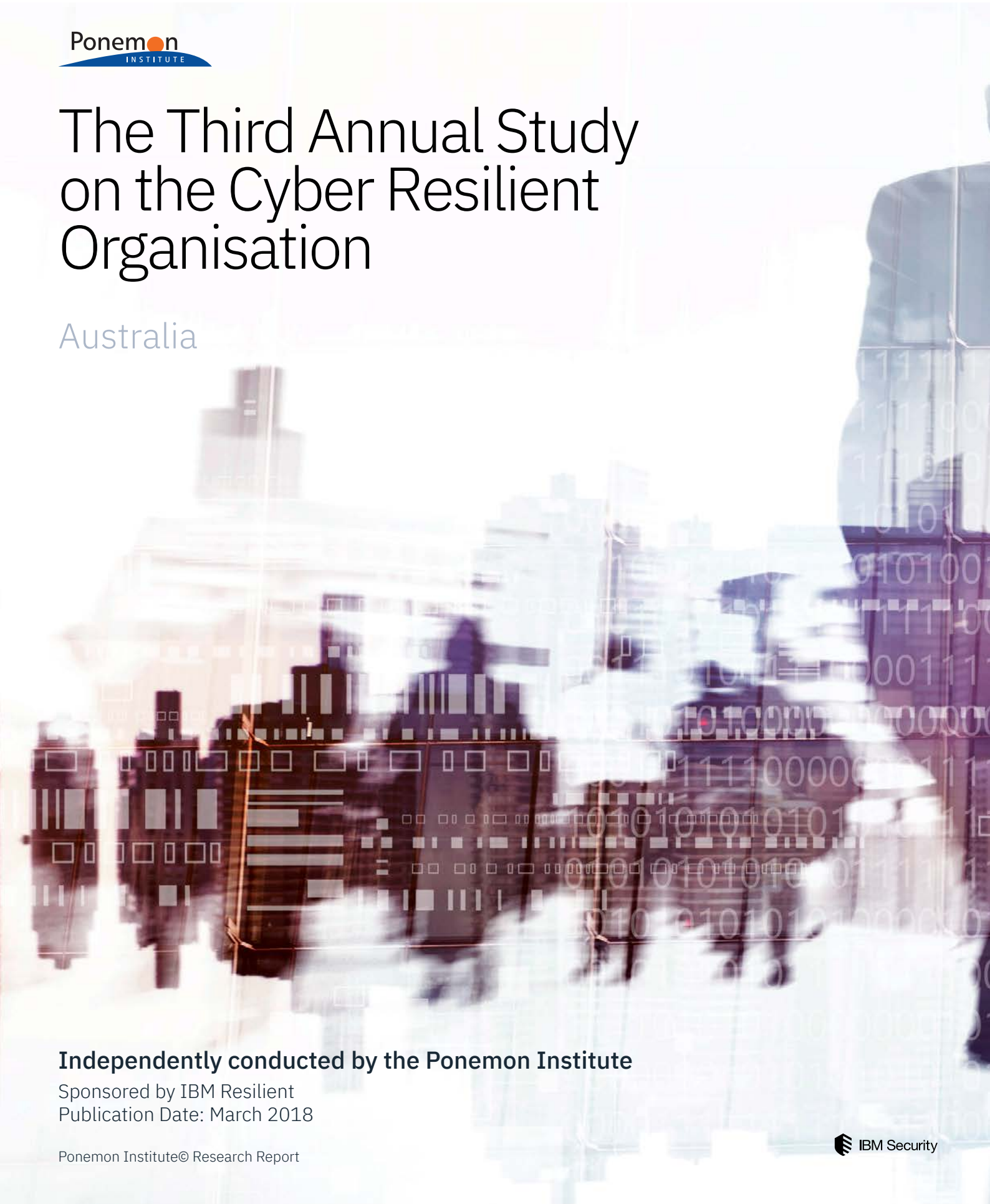
Ponemon INSTITUTE

The Third Annual Study on the Cyber Resilient Organisation

Australia



Independently conducted by the Ponemon Institute

Sponsored by IBM Resilient
Publication Date: March 2018

IBM Security

The Third Annual Study on the Cyber Resilient Organisation: Australia

Ponemon Institute, April 2018

Part 1. Introduction

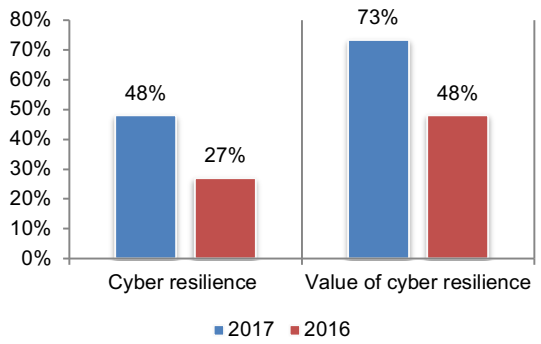
The Ponemon Institute and IBM Resilient are pleased to release the findings of the third annual study on the importance of cyber resilience for a strong security posture. *The key takeaway from this year's research is that organisations globally continue to struggle with responding to cybersecurity incidents. 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 Australia, the second time that this research has been conducted in this market.

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 organisations' cyber resilience on a scale from 1= low to 10 = high. As shown in Figure 1, since last year's research there has been a significant increase from 27 percent of respondents to 48 percent of respondents in the perception that their organisations have achieved a higher level of cyber resilience. Respondents' perceptions about the value of cyber resilience to their organisations also increased significantly (from 48 percent of respondents to 73 percent of respondents). At 48 percent, the Australian perception of cyber resilience is exactly in line with the global findings.

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

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



Major challenges to achieving cyber resilience remain.

Companies represented in this research revealed that there are a number of areas that hinder effective and efficient incident response. Chief among them is that 76 percent of organisations admit they do not have a formal cybersecurity incident response plan (CSIRP) that is applied consistently across the organisation. The report also found that just 39 percent of respondents feel that they have an adequate cyber resilience budget in place.

Following are other key takeaways from this research:

More respondents believe senior management recognises the value of cyber resilience. Since 2016, recognition among senior leadership about how enterprise risks affect their organisations' ability to withstand cyber attacks has remained the same. However, more respondents believe cyber resilience affects revenues and brand and reputation. 53 percent of respondents say their leaders understand that automation, machine learning, artificial intelligence and orchestration strengthens cyber resilience.

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

More companies are succeeding in improving their cyber resilience. Respondents are rating their ability to prevent and detect a cyber attack as higher than in 2016. 52 percent of respondents rate their ability to respond to a cyber attack as high or very high. 48 percent of respondents say their organisations' cyber resilience has significantly improved or improved over the past 12 months. In last year's study, 27 percent of respondents said their organisations' cyber resilience significantly improved or improved.

Hiring skilled personnel improves cyber resiliency. Reasons for improvement include hiring skilled personnel (68 percent of respondents), improved information governance practices (59 percent of respondents) and visibility into applications and data assets (57 percent of respondents).

Preparedness and a strong security posture are the most important factors to achieving a high level of cyber resilience. Respondents were asked to rate the most important factors for achieving cyber resilience. Preparedness and a strong security posture are the most important factors. Planned redundancies have increased in importance in the past two years.

IT and IT security are responsible for ensuring a high level of cyber resilience. If you combine the chief information officer (27 percent of respondents), chief information security officer (13 percent of respondents) and chief technology officer (5 percent), 45 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 achieving 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 overcome to improve cyber resilience. Respondents were asked to rate the importance of skilled cybersecurity professionals and the difficulty in hiring these personnel on a scale of 1 = low to 10 = high. Seventy-three percent of respondents rate the importance of having skilled cybersecurity professionals in their cybersecurity response plan (CSIRP) as high or very high. However, 74 percent of respondents rate the difficulty in hiring and retaining skilled IT security personnel as high or very high.

Staffing is inadequate. In fact, only 26 percent of respondents agree that in their organisation, staffing for IT security is sufficient to achieve a high level of cyber resilience. The ideal average FTE should be 38 full-time security professionals.

Incident response plans often do not exist or are "ad hoc." Only 24 percent of respondents say they have a CSIRP that is applied consistently across the enterprise. Of the 78 percent of respondents who say their organisation has a CSIRP, 44 percent of respondents say there is no set time period for reviewing and updating the plan, and 35 percent of respondents say they review once each year.

More funds are allocated to detection of a security incident. Respondents were asked to allocate 100 percentage points to five areas of a CSIRP. As discussed previously, respondents report their organisations have significantly improved their ability to detect an incident. Allocation of investment to detection has increased from 29 percent to 32 percent. Prevention has declined from 42 percent to 38 percent.

Funding decreases for cybersecurity and cyber resilience budgets. Only 39 percent of respondents say funding for IT security is sufficient to achieve a high level of cyber resilience.

The average budget for cybersecurity has declined from $7.4 million to $6.2 million and cyber resilience has decreased from $2.1 million to $1.6 million.

The severity and volume of cybersecurity incidents increases the time to resolve a security incident. 62 percent of respondents say the volume has increased (27 percent + 35 percent) and 65 percent (30 percent + 35 percent) say the severity has increased.

The increase in the volume and severity of cybersecurity incidents has had a negative effect on the time to resolve a cyber incident. 53 percent of respondents say the time to detect, contain and respond to a cyber crime incident has increased (32 percent) or increased significantly (21 percent).

More than half of companies represented in this study have deployed many of their core cybersecurity program activities. 54 percent of respondents say the maturity of their cybersecurity program is late-middle or mature stage.

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

Having an incident response platform and sharing intelligence about data breaches are considered key initiatives to improving cyber resilience. 48 percent of respondents say their organisations participate in an initiative or program for sharing information with government and industry peers about data breaches and incident response. 75 percent of respondents say sharing intelligence improves the security posture of their organisation, and 65 percent of respondents say it improves the effectiveness of their incident response plan. More respondents in this year's research say sharing information reduces the cost of detecting and preventing data breaches.

A lack of resources and no perceived benefits are reasons not to share threat intelligence. Why are some companies reluctant to share intelligence? According to respondents who don't share threat intelligence, it is because there is no perceived benefit (44 percent), a lack of resources (38 percent), and a risk of exposure of sensitive and confidential information (29 percent).

The survey findings for Australia are broadly in line with the global averages. Comparing the Australian results with the global findings, we can see that Australia is typically in the middle of the results. The Australian perception of cyber resilience is 48 percent, the same as the global number. Australian respondents are more likely to believe in the value of cyber resilience (73 percent versus 65 percent) but are less likely than others to participate in sharing threat intelligence (48 percent versus 53 percent). One area in which Australia seems to be lagging behind other countries is GDPR readiness, where only 19 percent of Australian respondents rated their ability to comply with the upcoming regulation as 'high' versus a global average of 56 percent.

Part 2. Key findings

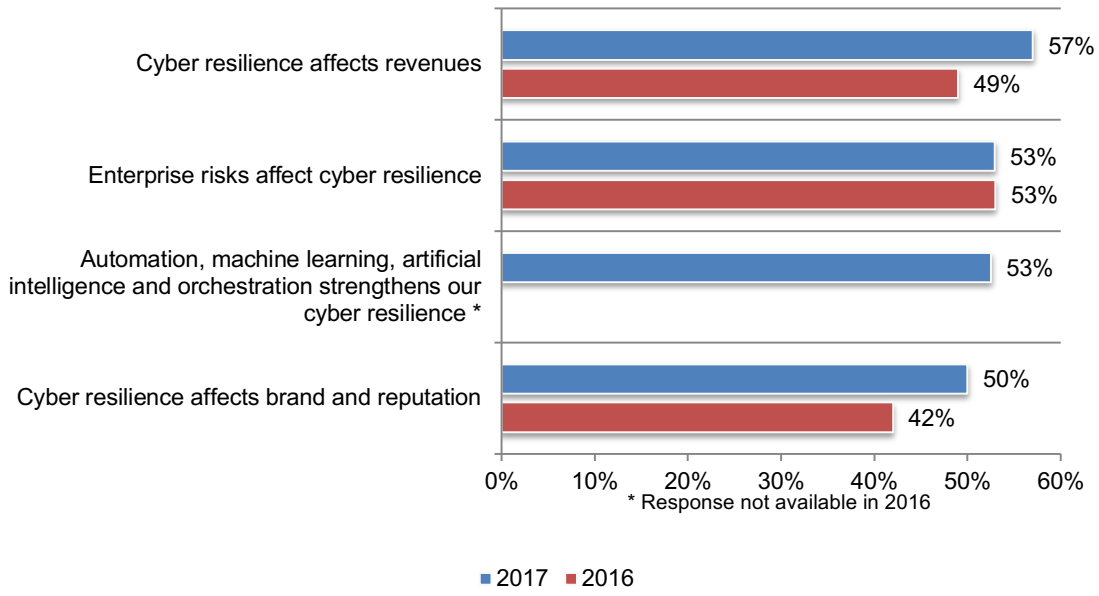
In this section of the report, we provide an analysis of the key findings. The complete audited findings are presented in the Appendix of this report. We have organised the findings according to the following topics.

- Cyber resilience effectiveness increases significantly
- Hurdles to further improvement in cyber resilience
- Technologies and governance practices to support cyber resilience

Cyber resilience effectiveness increases significantly

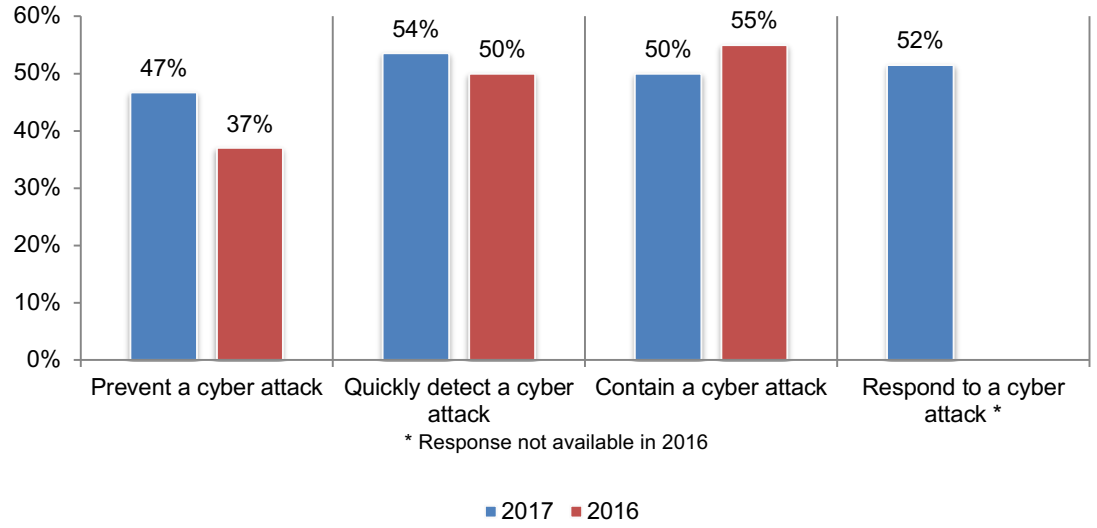
More respondents believe senior management recognises the value of cyber resilience. According to Figure 2**,** since 2016, recognition among senior leadership about how enterprise risks affect their organisations' ability to withstand cyber attacks has remained the same. However, more respondents believe cyber resilience affects revenues and brand and reputation. Fifty-three percent of respondents say their leaders understand that automation, machine learning, artificial intelligence and orchestration strengthens cyber resilience.

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



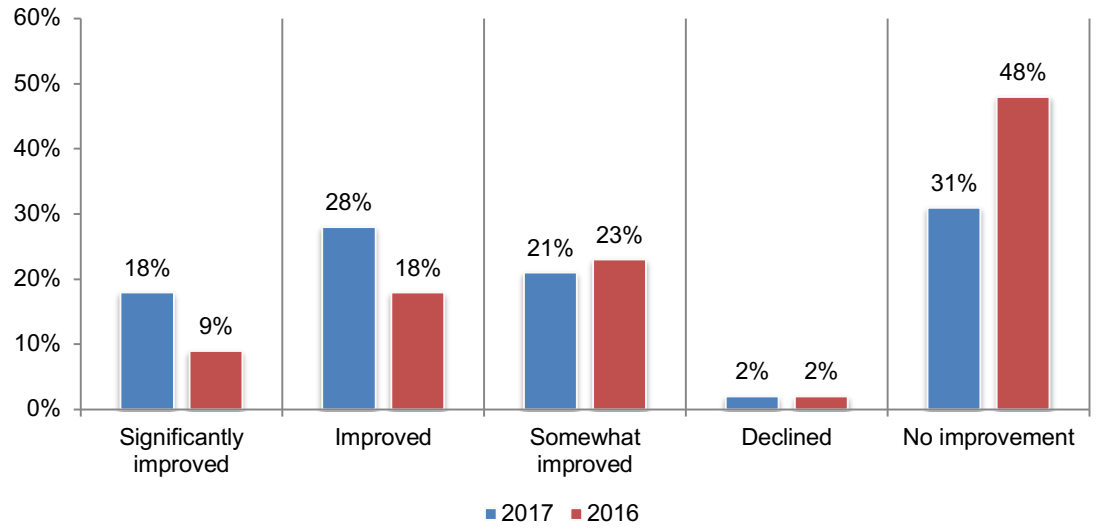
More companies are succeeding in improving their cyber resilience. As shown in Figure 3, respondents are rating their ability to prevent and detect a cyber attack as higher than in 2016, 52 percent of respondents rate their ability to respond to a cyber attack as high or very high.

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



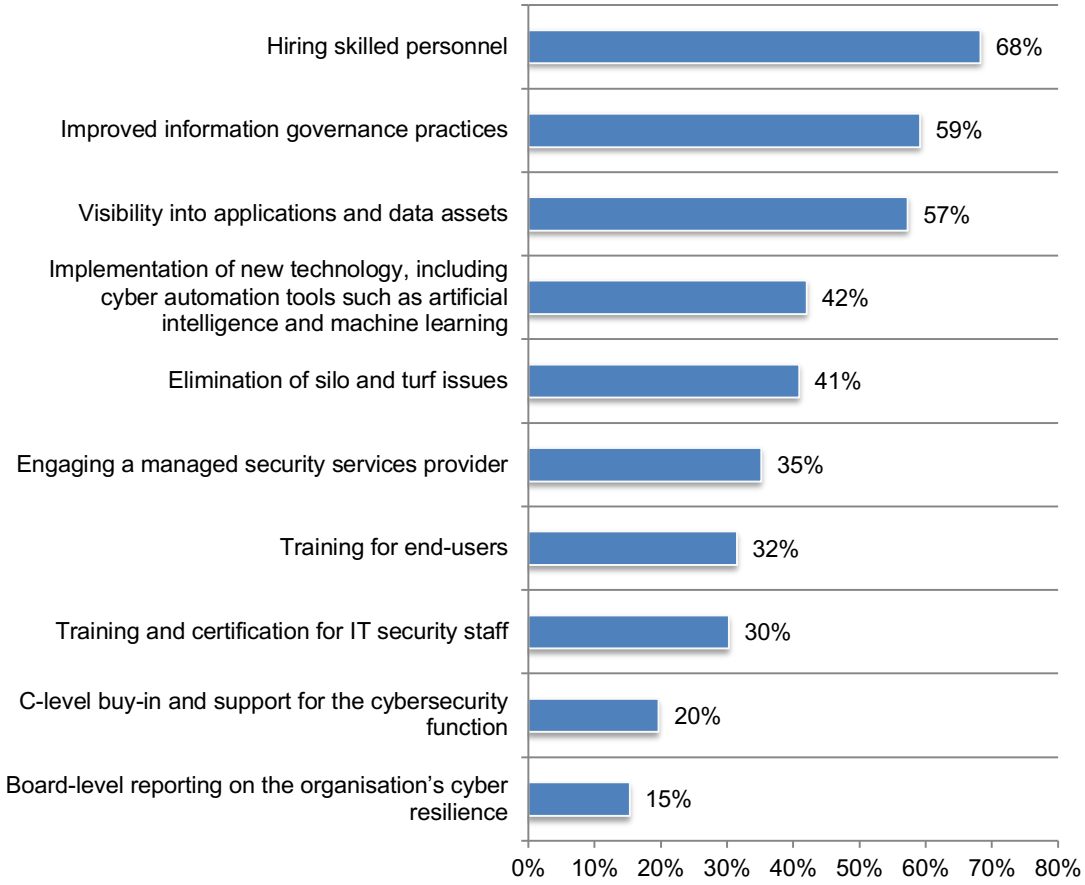
46 percent of respondents say their organisations' cyber resilience has significantly improved or improved over the past 12 months. In last year's study, 27 percent of respondents said their organisations' cyber resilience significantly improved or improved, as shown in Figure 4.

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



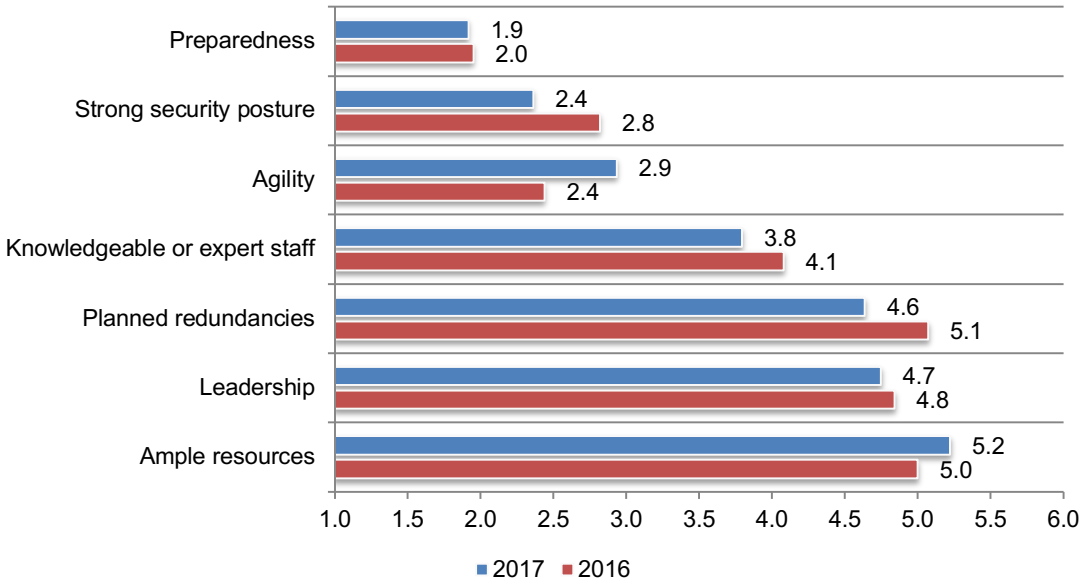
Hiring skilled personnel improves cyber resiliency. Reasons for improvement include hiring skilled personnel (68 percent of respondents), improved information governance practices (59 percent of respondents) and visibility into applications and data assets (57 percent of respondents), as shown in Figure 5.

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



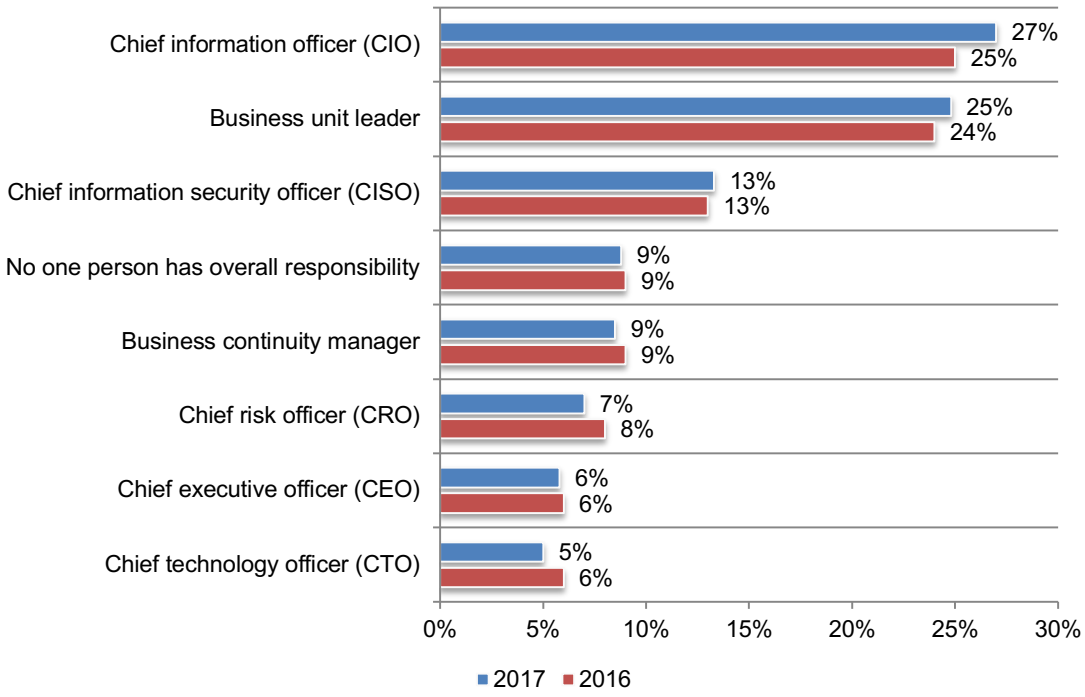
Preparedness and a strong security posture are the most important factors to achieving a high level of cyber resilience. Respondents were asked to rate the most important factors for achieving cyber resilience. According to Figure 6, preparedness and a strong security posture are the most important factors.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

Figure 6. The seven factors considered important in achieving a high level of cyber resilience
1 = most important to 7 = least important



IT and IT security are responsible for ensuring a high level of cyber resilience. Figure 7 presents the functions with overall responsibility for the strength of their organisations' cyber resilience activities. If you combine the chief information officer (27 percent of respondents), chief information security officer (13 percent of respondents) and chief technology officer (5 percent), 45 percent of respondents say the overall responsibility for cyber resilience resides in the IT and IT security function.

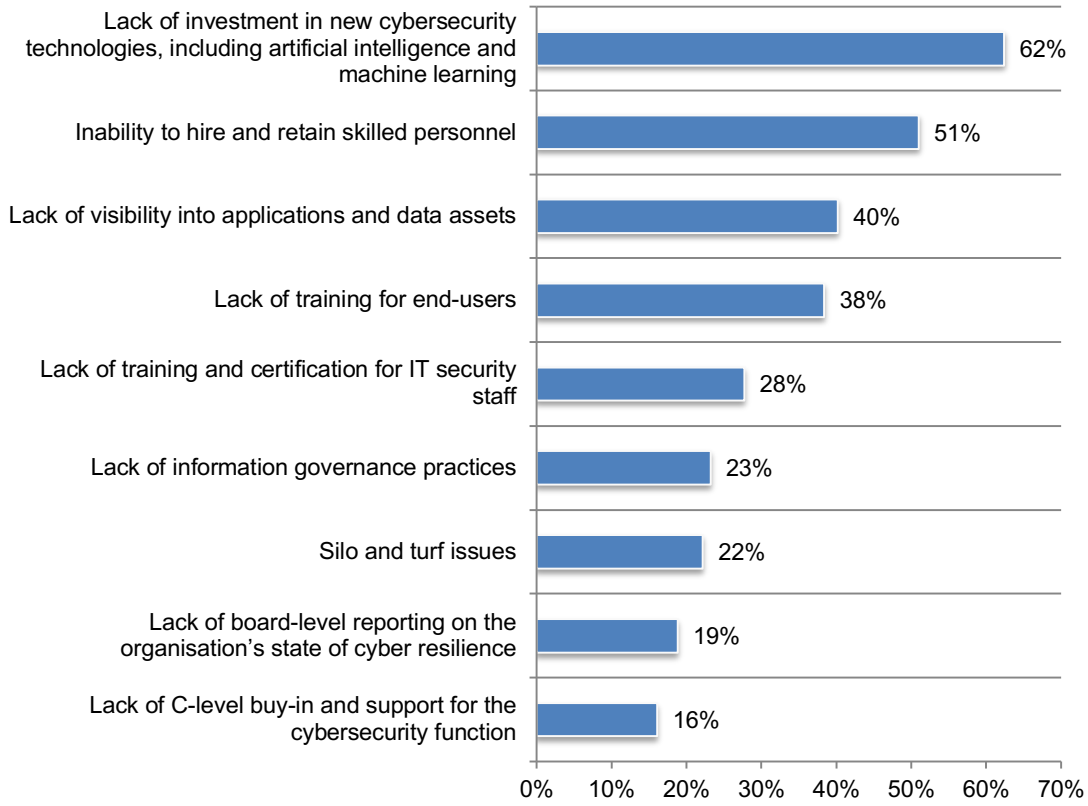
Figure 7. Who has overall responsibility for directing your organisation's efforts to ensure a high level of cyber resilience?



Hurdles to further improvements in cyber resilience

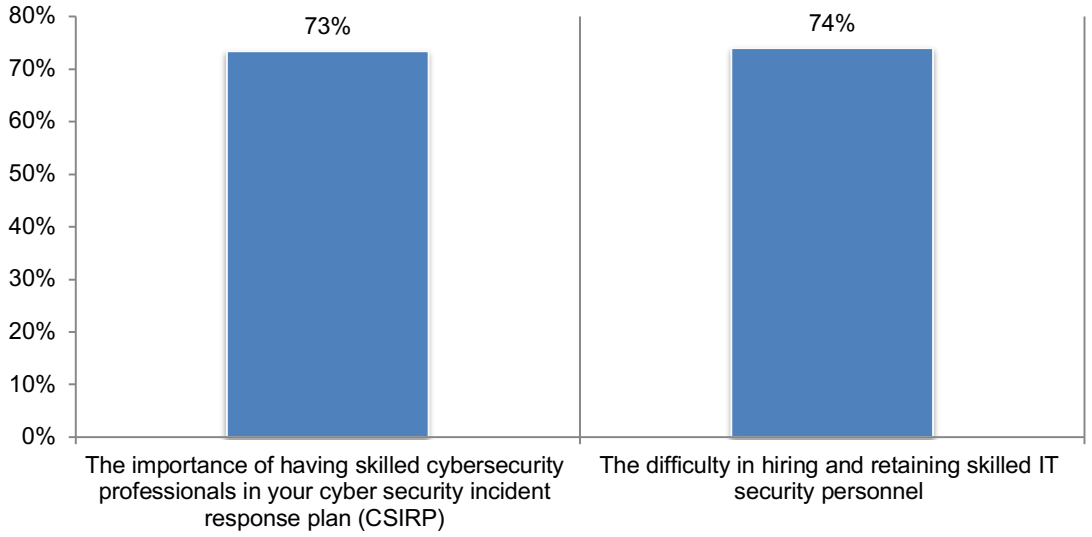
Cybersecurity technologies and skilled personnel are critical to achieving a high level of cyber resilience. Lack of investment in new cybersecurity technologies, including artificial intelligence and machine learning, and the inability to hire and retain skilled personnel are the biggest barriers to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

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



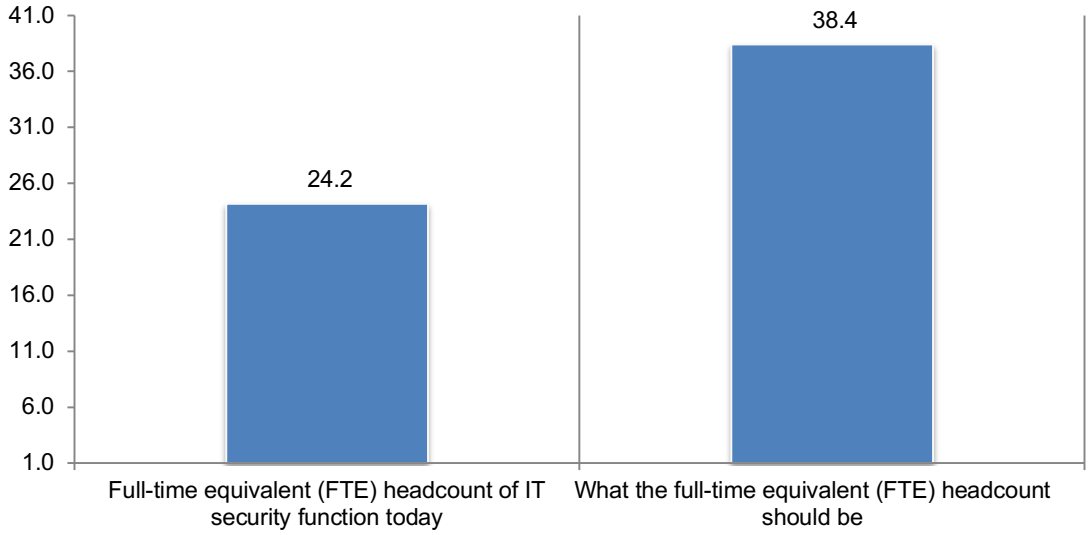
Hiring and retaining skilled IT security personnel is a serious hurdle to overcome to improve cyber resilience. Respondents were asked to rate the importance of skilled cybersecurity professionals and the difficulty in hiring these personnel on a scale of 1 = low to 10 = high. Seventy-three percent of respondents rate the importance of having skilled cybersecurity professionals in their cybersecurity response plan (CSIRP) as high or very high. However, 74 percent of respondents rate the difficulty in hiring and retaining skilled IT security personnel as high or 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 26 percent of respondents agree that in their organisation, staffing for IT security is sufficient to achieve a high level of cyber resilience. As shown in Figure 10, the ideal average FTE should be 38 full-time security professionals.

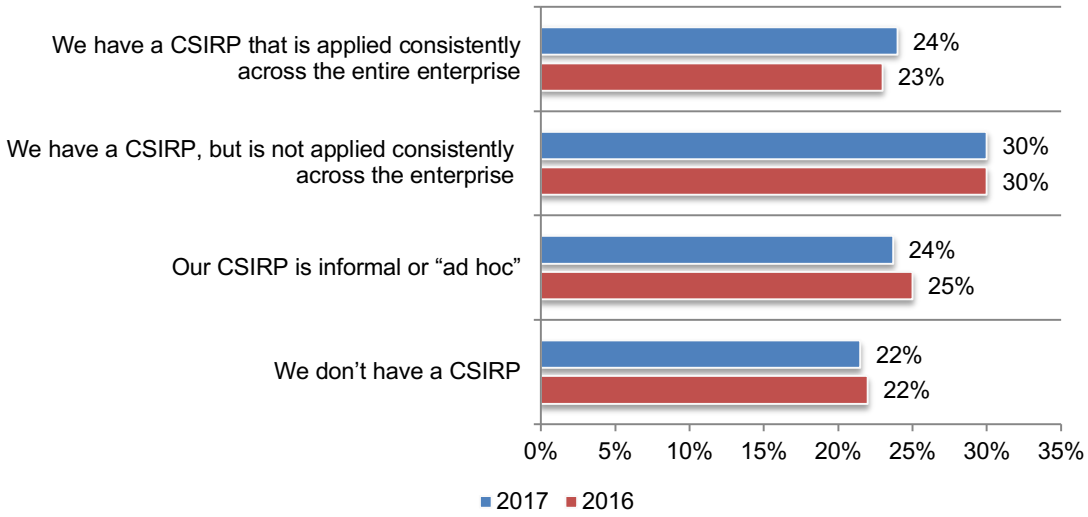
Figure 10. Average full-time headcount today and what it should be
Extrapolated average



Incident response plans often do not exist or are "ad hoc." According to Figure 11, only 24 percent of respondents say they have a CSIRP that is applied consistently across the enterprise.

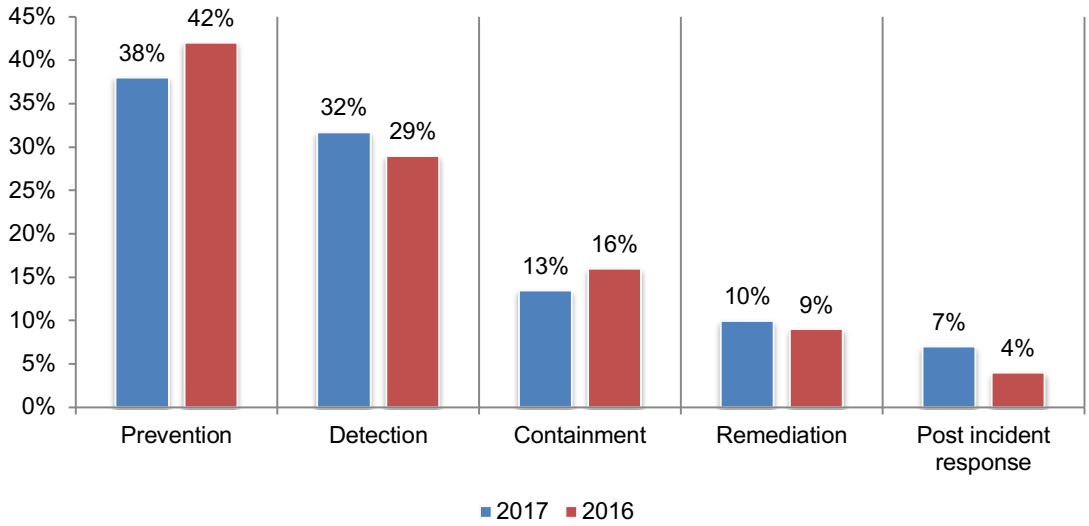
Of the 78 percent of respondents who say their organisation has a CSIRP, 44 percent of respondents say there is no set time period for reviewing and updating the plan, and 35 percent of respondents say they review once each year.

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



More funds are allocated to detection of a security incident. Respondents were asked to allocate 100 percentage points to five areas of a CSIRP. As discussed previously, respondents report their organisations have significantly improved their ability to detect an incident. As shown in Figure 12, allocation of investment to detection has increased from 29 percent to 32 percent. Prevention has declined from 42 percent to 38 percent.

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

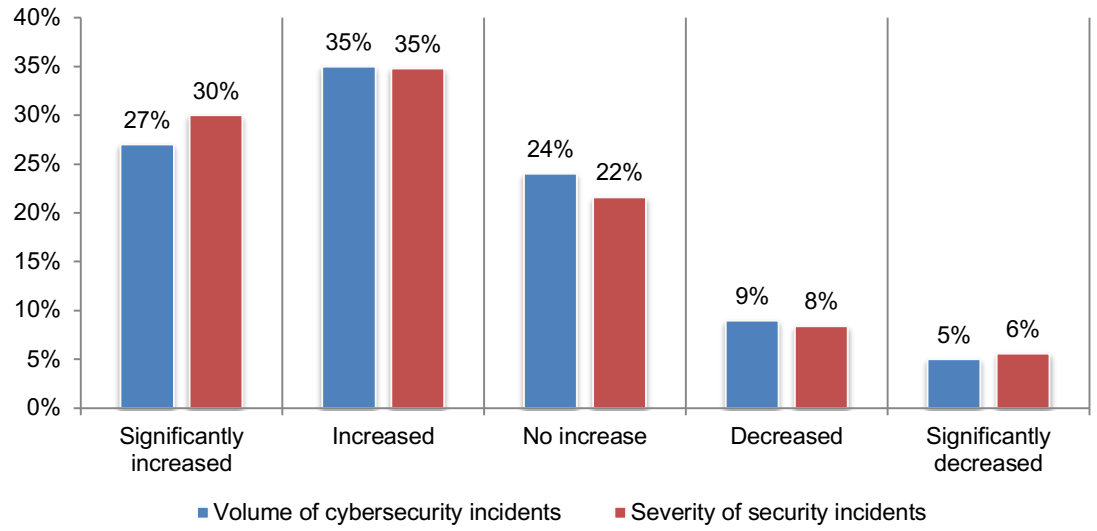


Funding decreases for cybersecurity and cyber resilience budgets. Only 39 percent of respondents say funding for IT security is sufficient to achieve a high level of cyber resilience. As shown in Table 1, the average budget for cybersecurity has declined from $7.4 million to $6.2 million and cyber resilience has decreased from $2.1 million to $1.6 million.

Table 1. Budget for cybersecurity & cyber resilience activities		
Extrapolated average (millions)	2017	2016
Cybersecurity budget	$6.2	$7.4
Percentage allocated to cyber resilience activities	25%	28%
Total average budget allocated to cyber resilience	$1.6	$2.1

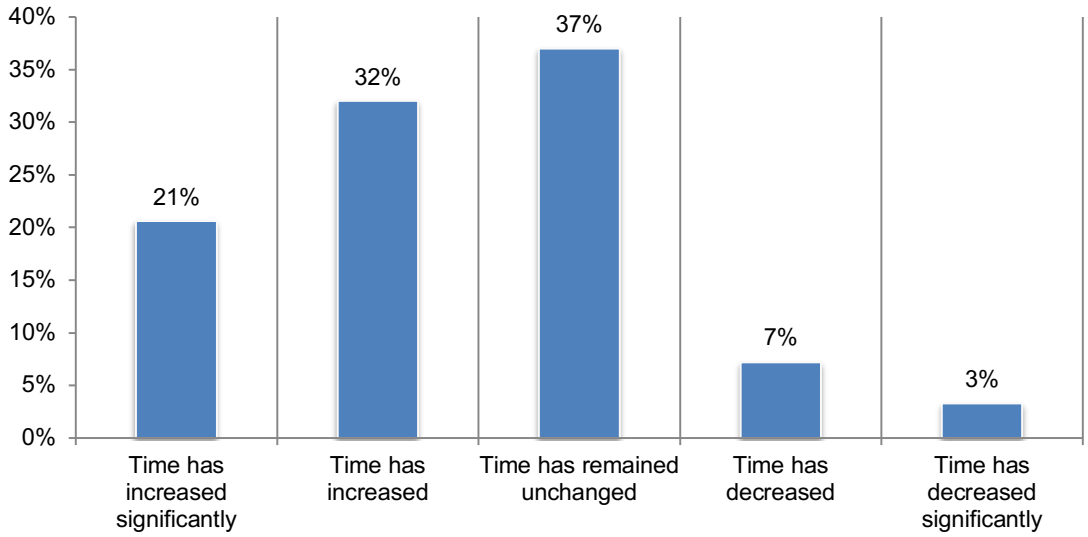
The severity and volume of cybersecurity incidents increases the time to resolve a security incident. As shown in Figure 13, 62 percent of respondents say the volume has increased (27 percent + 35 percent) and 65 percent (30 percent + 35 percent) say the severity has increased.

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



The increase in volume and severity of cybersecurity incidents has had a negative effect on the time to resolve a cyber incident has increased significantly. According to Figure 14, 53 percent of respondents say the time has increased significantly (21 percent) or increased (32 percent).

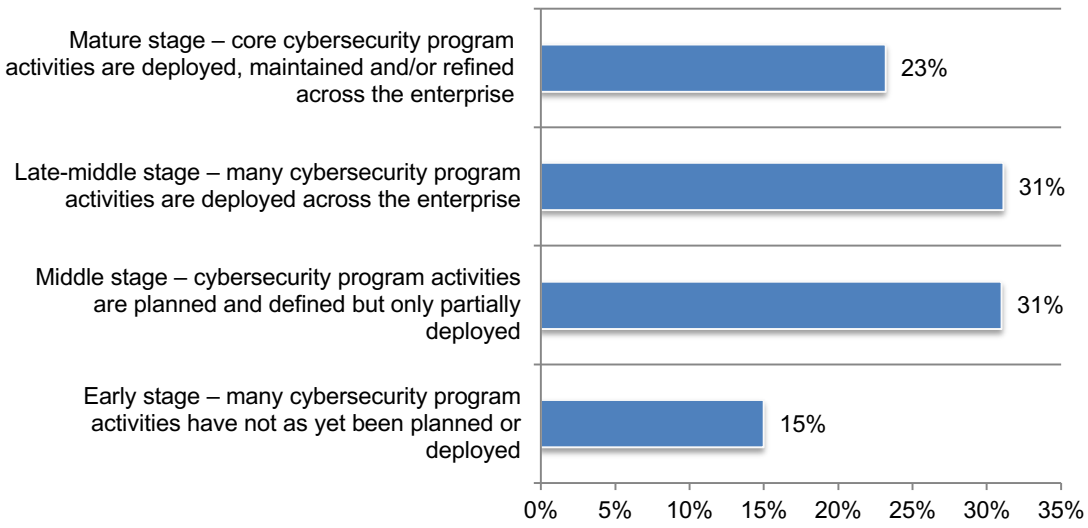
Figure 14. In the past 12 months, how has the time to detect, contain and respond to a cyber crime changed?



Technologies and governance practices to support cyber resilience

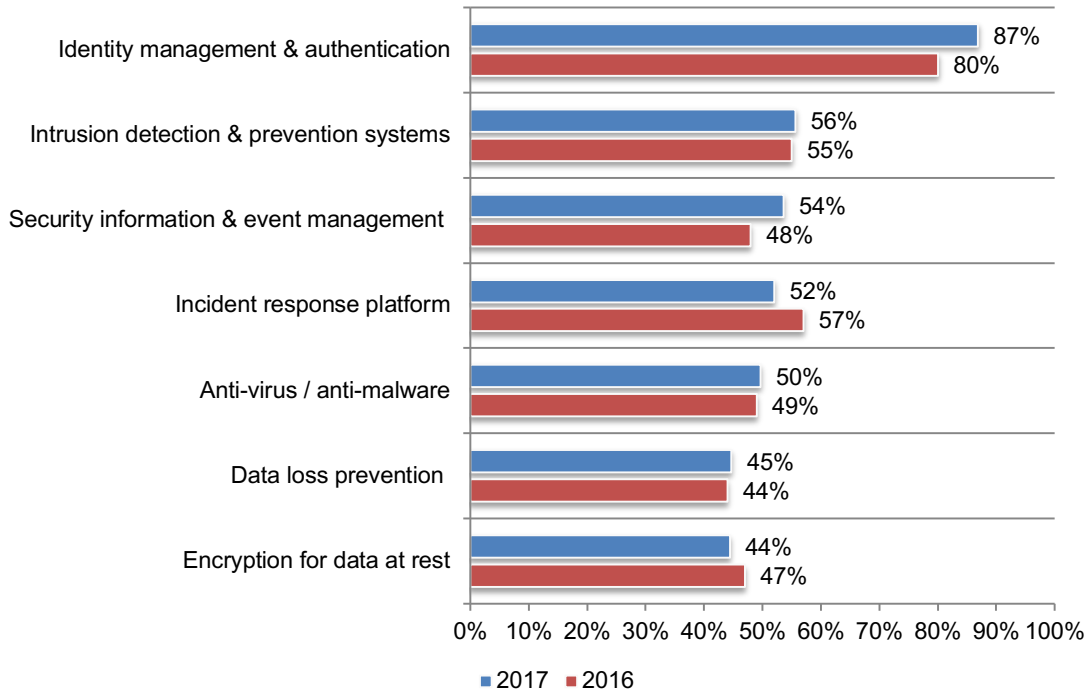
More than half of companies represented in this study have deployed many of their core cybersecurity program activities. As shown in Figure 15, 54 percent of respondents say the maturity of their cybersecurity program is late-middle or mature stage.

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



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

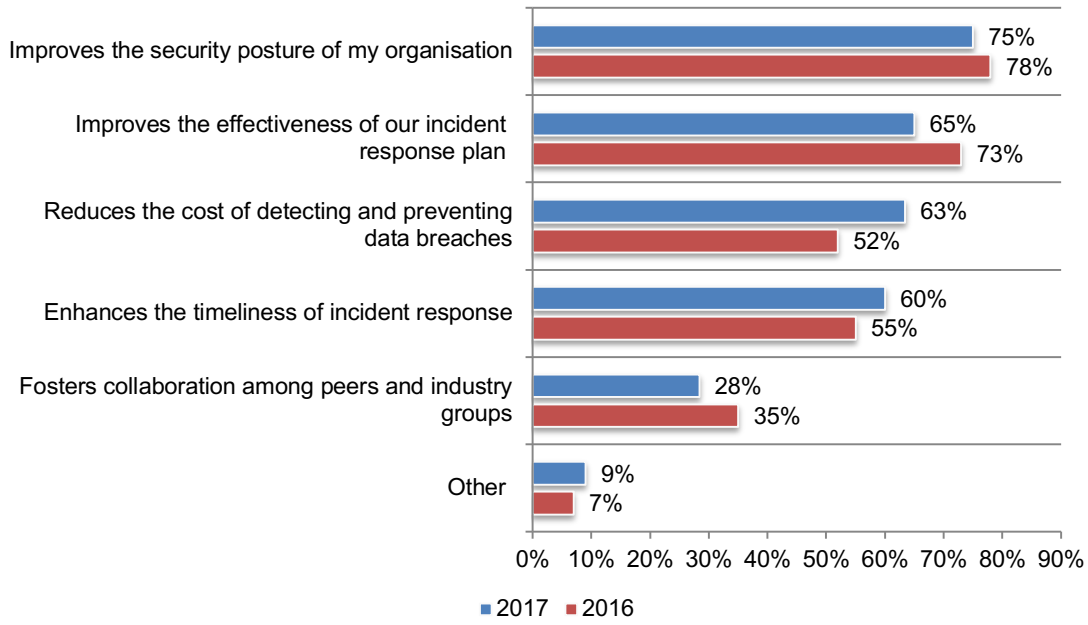
Figure 16. The seven most effective security technologies
Twenty-one technologies were listed in the survey instrument



Having an incident response platform and sharing intelligence about data breaches are considered key initiatives to improving cyber resilience. 48 percent of respondents say their organisations participate in an initiative or program for sharing information with government and industry peers about data breaches and incident response. This is under the global average of 53 percent.

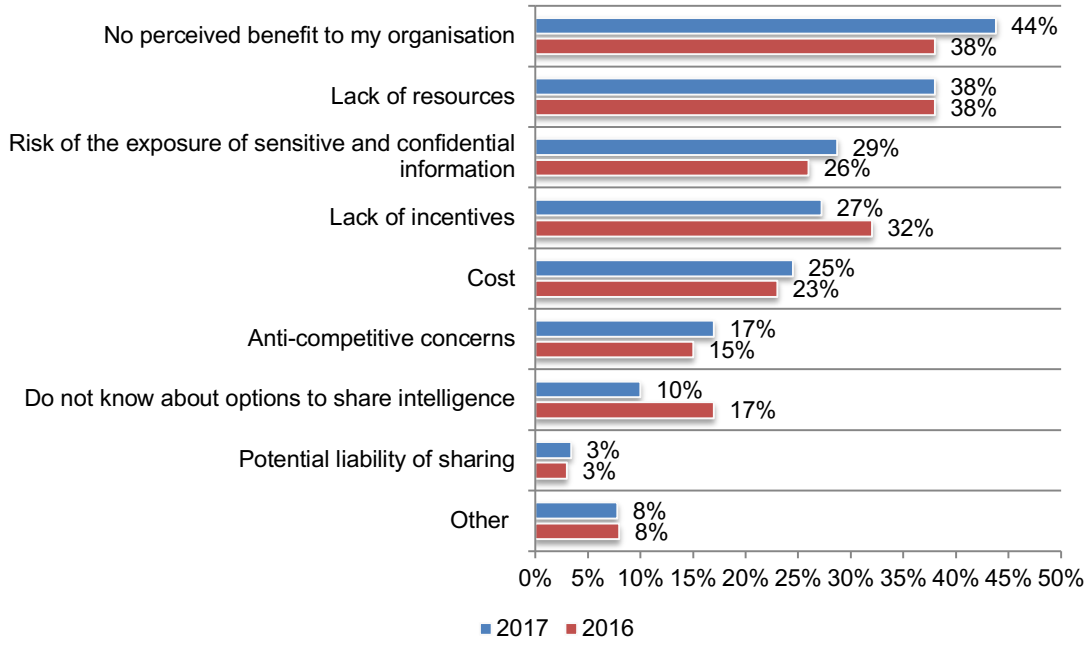
As shown in Figure 17, 75 percent of respondents say sharing intelligence improves the security posture of their organisation, and 65 percent of respondents say it improves the effectiveness of their incident response plan. More respondents in this year's research say sharing information reduces the cost of detecting and preventing data breaches.

Figure 17. Why does your organisation 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 no perceived benefit (44 percent), a lack of resources (38 percent), and the risk of exposure of sensitive and confidential information (29 percent), as can be seen in Figure 18.

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



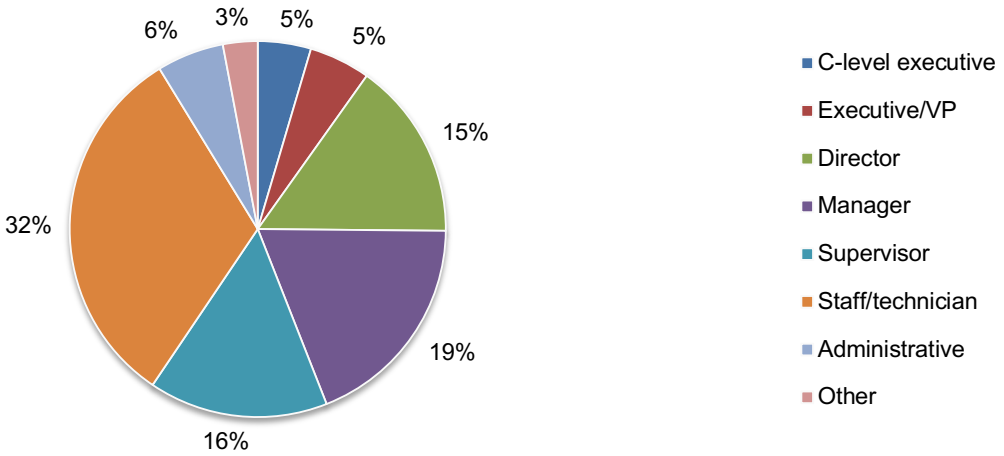
Part 4. Methods

Table 2 reports the sample response for Australia. Our sampling frame of practitioners in Australia consisted of 6,800 individuals who have bona fide credentials in IT or IT security fields. From this sampling frame, we captured 279 returns of which 44 were rejected for reliability issues. Our final 2017 sample was 254, thus resulting in an overall 3.5 percent response rate.

Table 2. Sample response	Freq	Pct%
Total sampling frame	6,800	100%
Total returns	279	4.1%
Rejected or screened surveys	44	0.6%
Final sample	254	3.5%

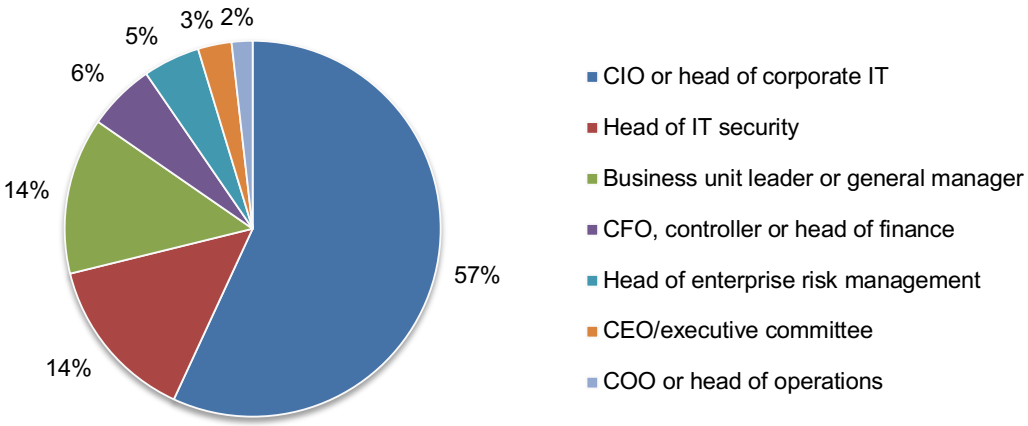
Pie Chart 1 reports respondents' organisational level within participating organisations. As can be seen, more than half of respondents (60 percent) are at or above the supervisory level.

Pie Chart 1. Distribution of respondents according to position level



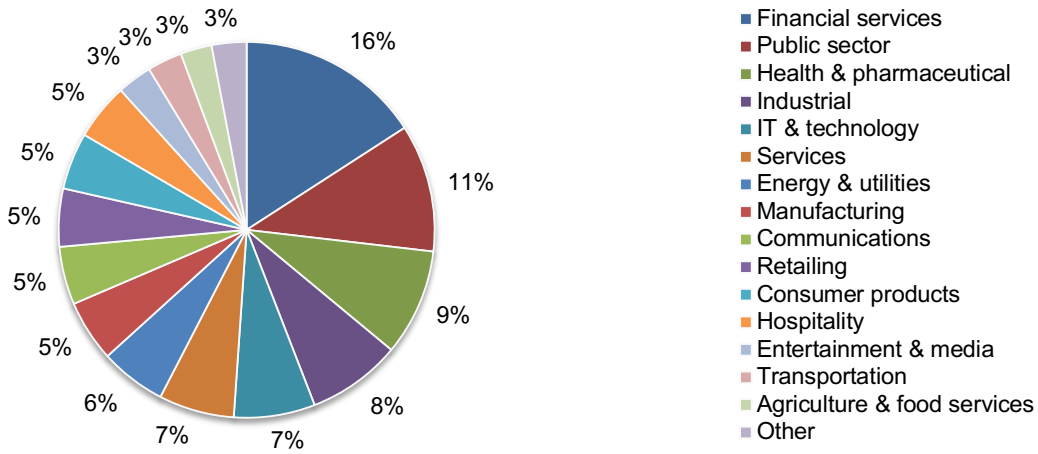
Pie Chart 2 reveals that 57 percent of respondents report directly to the CIO or head of corporate IT, 14 percent of respondents report to the head of IT security and 14 percent of respondents report to the business unit leader or general manager.

Pie Chart 2. Direct reporting channel or chain of command



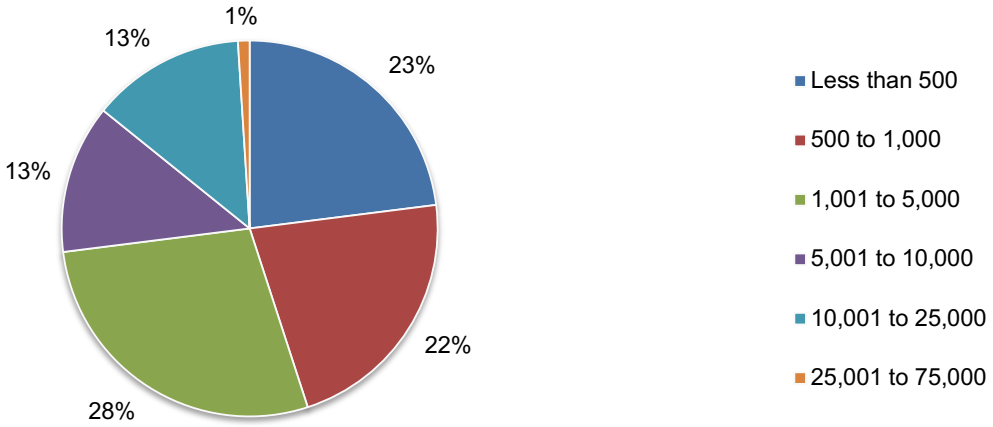
Pie Chart 3 reports the primary industry classification of respondents' organisations. This chart identifies financial services (16 percent) as the largest segment, followed by public sector (11 percent), health and pharmaceuticals (9 percent) and industrial (8 percent).

Pie Chart 3. Primary industry classification



Pie Chart 4 reveals that approximately half of respondents (55 percent) are from organisations with a worldwide headcount of more than 1,000 employees.

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



Part 4. Caveats to this study

There are inherent limitations to survey research that need to be carefully considered before drawing inferences from findings. The following items are specific limitations that are germane to most Web-based surveys.

- Non-response bias: The current findings are based on a sample of survey returns. We sent surveys to a representative sample of individuals, resulting in a large number of usable returned responses. Despite non-response tests, it is always possible that individuals who did not participate are substantially different in terms of underlying beliefs from those who completed the instrument.

- Sampling-frame bias: The accuracy is based on contact information and the degree to which the list is representative of individuals who are IT or IT security practitioners. We also acknowledge that the results may be biased by external events such as media coverage. Finally, because we used a Web-based collection method, it is possible that non-Web responses by mailed survey or telephone call would result in a different pattern of findings.

- Self-reported results: The quality of survey research is based on the integrity of confidential responses received from subjects. While certain checks and balances can be incorporated into the survey process, there is always the possibility that a subject did not provide accurate responses.

Appendix: Detailed Survey Results

The following tables provide the frequency or percentage frequency of responses to all survey questions contained in this study. All survey responses were captured in November 2017.

Survey response	2017	2016
Total sampling frame	6,800	7,800
Total returns	279	299
Rejected or screened surveys	44	45
Final sample	235	254
Response rate	3.5%	3.3%

Part 1. Screening

S1. What best describes your organisational role or area of focus?	2017	2016
IT security operations	28%	22%
IT operations	52%	56%
CSIRT team	14%	16%
Business continuity management	6%	6%
None of the above (stop)	0%	0%
Total	100%	100%

S2. Please check all the activities that you see as part of your job or role.	2017	2016
Managing budgets	55%	46%
Evaluating vendors	53%	57%
Setting priorities	46%	43%
Securing systems	57%	61%
Ensuring compliance	45%	48%
Ensuring system availability	55%	47%
None of the above (stop)	0%	0%
Total	311%	302%

Part 2. Background Questions

Q1a. Did your organisation have a data breach involving the loss or theft of more than 1,000 records containing sensitive or confidential customer or business information in the past 2 years?	2017	2016
Yes	54%	49%
No	43%	48%
Unsure	3%	3%
Total	100%	100%

Q1b. If yes, how frequently did these incidents occur during the past 2 years?	2017	2016
Only once	44%	40%
2 to 3 times	38%	43%
4 to 5 times	12%	10%
More than 5 times	6%	7%
Total	100%	100%

Q1c. If yes, did any of these data breaches require notification?	2017
Yes	9%
No	85%
Unsure	6%
Total	100%

Q2a. Did your organisation have a cybersecurity incident that resulted in a significant disruption to your organisation's IT and business processes in the past 2 years?	2017
Yes	54%
No	42%
Unsure	4%
Total	100%

Q2b. If yes, how frequently did these incidents occur during the past 2 years?	2017
Only once	18%
2 to 3 times	21%
4 to 5 times	36%
More than 5 times	25%
Total	100%

Q3a. How has the volume of cybersecurity incidents changed in the past 12 months?	2017
Significantly increased	27%
Increased	35%
No increase	24%
Decreased	9%
Significantly decreased	5%
Total	100%

Q3b. How has the severity of security incidents changed in the past 12 months?	2017
Significantly increased	30%
Increased	35%
No increase	22%
Decreased	8%
Significantly decreased	6%
Total	100%

Q4. As a result of data breaches and cyber crime incidents, how frequently do disruptions to business processes or IT services occur as a result of cybersecurity breaches?	2017	2016
Very frequently	16%	15%
Frequently	27%	29%
Somewhat frequently	34%	30%
Rarely	20%	24%
Never	2%	2%
Total	100%	100%

Q5. Using the following 10-point scale, please rate your organisation's cyber resilience from 1 = low resilience to 10 = high resilience.	2017	2016
1 or 2	7%	8%
3 or 4	10%	19%
5 or 6	35%	46%
7 or 8	26%	20%
9 or 10	22%	7%
Total	100%	100%
Extrapolated value	6.43	6.43

Q6. Using the following 10-point scale, please rate your organisation's ability to **prevent** a cyber attack from 1 = low to 10 = high.	2017	2016
1 or 2	8%	10%
3 or 4	21%	20%
5 or 6	24%	33%
7 or 8	24%	25%
9 or 10	23%	12%
Total	100%	100%
Extrapolated value	6.14	6.14

Q7. Using the following 10-point scale, please rate your organisation's ability to quickly **detect** a cyber attack from 1 = low to 10 = high.	2017	2016
1 or 2	8%	9%
3 or 4	12%	11%
5 or 6	27%	30%
7 or 8	29%	31%
9 or 10	25%	19%
Total	100%	100%
Extrapolated value	6.53	6.53

Q8. Using the following 10-point scale, please rate your organisation's ability to **contain** a cyber attack from 1 = low to 10 = high.	2017	2016
1 or 2	3%	4%
3 or 4	21%	19%
5 or 6	26%	22%
7 or 8	32%	41%
9 or 10	18%	14%
Total	100%	100%
Extrapolated value	6.30	6.30

Q9. Using the following 10-point scale, please rate your organisation's ability to **respond** to a cyber attack from 1 = low to 10 = high.	2017
1 or 2	3%
3 or 4	20%
5 or 6	25%
7 or 8	26%
9 or 10	26%
Total	100%
Extrapolated value	6.49

Q10. Please rate the value of cyber resilience to your organisation from 1 = low to 10 = high.	2017	2016
1 or 2	7%	7%
3 or 4	9%	13%
5 or 6	11%	32%
7 or 8	31%	27%
9 or 10	42%	21%
Total	100%	100%
Extrapolated value	7.37	7.37

Q11. Using the following 10-point scale, please rate the importance of having skilled cybersecurity professionals in your cyber security incident response plan (CSIRP) from 1 = low to 10 = high.	2017	2016
1 or 2	2%	2%
3 or 4	8%	7%
5 or 6	17%	16%
7 or 8	37%	38%
9 or 10	36%	37%
Total	100%	100%
Extrapolated value	7.46	7.46

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	7%
5 or 6	16%
7 or 8	43%
9 or 10	31%
Total	100%
Extrapolated value	7.31

Q13. Using the following 10-point scale, please rate your organisation's ability to comply with the EU General Data Protection Regulation from 1 = low to 10 = high.	2017	2016
1 or 2	13%	16%
3 or 4	30%	28%
5 or 6	39%	39%
7 or 8	12%	11%
9 or 10	7%	6%
Total	100%	100%
Extrapolated value	4.89	4.89

Q14. Following are 7 factors considered important in achieving a high level of cyber resilience. Please rank order each factor from 1 = most important to 7 = least important.	2017	2016
Agility	2.9	2.4
Preparedness	1.9	2.0
Planned redundancies	4.6	5.1
Strong security posture	2.4	2.8
Knowledgeable or expert staff	3.8	4.1
Ample resources	5.2	5.0
Leadership	4.7	4.8

Q15a. How has your organisation's cyber resilience changed in the past 12 months?	2017	2016
Significantly improved	18%	9%
Improved	28%	18%
Somewhat improved	21%	23%
Declined	2%	2%
No improvement	31%	48%
Total	100%	100%

Q15b. If your organisation 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	42%
Elimination of silo and turf issues	41%
Visibility into applications and data assets	57%
Improved information governance practices	59%
C-level buy-in and support for the cybersecurity function	20%
Board-level reporting on the organisation's cyber resilience	15%
Training and certification for IT security staff	30%
Training for end-users	32%
Hiring skilled personnel	68%
Engaging a managed security services provider	35%
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	21%
Time has increased	32%
Time has remained unchanged	37%
Time has decreased	7%
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	62%
Silo and turf issues	22%
Lack of visibility into applications and data assets	40%
Lack of information governance practices	23%
Lack of C-level buy-in and support for the cybersecurity function	16%
Lack of board-level reporting on the organisation's state of cyber resilience	19%
Lack of training and certification for IT security staff	28%
Lack of training for end-users	38%
Inability to hire and retain skilled personnel	51%
Total	300%

18a. Please check one statement that best describes your organisation's cyber security incident response plan (CSIRP).	2017	2016
We have a CSIRP that is applied consistently across the entire enterprise	24%	23%
We have a CSIRP, but is not applied consistently across the enterprise	30%	30%
Our CSIRP is informal or "ad hoc"	24%	25%
We don't have a CSIRP	22%	22%
Total	99%	100%

Q18b. If you have a CSIRP, how often is it reviewed and tested?	2017	2016
Each quarter	5%	7%
Twice per year	8%	8%
Once each year	35%	34%
No set time period for reviewing and updating the plan	44%	35%
We have not reviewed or updated since the plan was put in place	8%	16%
Total	100%	100%

Q19a. Does your organisation participate in an initiative or program for sharing information with government and industry peers about data breaches and incident response?	2017	2016
Yes	48%	53%
No	52%	47%
Total	100%	100%

Q19b. If your organisation shares information about its data breach experience and incident response plans, what are the main reasons? Please select only three choices.	2017	2016
Improves the security posture of my organisation	75%	78%
Improves the effectiveness of our incident response plan	65%	73%
Enhances the timeliness of incident response	60%	55%
Reduces the cost of detecting and preventing data breaches	63%	52%
Fosters collaboration among peers and industry groups	28%	35%
Other (please specify)	9%	7%
Total	301%	300%

Q19c. If no, why does your organisation not participate in a threat-sharing program? Please select only two choices.	2017	2016
Cost	25%	23%
Potential liability of sharing	3%	3%
Risk of the exposure of sensitive and confidential information	29%	26%
Anti-competitive concerns	17%	15%
Lack of resources	38%	38%
Lack of incentives	27%	32%
No perceived benefit to my organisation	44%	38%
Do not know about options to share intelligence	10%	17%
Other (please specify)	8%	8%
Total	200%	200%

Q20. If yes, which of the following security technologies have been the most effective in helping your organisation become cyber resilient. Please select your top seven choices.	2017	2016
Web application firewalls (WAF)	14%	14%
Incident response platform	52%	57%
Next generation firewalls	10%	10%
Security information & event management (SIEM)	54%	48%
Cloud SIEM	29%	28%
Anti-virus / anti-malware	50%	49%
Intrusion detection & prevention systems	56%	55%
Network traffic surveillance	40%	54%
Identity management & authentication	87%	80%
Code review and debugging systems	24%	22%
Wireless security solutions	2%	2%
Data tokenisation technology	9%	9%
Encryption for data in motion	32%	27%
Encryption for data at rest	44%	47%
Data loss prevention (DLP)	45%	44%
Virtual private networks (VPN)	25%	23%
Big data analytics for cybersecurity	34%	36%
DDoS solutions	14%	18%
Endpoint security solution	25%	24%
Governance solutions (GRC)	19%	17%
User Behavioral Analytics (UBA)	32%	33%
Other (please specify	5%	3%
Total	700%	700%

Strongly Agree and Agree response: Please express your opinion about each one of the following statements using the agreement scale.	2017	2016
Q21a. My organisation's leaders recognise that enterprise risks affect cyber resilience.	53%	48%
Q21b. My organisation's leaders recognise that cyber resilience affects revenues.	57%	47%
Q21c. My organisation's leaders recognise that cyber resilience affects brand and reputation.	50%	45%
Q21d. In my organisation, funding for IT security is sufficient to achieve a high level of cyber resilience	39%	33%
Q21e. In my organisation, staffing for IT security is sufficient to achieve a high level of cyber resilience	26%	33%
Q21f. My organisation's leaders recognise that automation, machine learning, artificial intelligence and orchestration strengthens our cyber resilience.	53%	

Q22. Who has overall responsibility for directing your organisation's efforts to ensure a high level of cyber resilience? Please check one choice only.	2017	2016
Business continuity manager	9%	9%
Business unit leader	25%	24%
Chief executive officer (CEO)	6%	6%
Chief information officer (CIO)	27%	25%
Chief technology officer (CTO)	5%	6%
Chief risk officer (CRO)	7%	8%
Chief information security officer (CISO)	13%	13%
No one person has overall responsibility	9%	9%
Other (please specify)	0%	0%
Total	100%	100%

Q23a. What is the full-time equivalent (FTE) headcount of your IT security function today?	2017
Less than 5	10%
5 to 10	22%
11 to 20	22%
21 to 30	11%
31 to 40	21%
41 to 50	6%
51 to 100	8%
More than 100	0%
Total	100%
Extrapolated value	24.2

Q23b. What should the full-time equivalent (FTE) headcount be to achieve cyber resilience?	2017
Less than 5	2%
5 to 10	5%
11 to 20	17%
21 to 30	21%
31 to 40	14%
41 to 50	25%
51 to 100	11%
More than 100	5%
Total	100%
Extrapolated value	38.4

Q24. How long has your organisation'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	25%
1 to 3 years	25%
4 to 6 years	17%
7 to 10 years	8%
More than 10 years	2%
Total	100%

Q25. What best describes the maturity level of your organisation'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	31%
Late-middle stage – many cybersecurity program activities are deployed across the enterprise	31%
Mature stage – Core cybersecurity program activities are deployed, maintained and/or refined across the enterprise	23%
Total	100%

Q28. What factors justify the funding of your organisation's IT security? Please select your top two choices.	2017	2016
System or application downtime	55%	60%
Information loss or theft	46%	43%
Performance degradation	8%	8%
Productivity loss	12%	9%
Revenue decline	9%	8%
Reputation damage	18%	22%
Customer defection	12%	7%
Compliance/regulatory failure	40%	42%
Other (please specify)	1%	1%
Total	200%	200%

Q29. Approximately, what is the dollar range that best describes your organisation's current **cyber security budget**?	2017	2016
< $1 million	21%	10%
$1 to 5 million	28%	24%
$6 to $10 million	32%	42%
$11 to $15 million	17%	23%
$16 to $20 million	2%	0%
$21 to $25 million	0%	1%
$26 to $50 million	0%	0%
> $50 million	0%	0%
Total	100%	100%
Extrapolated value ($millions)	6.2	7.39

Q30. Approximately, what percentage of the current **cyber security budget** will go to cyber resilience-related activities?	2017	2016
< 2%	0%	0%
2% to 5%	4%	3%
6% to 10%	8%	4%
11% to 20%	15%	18%
21% to 30%	45%	40%
31% to 40%	19%	19%
41% to 50%	7%	8%
51% to 60%	3%	3%
61% to 70%	0%	5%
71% to 80%	0%	0%
81% to 90%	0%	0%
91 to 100%	0%	0%
Total	100%	100%
Extrapolated value (percentage)	25%	28%

Q31. The following table lists five areas of a CSIRP in your organisation. Please allocate 100 points to denote the level of investment in each area.	2017	2016
Prevention	38	42
Detection	32	29
Containment	13	16
Remediation	10	9
Post incident response	7	4
Total	100	100

Organisational and respondent characteristics

D1. What best describes the position level within the organisation?	2017	2016
C-level executive	5%	4%
Executive/VP	5%	5%
Director	15%	15%
Manager	19%	21%
Supervisor	16%	14%
Staff/technician	32%	32%
Administrative	6%	6%
Consultant/contractor	1%	1%
Other (please specify)	2%	2%
Total	100%	100%

D2. What best describes your reporting channel or chain of command?	2017	2016
CEO/executive committee	3%	3%
COO or head of operations	2%	2%
CFO, controller or head of finance	6%	5%
CIO or head of corporate IT	57%	56%
Business unit leader or general manager	14%	12%
Head of compliance or internal audit	0%	2%
Head of enterprise risk management	5%	5%
Head of IT security	14%	13%
Other (please specify)	0%	2%
Total	100%	100%

D3. What best describes your organisation's primary industry classification?	2017	2016
Agriculture & food services	3%	3%
Communications	5%	5%
Consumer products	5%	6%
Defense & aerospace	0%	0%
Education & research	2%	2%
Energy & utilities	6%	6%
Entertainment & media	3%	3%
Financial services	16%	19%
Health & pharmaceutical	9%	9%
Hospitality	5%	5%
Industrial	8%	10%
IT & technology	7%	4%
Logistics & distribution	1%	1%
Manufacturing	5%	5%
Public sector	11%	8%
Retailing	5%	5%
Services	7%	6%
Transportation	3%	3%
Total	100%	100%

D4. What range best describes the full-time headcount of your global organisation?	2017	2016
Less than 500	23%	22%
500 to 1,000	22%	27%
1,001 to 5,000	28%	21%
5,001 to 10,000	13%	13%
10,001 to 25,000	13%	11%
25,001 to 75,000	1%	6%
More than 75,000	0%	0%
Total	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 organisations.

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.