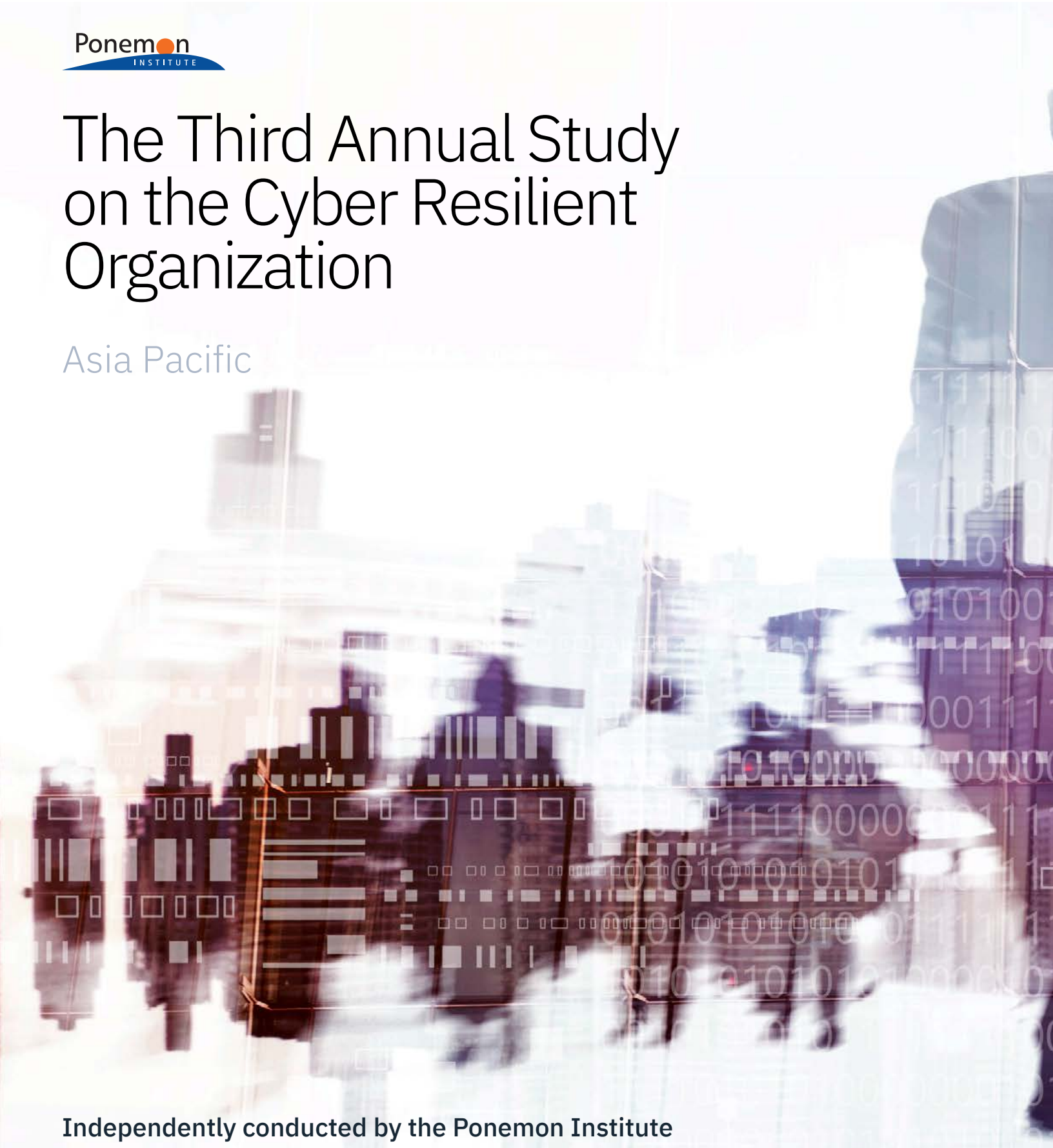
Ponemon INSTITUTE

The Third Annual Study on the Cyber Resilient Organization

Asia Pacific



Independently conducted by the Ponemon Institute

Sponsored by IBM Resilient
Publication Date: May 2018

IBM Security

The Third Annual Study on the Cyber Resilient Organization: Asia-Pacific

Ponemon Institute, May 2018

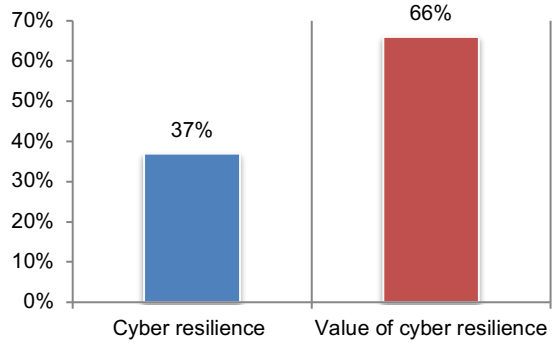
Part 1. Introduction

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.* More than 2,848 IT and IT security professionals from around the world[1] were surveyed. In this report we present the findings for Asia Pacific (639 respondents). This is the first time that this research has been carried out in the Asia-Pacific region, though Australia has previously been covered as a separate report.

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.

Respondents were asked to rate the value and level of their organizations' cyber resilience on a scale from 1= low to 10 = high. As shown in Figure 1, only 37 percent of respondents rate their level of cyber resilience as high but 66 percent of respondents say it is very valuable.

Figure 1. The value and level of cyber resilience
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 78 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 34 percent of respondents feel that they have an adequate cyber resilience budget in place.

Senior management recognizes the importance of advanced technologies to their organizations' cyber resilience. 66 percent of respondents say their senior managers recognize that automation, machine learning, artificial intelligence and orchestration strengthens their organizations' cyber resilience. They also recognize that enterprise risks affect cyber resilience (61 percent of respondents) and cyber resilience can affect revenues (56 percent of respondents). Almost half (48 percent of respondents) say it affects brand and reputation.

Companies are effective in preventing and responding to an attack. Respondents were asked to rate their organizations ability to prevent, detect and contain a cyber attack from 1 = low ability to 10 = high ability. Respondents are most confident in their ability to prevent and respond

[1] Other countries represented in this study are Brazil, France, Germany, the Middle East, the United Kingdom and the United States.

to a cyber attack as high. Less than half of respondents (48 percent) rate their ability to quickly detect a cyber attack. Seventy-one of respondents say their organizations' cyber resilience has improved significantly (16 percent), improved (29 percent) or somewhat improved (26 percent).

Hiring skilled personnel improves cyber resiliency. The 71 percent of respondents who say they have seen improvements in their cyber resilience cite the following reasons for improvement: hiring skilled personnel (61 percent of respondents), improving information governance practices (60 percent of respondents) and increasing visibility into applications and data assets (58 percent of respondents).

Preparedness and agility are the most important factors to achieving a high level of cyber resilience. Respondents rated preparedness and agility are the most important factors to achieving a high level of cyber resilience.

IT and IT security are responsible for ensuring a high level of cyber resilience. If you combine the chief information officer (31 percent of respondents), chief information security officer (12 percent of respondents) and chief technology officer (4 percent), 47 percent of respondents say the overall responsibility for cyber resilience resides in the IT and IT security function.

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.

Hiring and retaining skilled IT security personnel is a serious hurdle to improving cyber resilience. 76 percent of respondents rate the importance of having skilled cybersecurity professionals in your cybersecurity response plan (CSIRP) as high or very high. However, 73 percent of respondents rate the difficulty in hiring and retaining skilled IT security personnel as very high.

Staffing is inadequate. Only 31 percent of respondents agree that in their organization, staffing for IT security is sufficient to achieve a high level of cyber resilience. The ideal average FTE should be 51.5 full-time security professionals.

Incident response plans often do not exist or are "ad hoc". Only 22 percent of respondents say they have a CSIRP that is applied consistently across the enterprise. If they do have a CSIRP 38 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.

CSIRP prevention activities receive the most investment. As discussed previously, companies rate their ability to prevent cyber attacks as high. Prevention activities receive the greatest amount of funding (an average of 47 percent).

Funding is inadequate for cybersecurity and cyber resilience. Only 34 percent of respondents say funding for IT security is sufficient to achieve a high level of cyber resilience. The average budget for cyber resilience is $2.2 million.

The severity and volume of cybersecurity incidents increases the time to resolve a security incident. 65 percent of respondents say the volume has increased (30 percent + 35 percent) and 66 percent (29 percent + 37 percent) say the severity has increased.

The increase in volume and severity of cyber attacks has had a negative effect on the time to resolve a cyber incident has increased significantly. 57 percent of respondents say the time has increased significantly (25 percent) or increased (32 percent).

More than half of companies represented in this study have deployed many of their core cybersecurity program activities. 55 percent of respondents say the maturity of their cybersecurity program is late-middle or mature stage.

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. According to respondents, the seven most effective technologies for achieving cyber resilience are: identity management and authentication, anti-virus/anti-malware, intrusion detection and prevention systems, encryption for data at rest, incident response platforms, network traffic surveillance and data loss prevention. A total of 21 technologies were listed in the survey question.

Having an incident response platform and sharing threat intelligence are considered key initiatives to improving cyber resilience. Almost half of respondents (49 percent) say their organizations participate in an initiative or program for sharing information with government and industry peers about data breaches and incident response.

73 percent of respondents say sharing intelligence improves the security posture of their organization, and 69 percent of respondents say it improves the effectiveness of their incident response plan. 64 percent of respondents say threat intelligence sharing reduces the cost of detecting and preventing data breaches.

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 (45 percent), it costs too much (35 percent) or no perceived benefit (32 percent).

The level of cyber resilience in Asia-Pacific is lower than the global average. At 37 percent, respondents in Asia-Pacific are some way behind the global average of 48 percent. Interestingly, more Asia-Pacific respondents believed their cybersecurity program to be more mature or late-middle (55 percent) than the global average (53 percent). Generally, Asia-Pacific findings were similar to the global ones.

Part 2. Key findings

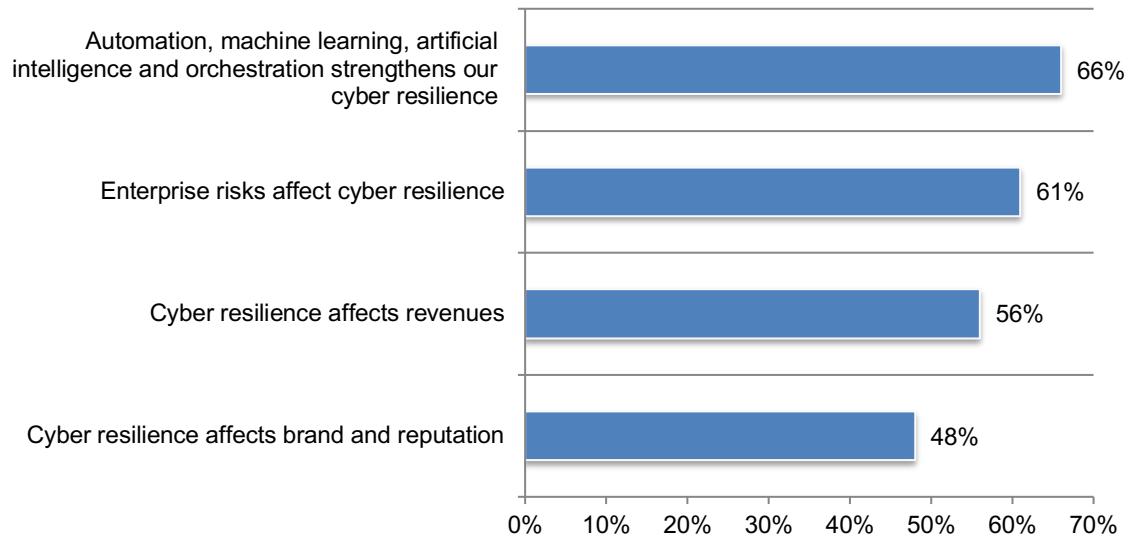
In this section of the report, we provide an analysis of the key findings. The complete audited findings are presented in the Appendix of this report. We have organized the findings according to the following topics.

- 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

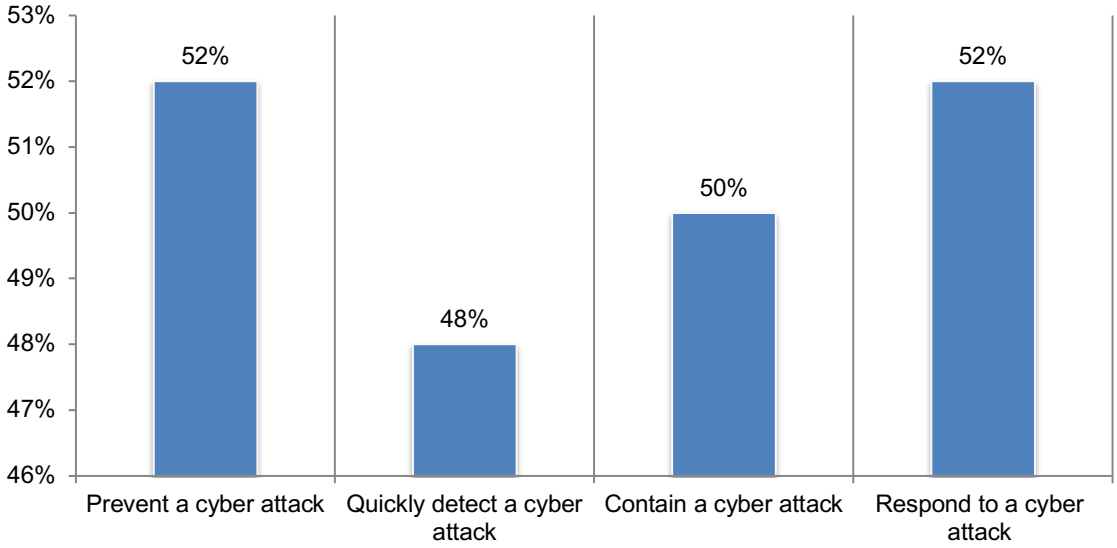
Senior management recognizes the importance of advanced technologies to their organizations' cyber resilience. According to Figure 2, 66 percent of respondents say their senior managers recognize that automation, machine learning, artificial intelligence and orchestration strengthens their organizations' cyber resilience. They also recognize that enterprise risks affect cyber resilience (61 percent of respondents) and cyber resilience can affect revenues (56 percent of respondents). Almost half (48 percent of respondents) say it affects brand and reputation.

Figure 2. Senior management's awareness about the impact of cyber resilience on the enterprise
Strongly agree and Agree responses combined



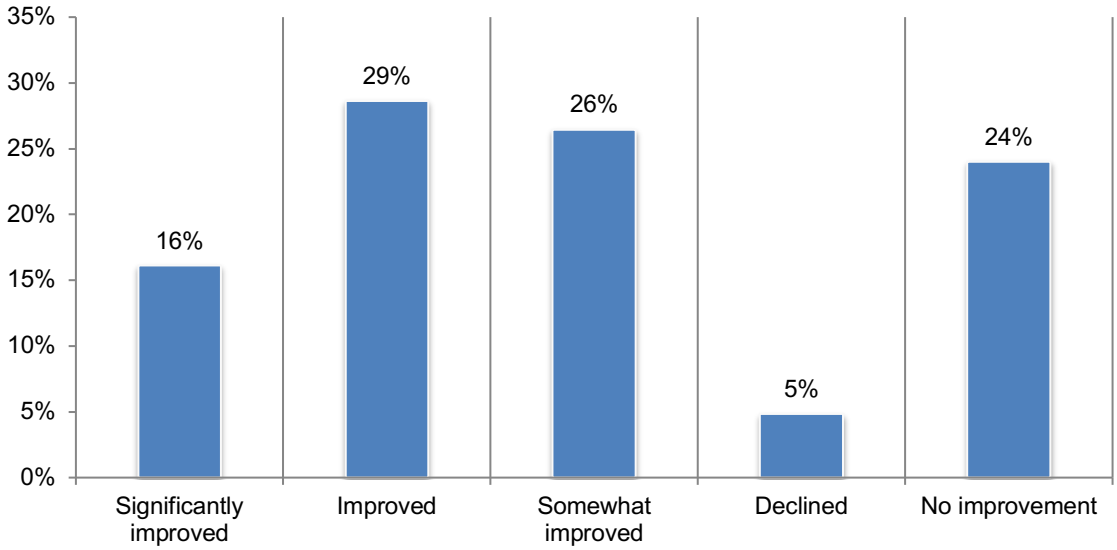
Companies are effective in preventing and responding to an attack. Respondents were asked to rate their organizations ability to prevent, detect and contain a cyber attack from 1 = low ability to 10 = high ability. As shown in Figure 3, respondents are most confident in their ability to prevent and respond to a cyber attack. Less than half of respondents (48 percent) rate their ability to quickly detect a cyber attack

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



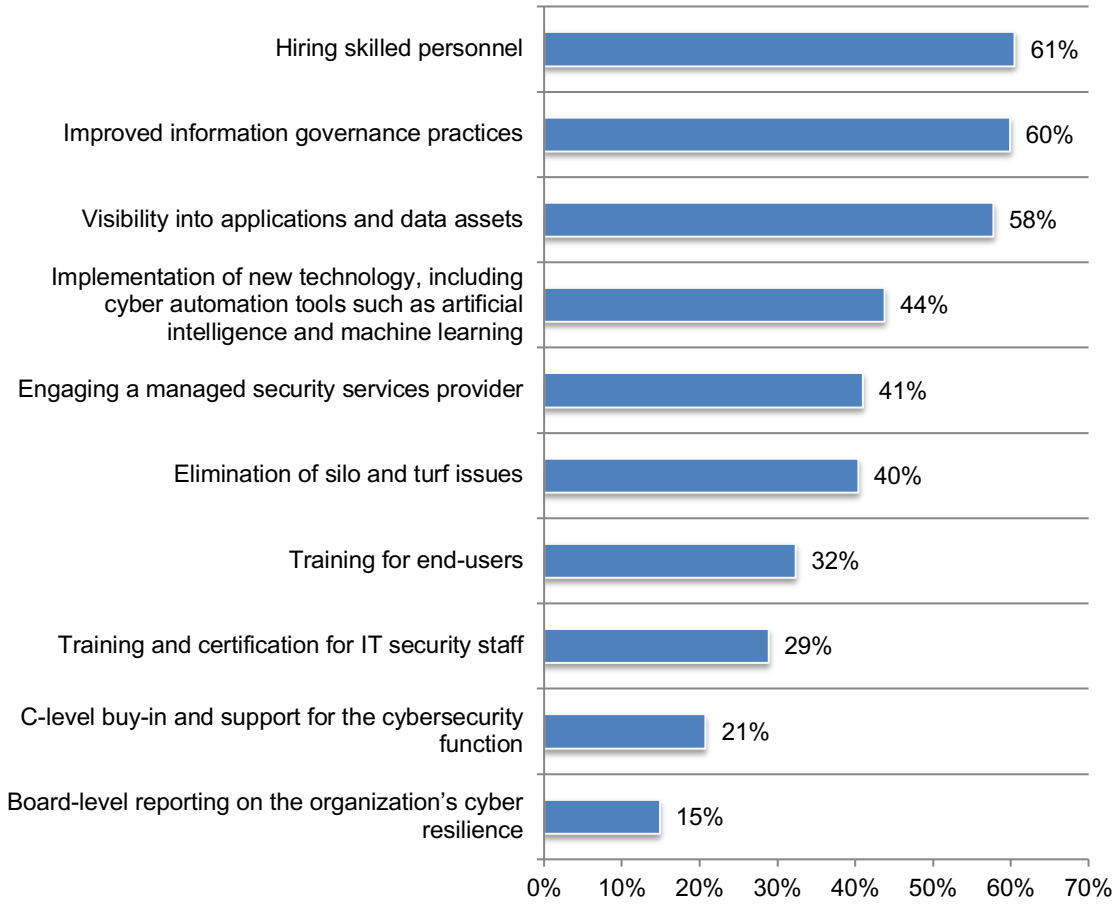
As shown in Figure 4, 71 percent of respondents say their organizations' cyber resilience has improved significantly (16 percent), improved (29 percent) or somewhat improved (26 percent).

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



Hiring skilled personnel improves cyber resiliency. The 71 percent of respondents who say they have seen improvements in their cyber resilience cite the following reasons for improvement: hiring skilled personnel (61 percent of respondents), improving information governance practices (60 percent of respondents) and increasing visibility into applications and data assets (58 percent of respondents), as shown in Figure 5.

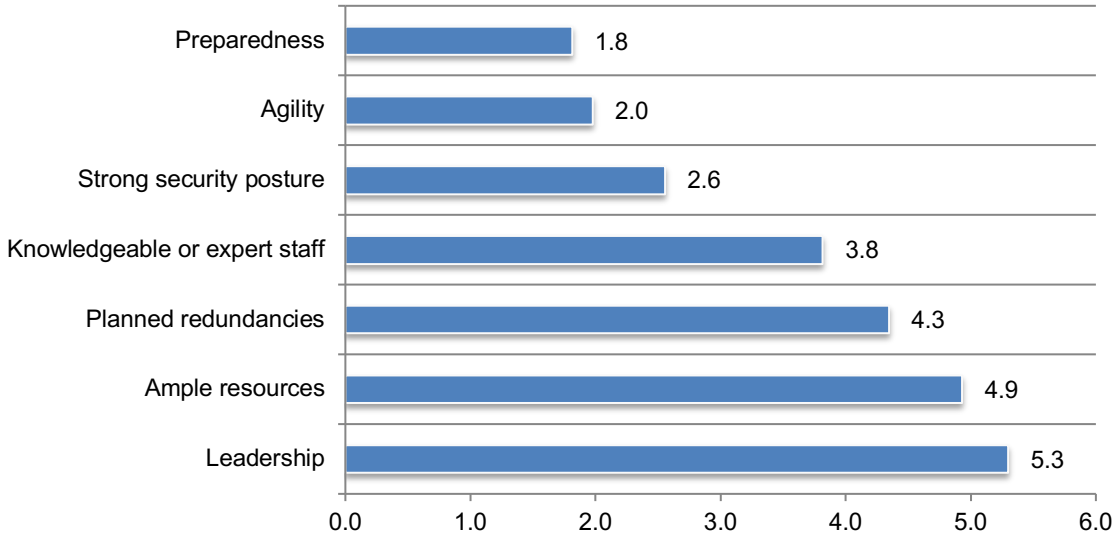
Figure 5. Why did your organization's cyber resilience improve?
Four choices allowed



Preparedness and agility are the most important factors to achieving a high level of cyber resilience. Respondents rated preparedness and agility are the most important factors for achieving cyber resilience, according to Figure 6.

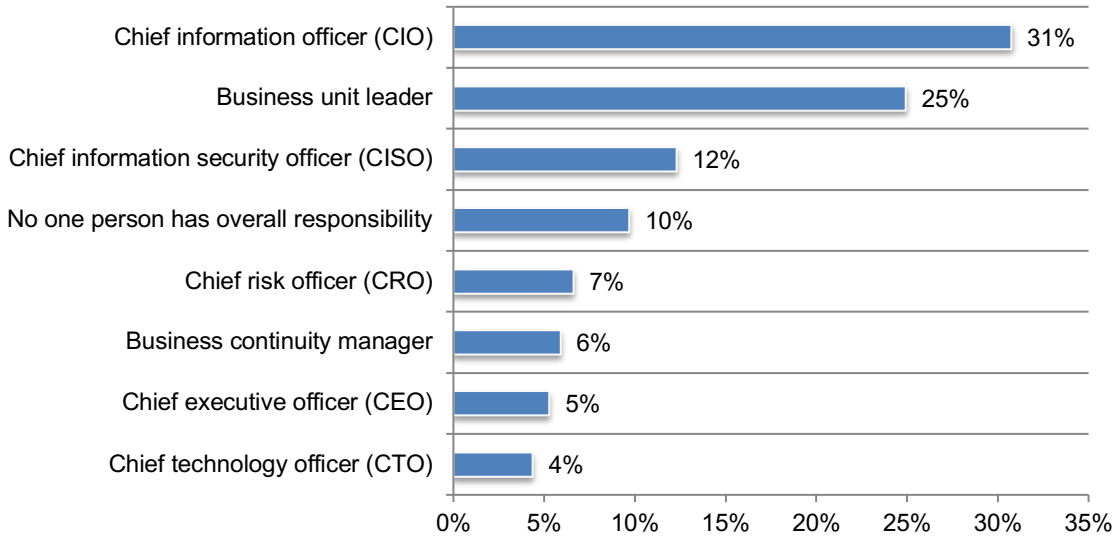
Figure 6. The seven factors considered important in achieving a high level of cyber resilience

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 (31 percent of respondents), chief information security officer (12 percent of respondents) and chief technology officer (4 percent), 47 percent of respondents say the overall responsibility for cyber resilience resides in the IT and IT security function.

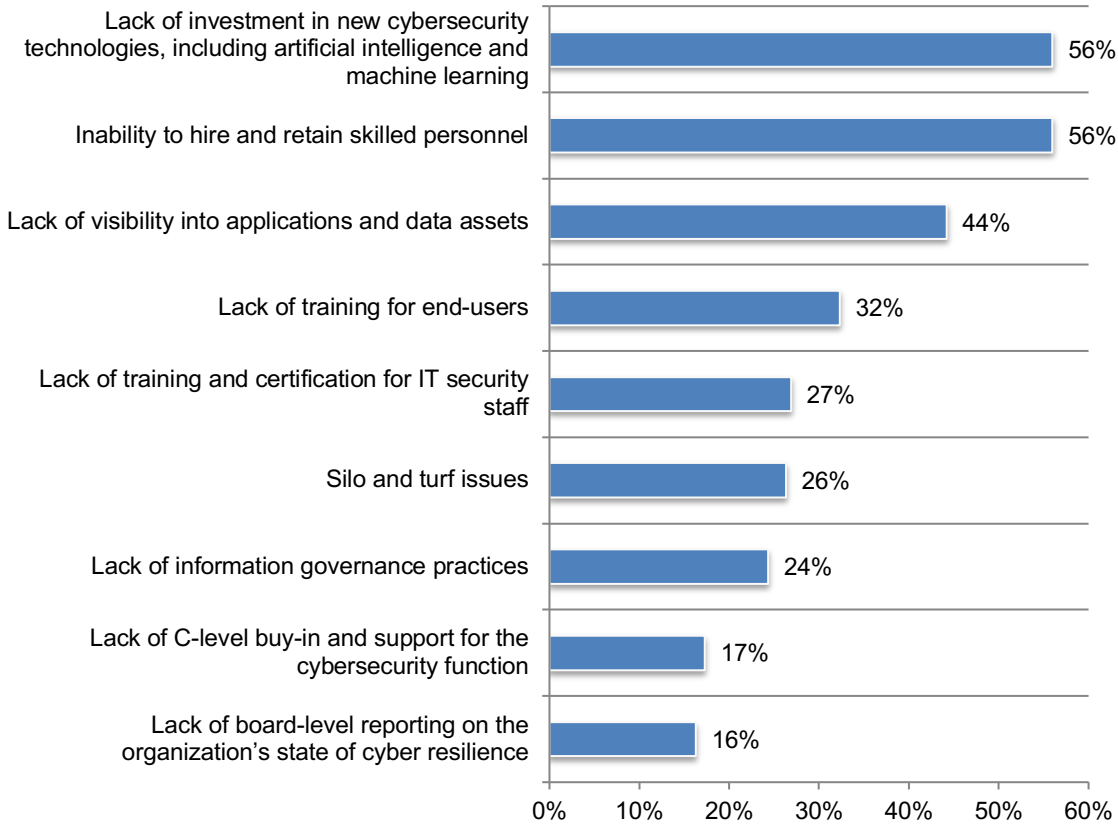
Figure 7. Who has overall responsibility for directing your organization's efforts to ensure a high level of cyber resilience?



Hurdles to further improvements in cyber resilience

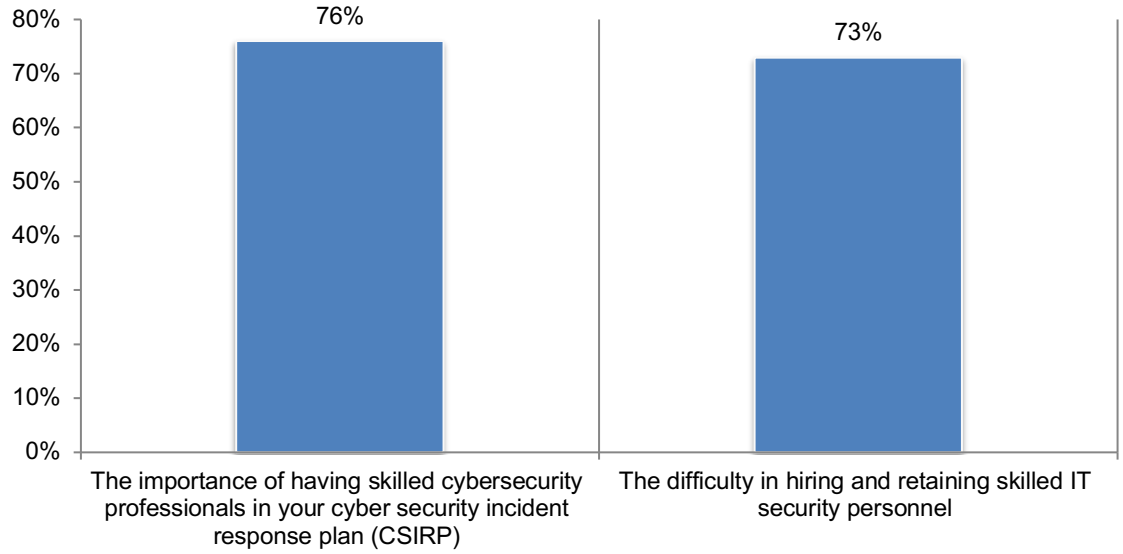
Cybersecurity technologies and skilled personnel are critical to a high level of cyber resilience. Lack of investment in new cybersecurity technologies, including artificial intelligence and machine learning, and the inability to hire and retain skilled personnel are the biggest barriers to cyber resilience,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

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



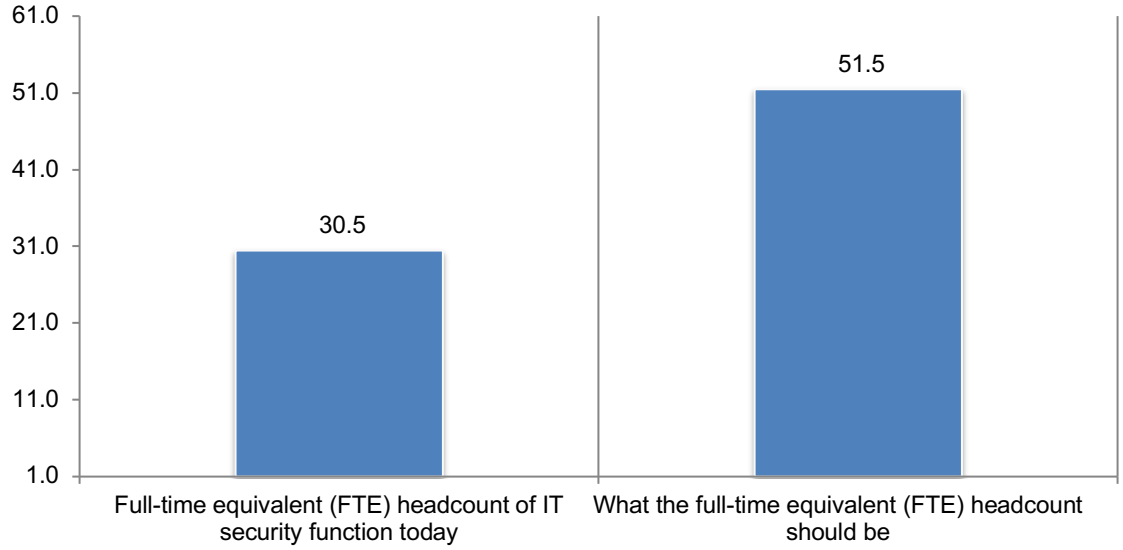
Hiring and retaining skilled IT security personnel is a serious hurdle to improving cyber resilience. 76 percent of respondents rate the importance of having skilled cybersecurity professionals in your cybersecurity response plan (CSIRP) as high or very high. However, 73 percent of respondents rate the 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



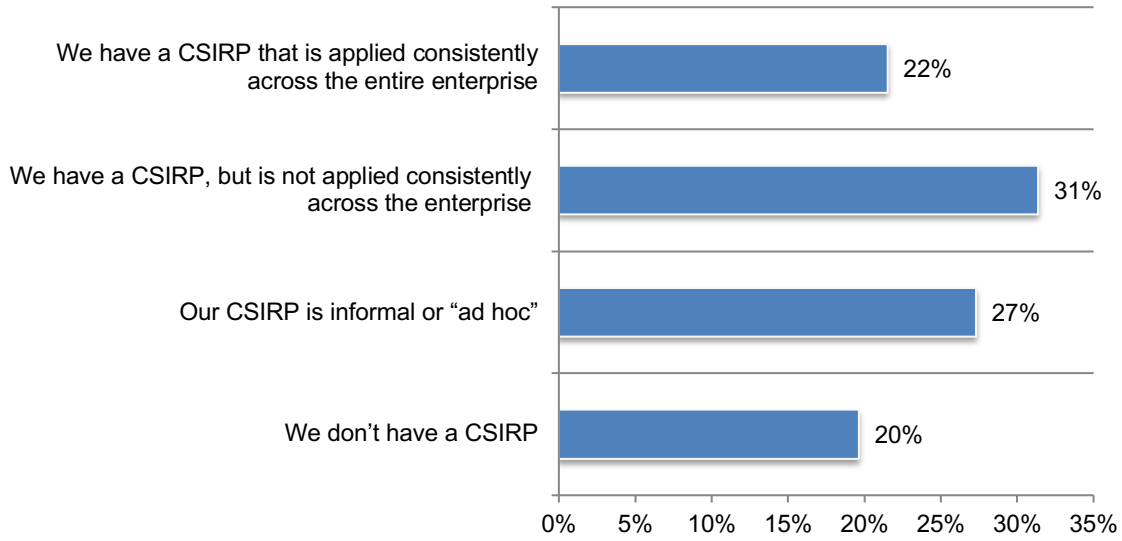
Staffing is inadequate. In fact, only 31 percent of respondents agree that in their organization, staffing for IT security is sufficient to achieve a high level of cyber resilience. As shown in Figure 10, the ideal average should be 51.5 full-time security professionals.

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



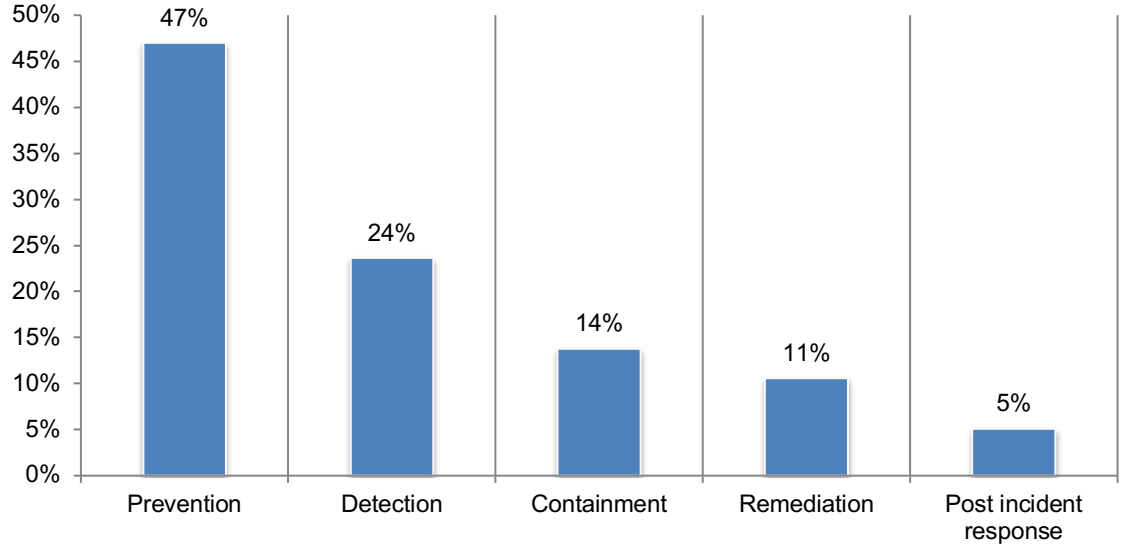
Incident response plans often do not exist or are "ad hoc." According to Figure 11, only 22 percent of respondents say they have a CSIRP that is applied consistently across the enterprise. If they do have a CSIRP 38 percent of respondents say there is no set time period for reviewing and updating the 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?



CSIRP prevention activities receive the most investment. As discussed previously, companies rate their ability to prevent cyber attacks as high. Prevention activities, as shown in Figure 12, receive the greatest amount of funding (47 percent).

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

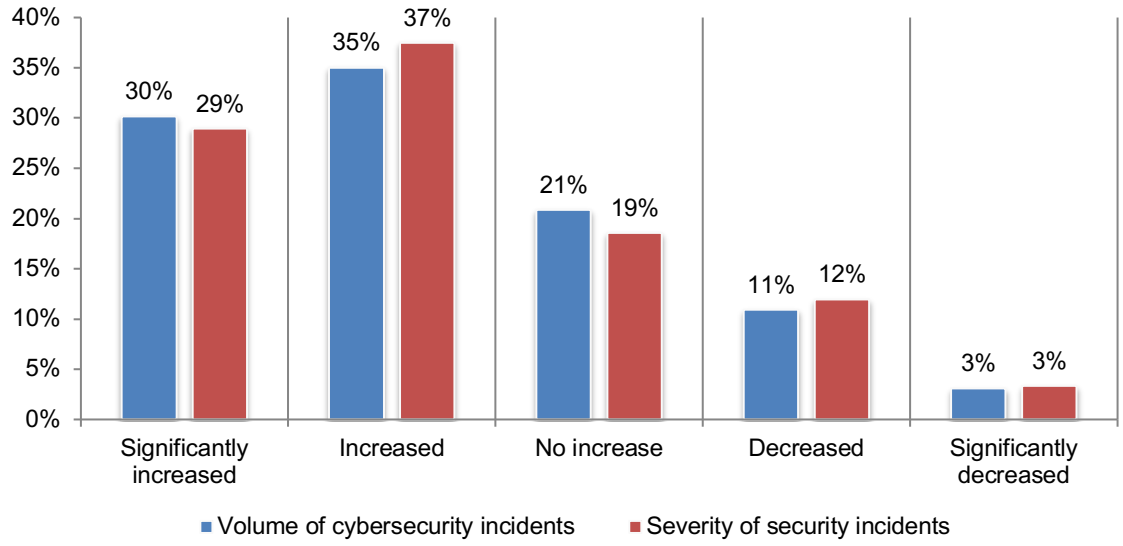


Funding is insufficient for cybersecurity and cyber resilience. Only 34 percent of respondents say funding for IT security is sufficient to achieve a high level of cyber resilience. As shown in Table 1, the average budget for cyber resilience is $2.2 million.

Table 1. Budget for cybersecurity & cyber resilience activities	
Extrapolated average (millions)	2017
Cybersecurity budget	$8.6
Percentage allocated to cyber resilience activities	26%
Total average budget allocated to cyber resilience	$2.2

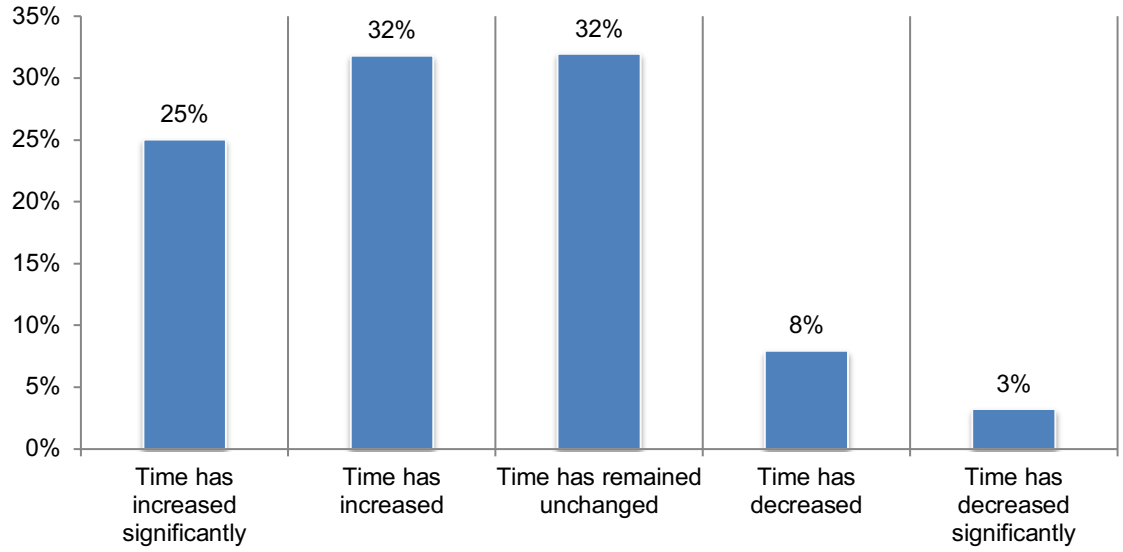
The severity and volume of cybersecurity incidents increases the time to resolve a security incident. As shown in Figure 13, 65 percent of respondents say the volume has increased (30 percent + 35 percent) and 66 percent (29 percent + 37 percent) say the severity has increased.

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, 57 percent of respondents say the time has increased significantly (25 percent) or increased (32 percent).

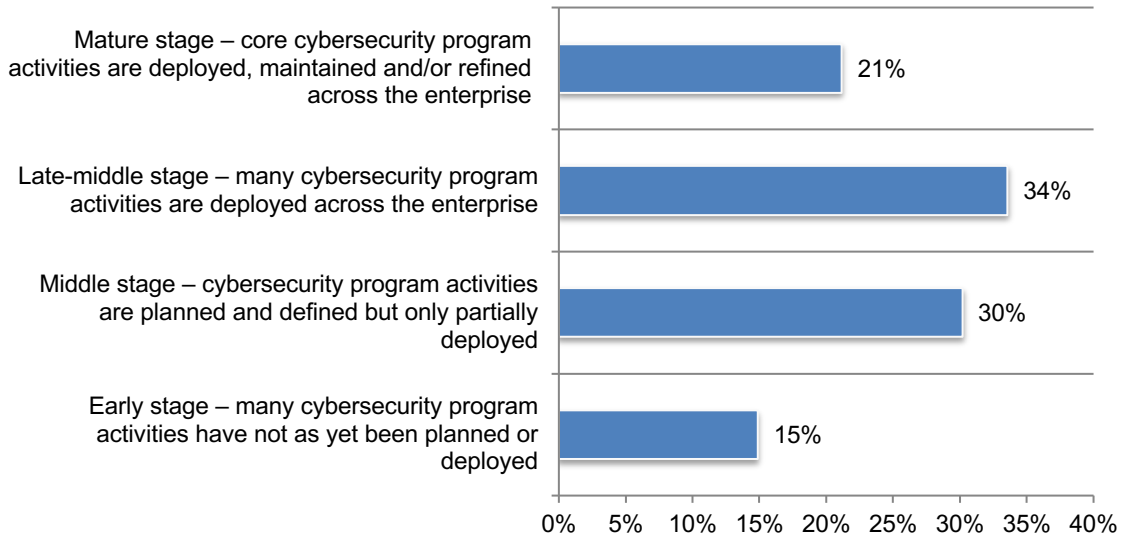
Figure 14. In the past 12 months, how has the time to detect, contain and respond to a cyber crime changed?



Technologies & governance practices to support cyber resilience

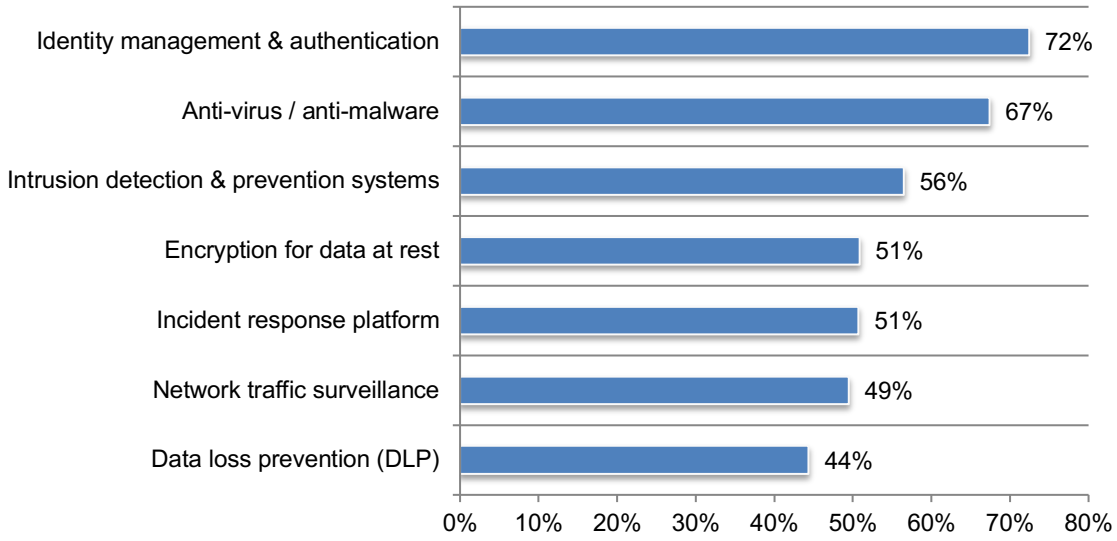
More than half of companies represented in this study have deployed many of their core cybersecurity program activities. As shown in Figure 15, 55 percent of respondents say the maturity of their cybersecurity program is late-middle or mature stage (21 percent + 34 percent).

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, encryption for data at rest, incident response platforms, network traffic surveillance and data loss prevention. A total of 21 technologies were listed in the survey question.

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



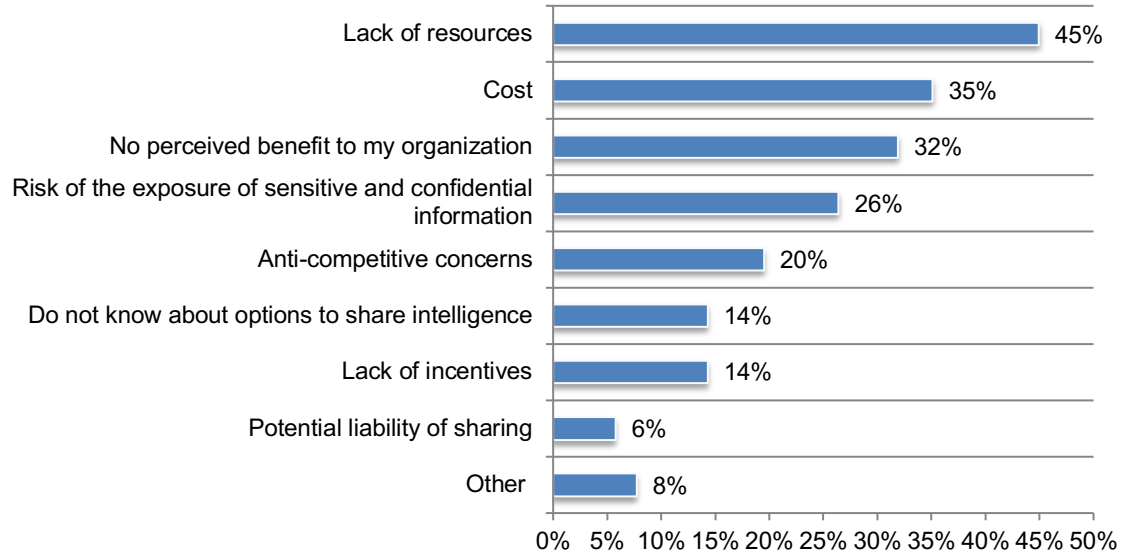
Having an incident response platform and sharing threat intelligence are considered key initiatives to improving cyber resilience. Almost half of respondents (49 percent) say their organizations participate in an initiative or program for sharing information with government and industry peers about data breaches and incident response.

As shown in Figure 19, 73 percent of respondents say sharing intelligence improves the security posture of their organization, and 69 percent of respondents say it improves the effectiveness of their incident response plan. 64 percent of respondents say threat intelligence sharing reduces the cost of detecting and preventing data breaches.

Figure 17. 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 (45 percent), it costs too much (35 percent) or no perceived benefit (32 percent), as can be seen in Figure 20.

Figure 18. Why doesn't your organization participate in a threat-sharing program?
Two choices allowed



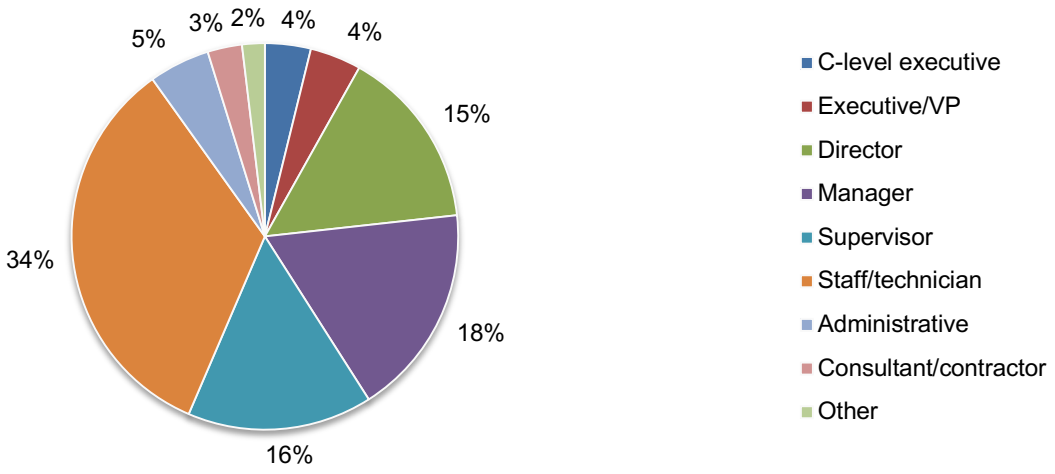
Part 4. Methods

Table 2 reports the sample response for Asia-Pacific. Our sampling frame of practitioners in Asia-Pacific consisted of 19,139 individuals who have bona fide credentials in IT or security fields. From this sampling frame, we captured 741 returns of which 102 were rejected for reliability issues. Our final 2017 sample was 639, thus resulting in an overall 3.3 percent response rate.

Table 2. Sample response	Freq	Pct%
Total sampling frame	19,139	100%
Total returns	741	3.9%
Rejected or screened surveys	102	0.8%
Final sample	639	3.3%

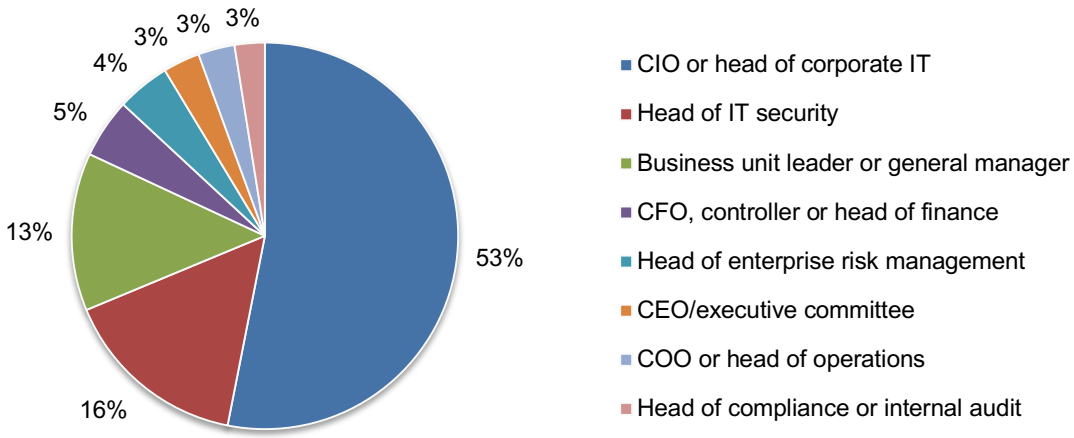
Pie Chart 1 reports respondents' organizational level within participating organizations. As can be seen, slightly more than half of the respondents (57 percent) are at or above the supervisory level.

Pie Chart 1. Distribution of respondents according to position level



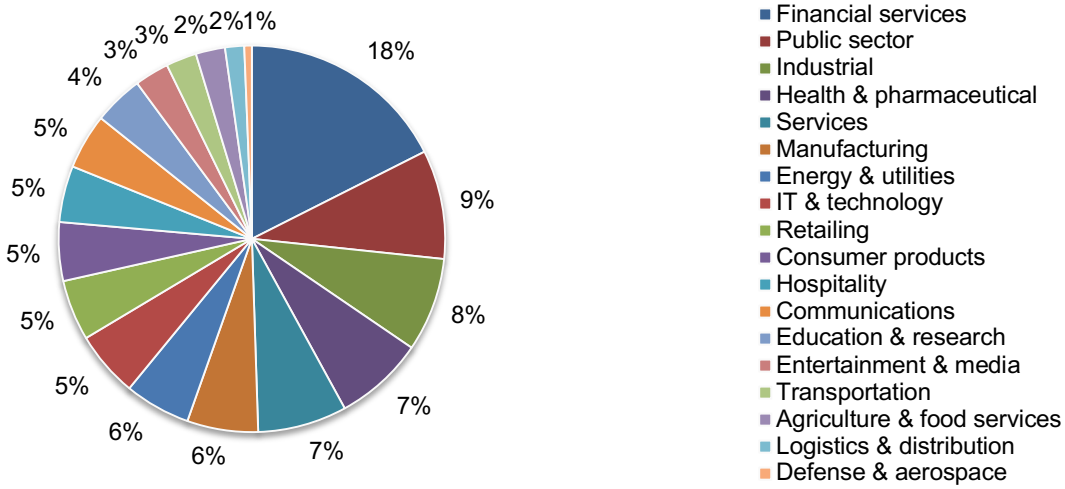
Pie Chart 2 reveals that 53 percent of respondents report directly to the CIO or head of corporate IT, 16 percent of respondents report to the head of IT security and 13 percent of respondents report to the business unit leader or general manager.

Pie Chart 2. Direct reporting channel or chain of command



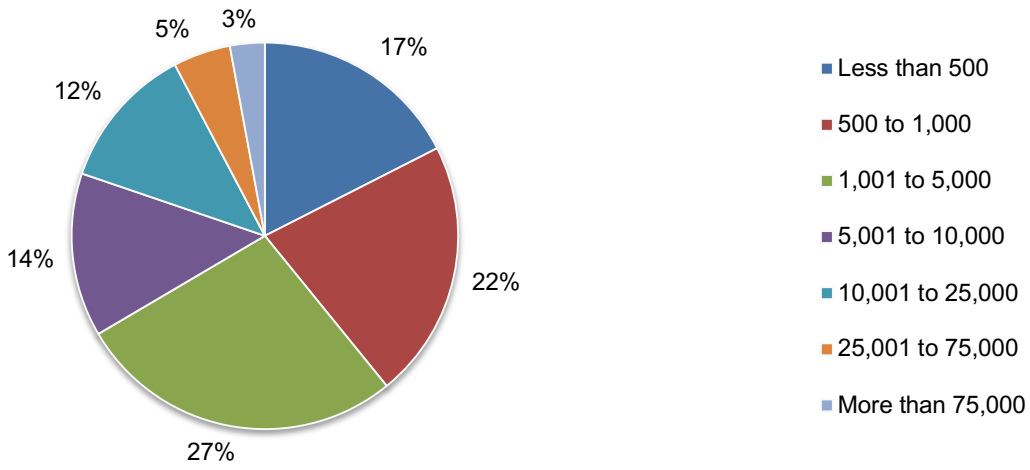
Pie Chart 3 reports the primary industry classification of respondents' organizations. This chart identifies financial services (18 percent of respondents) as the largest segment, followed by public sector (9 percent of respondents), industrial (8 percent of respondents), health and pharmaceuticals (7 percent of respondents) and services (7 percent of respondents).

Pie Chart 3. Primary industry classification



Pie Chart 4 reveals that 61 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
Total sampling frame	19,139
Total returns	741
Rejected or screened surveys	102
Final sample	639
Response rate	3.34%

Part 1. Screening

S1. What best describes your organizational role or area of focus?	2017
IT security operations	36%
IT operations	45%
CSIRT team	15%
Business continuity management	5%
None of the above (stop)	0%
Total	100%

S2. Please check all the activities that you see as part of your job or role.	2017
Managing budgets	48%
Evaluating vendors	50%
Setting priorities	41%
Securing systems	48%
Ensuring compliance	42%
Ensuring system availability	42%
None of the above (stop)	0%
Total	271%

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
Yes	55%
No	41%
Unsure	5%
Total	100%

Q1b. If yes, how frequently did these incidents occur during the past 2 years?	2017
Only once	40%
2 to 3 times	39%
4 to 5 times	11%
More than 5 times	9%
Total	100%

Q1c. If yes, did any of these data breaches require notification?	2017
Yes	10%
No	84%
Unsure	5%
Total	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	55%
No	41%
Unsure	4%
Total	100%

Q2b. If yes, how frequently did these incidents occur during the past 2 years?	2017
Only once	16%
2 to 3 times	22%
4 to 5 times	35%
More than 5 times	27%
Total	100%

Q3a. How has the volume of cybersecurity incidents changed in the past 12 months?	2017
Significantly increased	30%
Increased	35%
No increase	21%
Decreased	11%
Significantly decreased	3%
Total	100%

Q3b. How has the severity of security incidents changed in the past 12 months?	2017
Significantly increased	29%
Increased	37%
No increase	19%
Decreased	12%
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
Very frequently	19%
Frequently	25%
Somewhat frequently	31%
Rarely	21%
Never	3%
Total	100%

Q5. Using the following 10-point scale, please rate your organization's cyber resilience from 1 = low resilience to 10 = high resilience.	2017
1 or 2	12%
3 or 4	17%
5 or 6	33%
7 or 8	21%
9 or 10	16%
Total	100%
Extrapolated value	5.73

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
1 or 2	10%
3 or 4	17%
5 or 6	21%
7 or 8	26%
9 or 10	26%
Total	100%
Extrapolated value	6.36

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
1 or 2	9%
3 or 4	16%
5 or 6	28%
7 or 8	27%
9 or 10	21%
Total	100%
Extrapolated value	6.19

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
1 or 2	3%
3 or 4	19%
5 or 6	27%
7 or 8	36%
9 or 10	14%
Total	100%
Extrapolated value	6.25

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	3%
3 or 4	15%
5 or 6	29%
7 or 8	35%
9 or 10	17%
Total	100%
Extrapolated value	6.46

Q10. Please rate the value of cyber resilience to your organization from 1 = low to 10 = high.	2017
1 or 2	6%
3 or 4	10%
5 or 6	17%
7 or 8	33%
9 or 10	33%
Total	100%
Extrapolated value	7.04

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
1 or 2	3%
3 or 4	6%
5 or 6	16%
7 or 8	39%
9 or 10	37%
Total	100%
Extrapolated value	7.52

Q12. Please rate the difficulty in hiring and retaining skilled IT security personnel from 1 = low to 10 = high.	2017
1 or 2	3%
3 or 4	6%
5 or 6	18%
7 or 8	42%
9 or 10	31%
Total	100%
Extrapolated value	7.32

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
1 or 2	16%
3 or 4	31%
5 or 6	33%
7 or 8	12%
9 or 10	8%
Total	100%
Extrapolated value	4.83

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
Agility	2.0
Preparedness	1.8
Planned redundancies	4.3
Strong security posture	2.6
Knowledgeable or expert staff	3.8
Ample resources	4.9
Leadership	5.3

Q15a. How has your organization's cyber resilience changed in the past 12 months?	2017
Significantly improved	16%
Improved	29%
Somewhat improved	26%
Declined	5%
No improvement	24%
Total	100%

Q15b. If your organization has improved its cyber resilience, what caused the improvement? Please check your four top choices.	2017
Implementation of new technology, including cyber automation tools such as artificial intelligence and machine learning	44%
Elimination of silo and turf issues	40%
Visibility into applications and data assets	58%
Improved information governance practices	60%
C-level buy-in and support for the cybersecurity function	21%
Board-level reporting on the organization's cyber resilience	15%
Training and certification for IT security staff	29%
Training for end-users	32%
Hiring skilled personnel	61%
Engaging a managed security services provider	41%
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	25%
Time has increased	32%
Time has remained unchanged	32%
Time has decreased	8%
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	56%
Silo and turf issues	26%
Lack of visibility into applications and data assets	44%
Lack of information governance practices	24%
Lack of C-level buy-in and support for the cybersecurity function	17%
Lack of board-level reporting on the organization's state of cyber resilience	16%
Lack of training and certification for IT security staff	27%
Lack of training for end-users	32%
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
We have a CSIRP that is applied consistently across the entire enterprise	22%
We have a CSIRP, but is not applied consistently across the enterprise	31%
Our CSIRP is informal or "ad hoc"	27%
We don't have a CSIRP	20%
Total	100%

Q18b. If you have a CSIRP, how often is it reviewed and tested?	2017
Each quarter	6%
Twice per year	7%
Once each year	34%
No set time period for reviewing and updating the plan	38%
We have not reviewed or updated since the plan was put in place	15%
Total	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
Yes	49%
No	51%
Total	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
Improves the security posture of my organization	73%
Improves the effectiveness of our incident response plan	69%
Enhances the timeliness of incident response	63%
Reduces the cost of detecting and preventing data breaches	64%
Fosters collaboration among peers and industry groups	27%
Other (please specify)	5%
Total	300%

Q19c. If no, why does your organization not participate in a threat-sharing program? Please select only two choices.	2017
Cost	35%
Potential liability of sharing	6%
Risk of the exposure of sensitive and confidential information	26%
Anti-competitive concerns	20%
Lack of resources	45%
Lack of incentives	14%
No perceived benefit to my organization	32%
Do not know about options to share intelligence	14%
Other (please specify)	8%
Total	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
Other (please specify	3%
Wireless security solutions	9%
Next generation firewalls	10%
DDoS solutions	14%
Web application firewalls (WAF)	15%
Governance solutions (GRC)	15%
Data tokenization technology	17%
Code review and debugging systems	21%
Endpoint security solution	23%
Cloud SIEM	23%
Virtual private networks (VPN)	27%
User Behavioral Analytics (UBA)	27%
Big data analytics for cybersecurity	30%
Encryption for data in motion	35%
Security information & event management (SIEM)	39%
Data loss prevention (DLP)	44%
Network traffic surveillance	49%
Incident response platform	51%
Encryption for data at rest	51%
Intrusion detection & prevention systems	56%
Anti-virus / anti-malware	67%
Identity management & authentication	72%
Total	700%

Strongly Agree and Agree response: Please express your opinion about each one of the following statements using the agreement scale.	2017
Q21a. My organization's leaders recognize that enterprise risks affect cyber resilience.	61%
Q21b. My organization's leaders recognize that cyber resilience affects revenues.	56%
Q21c. My organization's leaders recognize that cyber resilience affects brand and reputation.	48%
Q21d. In my organization, funding for IT security is sufficient to achieve a high level of cyber resilience	34%
Q21e. In my organization, staffing for IT security is sufficient to achieve a high level of cyber resilience	31%
Q21f. My organization's leaders recognize that automation, machine learning, artificial intelligence and orchestration strengthens our cyber resilience.	66%

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
Business continuity manager	6%
Business unit leader	25%
Chief executive officer (CEO)	5%
Chief information officer (CIO)	31%
Chief technology officer (CTO)	4%
Chief risk officer (CRO)	7%
Chief information security officer (CISO)	12%
No one person has overall responsibility	10%
Other (please specify)	0%
Total	100%

Q23a. What is the full-time equivalent (FTE) headcount of your IT security function today?	2017
Less than 5	9%
5 to 10	16%
11 to 20	16%
21 to 30	14%
31 to 40	21%
41 to 50	12%
51 to 100	11%
More than 100	2%
Total	100%
Extrapolated value	30.5

Q23b. What should the full-time equivalent (FTE) headcount be to achieve cyber resilience?	2017
Less than 5	1%
5 to 10	3%
11 to 20	10%
21 to 30	14%
31 to 40	15%
41 to 50	24%
51 to 100	21%
More than 100	12%
Total	100%
Extrapolated value	51.5

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	24%
Less than 1 year	24%
1 to 3 years	25%
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	15%
Middle stage – cybersecurity program activities are planned and defined but only partially deployed	30%
Late-middle stage – many cybersecurity program activities are deployed across the enterprise	34%
Mature stage – Core cybersecurity program activities are deployed, maintained and/or refined across the enterprise	21%
Total	100%

Q28. What factors justify the funding of your organization's IT security? Please select two choices.	2017
System or application downtime	57%
Information loss or theft	50%
Performance degradation	17%
Productivity loss	12%
Revenue decline	9%
Reputation damage	12%
Customer defection	7%
Compliance/regulatory failure	36%
Other (please specify)	2%
Total	200%

Q29. Approximately, what is the dollar range that best describes your organization's current **cyber security budget**?	2017
< $1 million	14%
$1 to 5 million	22%
$6 to $10 million	31%
$11 to $15 million	17%
$16 to $20 million	12%
$21 to $25 million	3%
$26 to $50 million	1%
> $50 million	0%
Total	100%
Extrapolated value ($millions)	8.6

Q30. Approximately, what percentage of the current **cyber security budget** will go to cyber resilience-related activities?	2017
< 2%	0%
2% to 5%	3%
6% to 10%	11%
11% to 20%	14%
21% to 30%	43%
31% to 40%	13%
41% to 50%	10%
51% to 60%	5%
61% to 70%	2%
71% to 80%	0%
81% to 90%	0%
91 to 100%	0%
Total	100%
Extrapolated value (percentage)	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
Prevention	47
Detection	24
Containment	14
Remediation	11
Post incident response	5
Total	100

Organizational and respondent characteristics

D1. What best describes the position level within the organization?	2017
C-level executive	4%
Executive/VP	4%
Director	15%
Manager	18%
Supervisor	16%
Staff/technician	34%
Administrative	5%
Consultant/contractor	3%
Other (please specify)	2%
Total	100%

D2. What best describes your reporting channel or chain of command?	2017
CEO/executive committee	3%
COO or head of operations	3%
CFO, controller or head of finance	5%
CIO or head of corporate IT	53%
Business unit leader or general manager	13%
Head of compliance or internal audit	3%
Head of enterprise risk management	4%
Head of IT security	16%
Other (please specify)	0%
Total	100%

D3. What best describes your organization's primary industry classification?	2017
Agriculture & food services	2%
Communications	5%
Consumer products	5%
Defense & aerospace	1%
Education & research	4%
Energy & utilities	6%
Entertainment & media	3%
Financial services	18%
Health & pharmaceutical	7%
Hospitality	5%
Industrial	8%
IT & technology	5%
Logistics & distribution	2%
Manufacturing	6%
Public sector	9%
Retailing	5%
Services	7%
Transportation	3%
Total	100%

D4. What range best describes the full-time headcount of your global organization?	2017
Less than 500	17%
500 to 1,000	22%
1,001 to 5,000	27%
5,001 to 10,000	14%
10,001 to 25,000	12%
25,001 to 75,000	5%
More than 75,000	3%
Total	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.