%	28%
4 to 6 years	17%	16%
7 to 10 years	10%	9%
More than 10 years	3%	2%
Total	100%	100%

Q31a. What is the full-time equivalent (FTE) headcount of your **privacy** function today?	FY2018
Less than 1	31%
1 to 3	31%
4 to 5	21%
6 to 10	15%
More than 10	1%
Total	100%
Extrapolated value	3.21

Q31b. What should the full-time equivalent (FTE) **privacy** headcount be to achieve cyber resilience?	FY2018
Less than 1	24%
1 to 3	29%
4 to 5	24%
6 to 10	19%
More than 10	5%
Total	100%
Extrapolated value	3.95

Q32. How long has your organization's current CPO or privacy leader held their position?	FY2018
Currently, we don't have a CPO or **privacy** leader	27%
Less than 1 year	11%
1 to 3 years	19%
4 to 6 years	20%
7 to 10 years	14%
More than 10 years	9%
Total	100%

Part 5. Budget for cyber resilience activities

Q35. What factors justify the funding of your organization's cybersecurity function? Please select your top two choices.	FY2018	FY2017	FY2016
System or application downtime	44%	61%	62%
Information loss or theft	56%	47%	48%
Performance degradation	6%	10%	9%
Productivity loss	14%	9%	9%
Revenue decline	8%	8%	7%
Reputation damage	19%	18%	20%
Customer defection	8%	8%	8%
Compliance/regulatory failure	44%	36%	36%
Other (please specify)	0%	1%	1%
Total	200%	200%	200%

Q36. Approximately, what is the dollar range that best describes your organization's **cybersecurity budget for 2019**?	FY2018	FY2017	FY2016
< $1 million	5%	6%	5%
$1 to 5 million	15%	18%	16%
$6 to $10 million	30%	28%	29%
$11 to $15 million	26%	23%	25%
$16 to $20 million	15%	15%	15%
$21 to $25 million	6%	7%	6%
$26 to $50 million	2%	1%	2%
> $50 million	1%	1%	1%
Total	100%	100%	100%
Extrapolated value ($millions)	$ 11.6	11.3	11.4

Q37. Approximately, what percentage of the **2019 cybersecurity budget** will go to cyber resilience-related activities?	FY2018	FY2017	FY2016
< 2%	0%	0%	0%
2% to 5%	2%	2%	2%
6% to 10%	7%	8%	7%
11% to 20%	11%	12%	13%
21% to 30%	32%	34%	35%
31% to 40%	25%	22%	22%
41% to 50%	11%	10%	10%
51% to 60%	7%	8%	6%
61% to 70%	4%	4%	5%
71% to 80%	1%	1%	0%
81% to 90%	0%	0%	0%
91 to 100%	0%	0%	0%
Total	100%	100%	100%
Extrapolated value (percentage)	31%	30%	30%

Organizational and respondent characteristics

D1. What best describes your position level within the organization?	FY2018	FY2017	FY2016
C-level executive	4%	4%	4%
Executive/VP	5%	4%	3%
Director	16%	16%	16%
Manager	21%	19%	20%
Supervisor	16%	14%	14%
Staff/technician	31%	33%	34%
Administrative	4%	6%	5%
Consultant/contractor	2%	2%	2%
Other (please specify)	2%	2%	1%
Total	100%	100%	100%

D2. What best describes your reporting channel or chain of command?	FY2018	FY2017	FY2016
CEO/executive committee	3%	2%	3%
COO or head of operations	3%	3%	3%
CFO, controller or head of finance	1%	5%	4%
CIO or head of corporate IT	50%	54%	54%
CPO or head of privacy or data protection	1%		
Business unit leader or general manager	12%	12%	12%
Head of compliance or internal audit	3%	4%	3%
Head of enterprise risk management	9%	6%	7%
Head of Cybersecurity	16%	15%	14%
Other (please specify)	0%	1%	2%
Total	100%	100%	100%

D3. What best describes your organization's primary industry classification?	FY2018	FY2017	FY2016
Agriculture & food services	1%	2%	2%
Communications	3%	4%	4%
Consumer products	6%	4%	5%
Defense & aerospace	1%	1%	1%
Education & research	1%	3%	2%
Energy & utilities	6%	6%	6%
Entertainment & media	2%	2%	1%
Financial services	16%	17%	17%
Health & pharmaceutical	8%	8%	8%
Hospitality	2%		
Industrial	10%	3%	3%
IT & technology	5%	9%	10%
Logistics & distribution	1%	5%	4%
Manufacturing	6%	2%	1%
Public sector	10%	6%	7%
Retailing	9%	9%	10%
Services	11%	6%	7%
Transportation	3%	10%	9%
Other	1%	3%	3%
Total	100%	100%	100%

D4. What range best describes the full-time headcount of your global organization?	FY2018	FY2017	FY2016
Less than 500	13%	15%	14%
500 to 1,000	18%	21%	21%
1,001 to 5,000	27%	26%	24%
5,001 to 10,000	20%	17%	17%
10,001 to 25,000	11%	11%	12%
25,001 to 75,000	7%	6%	7%
More than 75,000	5%	4%	4%
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.