Australian Government

Australian Cyber Security Centre

ACSC

AUSTRALIAN CYBER SECURITY CENTRE

2016

CYBER SECURITY SURVEY

Use of the Coat of Arms

Contact us

Enquiries regarding the licence and any use of this document are welcome at:

Attorney-General's Department
Robert Garran Offices
3–5 National Cct
BARTON ACT 2600

Email: copyright@ag.gov.au

ISBN:

978-1-920838-05-8 (Print)

978-1-920838-06-5 (Online)

Contents

Introduction

This is the first Australian Cyber Security Centre (ACSC) Cyber Security Survey to look across both the government and private sectors in combination. It provides an overview of how prepared Australian organisations are to meet the growing cyber threat.

This report should be viewed as a companion to the ACSC 2016 Threat Report. Both reports reflect the experience, focus, and mandates of the ACSC's member organisations. But while the 2016 Threat Report provides an insight into what the Centre has been seeing, learning, and responding to, the aim of this survey is to gain an understanding of how ready Australian organisations are to prevent and respond to cyber threats.

Although modest in number, the survey sample reflects some of Australia's most significant systems of national interest — whether owned or operated by the government or private sector. A compromise of these systems could result in significant impacts on Australia's economic prosperity, social wellbeing, national defence and security.

The cyber threat remains ever-present. Most organisations (90%) faced some form of attempted or successful cyber security compromise during the 2015-16 financial year. Organisations faced numerous malicious cyber threats on a daily basis — through spear phishing emails alone, organisations are affected up to hundreds of times a day.

These figures reinforce the message to all organisations that experiencing a cyber incident is not a matter of if but when, and what type.

When weighing investment in cyber security against other business needs, senior management need to consider the overall level of cyber risk, their organisation's exposure to such risks, and the potential whole-of-business cost that could be incurred if a serious cyber incident were to occur on their network. The costs of compromise are almost certainly more expensive than preventative measures.

Executive summary

The cyber threat remains ever-present. Most organisations (90%) faced some form of attempted or successful cyber security compromise during the 2015-16 financial year. Organisations faced numerous malicious cyber threats on a daily basis — through spear phishing emails alone, organisations are affected up to hundreds of times a day.

This survey found that, in total, 86% of organisations surveyed experienced attempts to compromise the confidentiality, integrity or availability of their network data or system. Just over half (58%) experienced at least one incident that successfully compromised data and/or systems.

Findings suggest that the current level of cyber threat activity is disruptive for organisations regardless of whether an attempt to compromise a network is successful or not. Sixty percent (60%) of organisations surveyed experienced tangible impacts on their business due to attempted or successful compromises.

The fact that most organisations rated these incidents as relatively low in severity, but can still point to real business impacts as a result, should give pause for thought.

The survey also demonstrates that cyber resilience is a whole-of-business concern, and that an organisation's ability to deal with a cyber incident is reliant on a variety of factors — not just the technical controls that are in place. Cyber resilience refers to an organisation's ability to prepare for, withstand and recover from cyber threats and incidents.

> …the majority of organisations surveyed displayed a high level of resilience...

The good news is that the majority of organisations surveyed displayed a high level of resilience — as would be expected from the types of businesses and agencies that were surveyed and are partners of the ACSC.

Despite the overall resilience, there are still a number of significant challenges that suggest organisations could do more to prepare for and adapt to continually changing cyber threats. Just over half (51%) of all organisations surveyed said they tend to be alerted to possible breaches by external parties before they detect it themselves.

Given that only 2% of organisations reported having completely outsourced IT functions, these figures suggest organisations are not adequately focusing on monitoring networks and detecting potentially malicious activity.

Organisations were asked about their security posture, including all the technical and non-technical policies, procedures and controls that enable it to be protected against cyber threats. Most reported having a range of these cyber security controls in place but, unsurprisingly, organisations that are less resilient attitudinally are also less likely to have the listed cyber security controls in place.

Gaps are also evident where organisational attitudes or exposure to risk may be out of step with the technical controls in place. For example, organisations have embraced practices that offer greater workplace flexibility, such as using personal devices at work or working remotely from home; yet significantly fewer of these organisations have mobile device management systems or identity and access management systems in place to manage these risks. Further, only 56% of organisations surveyed have a process in place to identify critical systems and data.

Despite these gaps there have been improvements. For example, 71% of organisations report having a cyber security incident response plan in place compared with 60% in the 2015 ACSC Cyber Security Survey of Major Australian Businesses.

> ...71% of organisations report having a cyber security incident response plan in place... ”

Now the focus needs to be on ensuring those plans remain relevant. Of all organisations that have incident response plans, less than half (46%) regularly review and exercise these plans. Fifteen percent (15%) either never test the plan, or test it on an ad hoc basis, with 24% testing less than once a year. As the threat environment continually evolves — with new software, tools, technologies and techniques constantly released — these plans must be regularly reviewed and updated in order to remain effective.

Finally, the ACSC has a clear and important role to play providing impartial information, guidance and support to both private sector and government organisations.

While government organisations were more likely to seek this type of assistance from government sources (80%), more than half of private sector organisations surveyed (56%) also accessed government sources for cyber security information, advice or guidance. The ACSC and its agencies were the primary source of such information.

In recognition of the leading role the ACSC plays in providing guidance, more needs to be done to raise the value of reporting both attempted and successful incidents. As noted in the 2016 Threat Report, reports help the ACSC develop a better understanding of the threat environment to better assist other organisations who are also at risk. This knowledge also enables the government to develop appropriate cyber security advice, incident response assistance, mitigation strategies, training measures and policies.

About the Australian Cyber Security Centre

The ACSC co-locates key operational elements of the Government's cyber security capabilities in one facility to enable a more complete understanding of sophisticated cyber threats, facilitate faster and more effective responses to significant cyber incidents, and foster better interaction between government and industry partners. We work with government and business to reduce the security risk to Australia's government networks, systems of national interest, and targets of cybercrime where there is a significant impact to security or prosperity.

The ACSC is the focal point for the cyber security efforts of the Australian Signals Directorate (ASD), the Defence Intelligence Organisation (DIO), the Australian Security Intelligence Organisation (ASIO), the Computer Emergency Response Team (CERT) Australia, the Australian Criminal Intelligence Commission (ACIC), and the Australian Federal Police (AFP).

ASD is the Commonwealth authority for cyber and information security and provides advice and assistance to Commonwealth and State authorities on matters relating to the security and integrity of information that is processed, stored or communicated by electronic or similar means. ASD undertakes its cyber and information security mandate from within the ACSC and is the lead for the operational management of the Centre through the position of Coordinator ACSC. In addition, ASD carries out an intelligence mission in support of its cyber and information security mandate.

DIO leads the ACSC's Cyber Threat Assessment team — jointly staffed with ASD — to provide the Australian Government with an all-source, strategic, cyber threat intelligence assessment capability.

ASIO's role is to protect the nation and its interests from threats to security through intelligence collection, assessment, and advice for Government, government agencies, and business. ASIO's cyber program is focused on investigating and assessing the threat to Australia from malicious state-sponsored cyber activity. ASIO's contribution to the ACSC includes intelligence collection, investigations and intelligence-led outreach to business and government partners.

CERT Australia is the Government contact point for cyber security issues affecting major Australian businesses including owners and operators of Australia's critical infrastructure and other systems of national interest. CERT Australia helps these organisations understand the cyber threat landscape and better prepare for, defend against, and mitigate cyber threats and incidents through the provision of advice and support on cyber threats and vulnerabilities.

The **ACIC** provides the Australian Government's cybercrime intelligence function within the ACSC. Its role in the Centre is to discover and prioritise cybercrime threats to Australia, understand the criminal networks behind them and initiate and enhance response strategies by working closely with law enforcement, intelligence and industry security partners in Australia and internationally.

The **AFP** is the Australian Government's primary policing agency responsible for combating serious and organised crime and protecting Commonwealth interests from criminal activity in Australia and overseas. The AFP's Cybercrime Investigation teams within the ACSC provide the AFP with the capability to undertake targeted intelligence and to investigate and refer matters for prosecution for those believed to have committed cybercrimes of national significance. The AFP is also the ACSC's conduit for State and Territory law enforcement.

The ACSC’s key areas of collaboration are:

- triaging and responding to significant cyber security incidents affecting national security or economic prosperity;
- identifying, analysing, and conducting research into sophisticated malicious cyber activity targeting Australia;
- creating shared situational awareness of the cyber threat by developing alerts, warning and mitigation advice, and producing intelligence;
- working closely with government organisations, critical infrastructure owners and operators, and key industry partners and sectors to reduce security risk and limit the threat to Australia’s most important networks and systems; and
- developing relationships with key international partners.

For more information about the ACSC, visit https://www.acsc.gov.au. To provide feedback or otherwise contact the ACSC about this report, please contact 1300 CYBER1 or use other details available at: https://www.acsc.gov.au/contact.htm

About this survey

Survey objectives and methodology

The Australian Cyber Security Centre (ACSC) 2016 Cyber Security Survey explores the cyber security attitudes, needs and experiences of major organisations in the Australian government and business sectors. The results are intended to assist the Australian government and private sector organisations to understand how well positioned they are to defend themselves against cyber security threats.

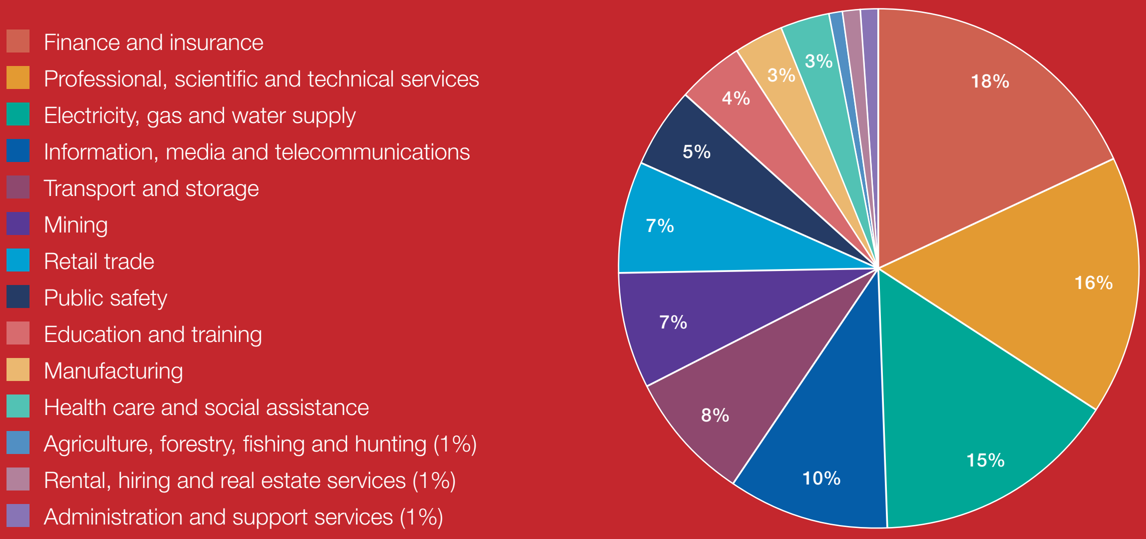
- The survey was conducted online among organisations that are currently partners of ACSC and its agencies. Partner organisations include government departments and agencies, and major Australian businesses.
- The survey was developed in consultation with ACSC agencies, tested among a small sample of partner organisations and approved for use by the Statistical Clearing House in the Australian Bureau of Statistics.
- Fieldwork was conducted from 31 October to 26 November 2016.

- The survey was designed to be completed by someone with decision making responsibilities regarding cyber security and IT management in the organisation.
- 113 organisations completed the survey in 2016, including 68 private sector and 45 government organisations.
- Although the respondent sample is modest, the sample reflects some of Australia’s most significant systems of national interest.
- Unless otherwise noted, all results presented in this report are given as a proportion of the total sample of 113 organisations.

Participant profile

The characteristics of surveyed organisations

Figure 1: Industry sector – not including government



Organisation type

Private sector (including privately and publicly owned, not-for-profit and mutual organisations	60%
Government	40%

Organisation size

Small/medium <200 employees	27%
Large 200+ employees	43%

Respondent role

Chief Information Security Officer (CISO)	35%
Chief Information Officer	20%
Information Security Manager / Information Security Officer	9%
IT Manager	5%
Chief Executive Officer (CEO) / Managing Director (MD)	4%
Other Executive / Director	4%

As well as looking at the basic characteristics of the organisation — such as size or sector — from a security perspective it is also revealing to consider the respondents according to their exposure to risk and IT management.

Exposure to risk

The majority of surveyed organisations are exposed to cyber security risks through international connectivity and online operations. More than half of organisations surveyed (54%) have a physical presence in both Australia and overseas, operating in multiple locations.

Almost nine in ten (87%) interact directly with overseas organisations and 50% of these share networks, systems or data storage with these overseas organisations. The majority of organisations also use a variety of online facilities, most commonly including employee and company email addresses (99%), staff that work remotely (97%), and websites and online blogs (93%).

The normalisation of Bring Your Own Device (BYOD) solutions is clear, with close to three quarters of organisations surveyed (73%) allowing employees to use personal devices for business reasons.

IT management

Over half (55%) of surveyed organisations outsource elements of their IT function, though only 2% have a completely outsourced IT capability.

Organisations surveyed most commonly had no more than five people specifically responsible for IT security within their IT function. Only 5% of organisations with internal IT staff had no staff specifically responsible for IT security, compared to 31% for organisations with externally managed IT. This difference is of particular concern considering the information security risks associated with outsourcing IT management.

The IT function is based in Australia for 71% of organisations surveyed, while 28% of organisations have elements of their IT function located in Australia as well as overseas.

Cloud computing security considerations

For advice on securing a range of cloud services for both tenants and service providers, visit:

https://www.asd.gov.au/infosec/cloudsecurity.htm

Physical presence

An Australian organisation with physical presence in just one location	16%
An Australian organisation with physical presence in multiple locations, in Australia only	30%
An Australian organisation with physical presence in multiple locations, including overseas	36%
An overseas-based organisation with physical presence in just one location in Australia	0%
An overseas-based organisation with physical presence in multiple locations in Australia	18%

Base: Businesses only (68)

Overseas physical presence

New Zealand	50%
China	46%
USA	38%
Singapore	35%
Indonesia	35%
UK	31%
India	27%

Base: Businesses only (68)

Interaction with overseas organisations

Interact directly with other organisations based overseas	87%
Of these, have shared networks, systems or data storage with the overseas organisation	50%

Base: All respondents (113)

Relevant characteristics

Email addresses	99%
Remote staff	97%
Websites / online blogs	93%
Externally hosted web services	85%
Social media accounts	84%
Personal devices used for business	73%
Online business banking	65%
Online customer ordering / payments	53%
Industrial control system	44%

Base: All respondents (113)

Staff responsible for IT security

	Internal	Outsourced
No staff members specifically responsible	5%	31%
1–5 staff members	69%	36%
6–14 staff members	15%	14%
15+ staff members	10%	13%
Don't know	1%	6%

Base: All respondents (113)

Resilience

To measure resilience, survey respondents were asked to characterise their organisation based on a range of factors that can be taken as potential indicators of cyber resilience. These factors were presented as pairs, with one statement in the pair describing a more cyber-resilient attitude or practice, and the other statement describing a less cyber-resilient attitude or practice. Information on what makes organisations more cyber resilient is discussed in the next section.

Participants were asked to select the statement from the pair best describing their organisation. Each organisation received a score from 7 to 14 based on the statements they selected. For the purposes of analysis against other items in the survey, those scoring 12 or above were classified as more resilient organisations. Those scoring less than 12 were classified as less resilient organisations.

The average score across the sample was 12, indicating that most of the organisations surveyed displayed a high level of resilience.

Organisational attitudes and resilience

Exploring indicators of cyber security maturity

Cyber resilience refers to an organisation's ability to prepare for, withstand and recover from cyber threats and incidents, regardless of whether such occurrences are deliberate, accidental, or naturally occurring.

The ACSC's 2016 Threat Report observes that relatively few organisations that have reported experiencing significant cyber security incidents had sufficiently planned or prepared for such an event.

Beyond having the necessary technical controls in place, organisations that are cyber resilient have an appropriate appreciation of the risks and threats facing them and are motivated and well prepared to respond with an approach that encompasses people, processes and technology.

The good news is that most organisations surveyed (70%) displayed a high level of resilience — falling into the more cyber-resilient category.

Despite a high level of resilience overall, there are still a number of significant challenges that suggest organisations are not as well prepared as they could be.

> …there are still a number of significant challenges that suggest organisations are not as well prepared as they could be. ”

A high proportion (43%) of organisations indicated they tend not to identify cyber security threats or vulnerabilities until after they have manifested into a compromise. Further, just over half (51%) of all organisations surveyed said they tend to be alerted to possible breaches by external parties before they notice it themselves.

Given that only 2% of organisations reported having a completely outsourced IT function, these figures suggest organisations are not adequately monitoring networks and systems and detecting potentially malicious activity.

Findings suggest that some organisations are also failing to adequately measure or consider the impact of incidents. Nearly one in ten (9%) of the organisations characterised as less resilient did not know the impact of cyber security incidents on their organisation — compared to just 1% of more resilient organisations.

What does a cyber-resilient organisation look like?

A number of attitudes and practices clearly differentiate organisations with a more resilient cyber security posture from those with a less resilient posture.

More cyber-resilient organisations:

- Maintain good situational awareness by regularly seeking external information, advice or guidance on cyber security.
- Approach cyber security from a risk-reduction rather than compliance mindset, considering information security alongside other business risks.
- Have a strong security culture across the whole organisation and understand that everyone shares responsibility for cyber security, not just the IT department.
- Discuss cyber security at board level and with senior management, with regular updates on the agenda.
- Proactively identify and head off threats before they are successful.
- Share information with trusted networks and alert other organisations to possible breaches of their own security.

Board-level consideration of cyber security

One of the key factors that distinguish more cyber-resilient organisations from less resilient ones is that cyber security is regularly discussed at the most senior board or management level.

Although eight in ten (81%) of organisations surveyed recognise all staff have responsibility for ensuring cyber security, and, overall, seven in ten (73%) regularly discussed cyber security at the most senior management levels, the figures tell a different story when we look at these results through the lens of resilience.

> …cyber-resilient respondents were far more likely to have discussed cyber security at the board level within the last three months…

More cyber-resilient respondents were far more likely to have discussed cyber security at the board level within the last three months (87%) compared with those categorised as less resilient (59%).

The context of senior level discussions is also important. Overall the most common reason for the most recent discussion of cyber security at board level was a regular or scheduled cyber threat briefing (48%). A further 22% of discussions were briefings given at the request of the Board or senior management.

But differences again emerge when the results are compared for more and less cyber-resilient organisations.

Although just 11% of recent board-level discussions were prompted by an actual cyber security incident, overall, less resilient organisations were generally more likely than others to be reactively discussing cyber security. For example, 21% of recent discussions among less resilient organisations were prompted by an incident, compared with just 6% for more resilient organisations.

Regardless of resilience more needs to be done to embed cyber security into the core strategic business of senior management.

Overall one third (31%) of organisations indicated senior management is only updated on cyber security after incidents or breaches have occurred; and cyber security is rarely, if ever, discussed at the most senior level (27%).

These figures suggest that senior level decision makers are less likely to have an appreciation of the business risks associated with the cyber threat, and as a result may not view the potential impacts or level of risk as sufficient to warrant further investment in cyber security. This research suggests that involvement of senior management is seen as a leading factor in successfully mitigating cyber security risks. Ultimately, better understanding by senior decision makers of cyber security helps organisations respond to incidents more effectively. This is explored in further detail later in the report.

Six questions senior management need to be asking about ICT security

Make sure you are discussing the right questions with your ICT security team to review your organisation's information security.

https://www.asd.gov.au/publications/protect/senior_management_questions.htm

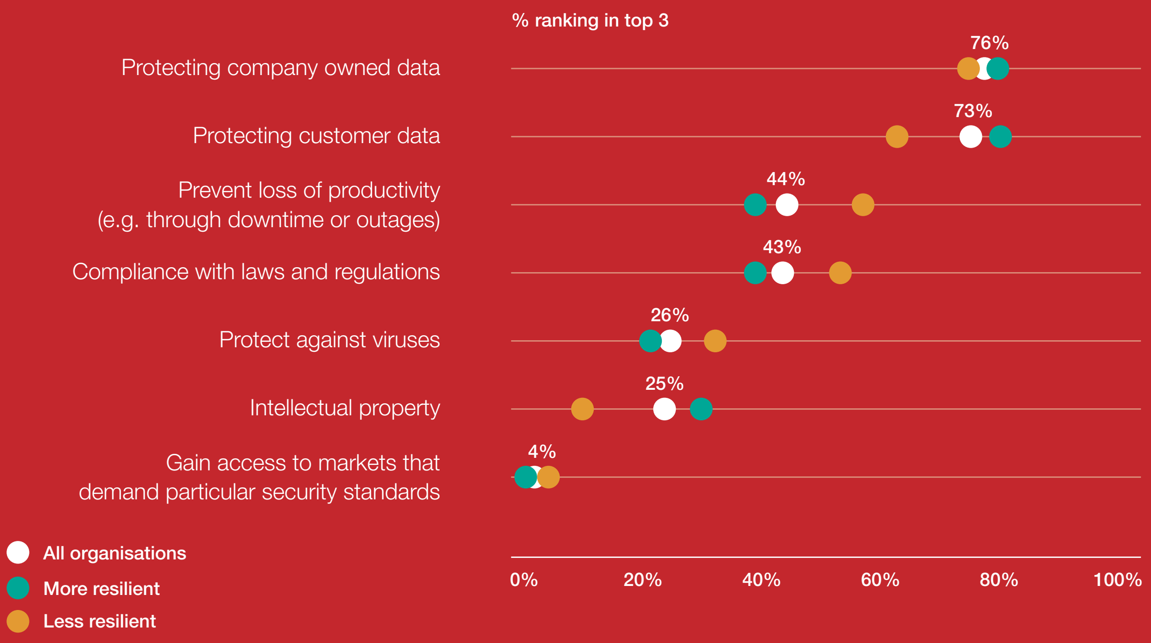
Investment in cyber security

Survey participants were asked to rank the importance of a range of factors in motivating their organisation to invest in cyber security. The proportion ranking each factor as one of their top three motivations is shown in Figure 2.

Organisations are primarily motivated by the need to safeguard company owned data (76%) and protect customer information (73%). This is unsurprising given most major organisations surveyed have responsibility for significant business operations and human resources data, proprietary information, and sensitive, classified or valuable client information. For some organisations, privacy legislation establishes a legal obligation to protect personally identifiable information.

Nine organisations specified motivations in their top three that were different from, or in addition to, those listed in the survey question. These included protecting brand reputation or integrity, protecting systems and critical infrastructure, and contractual obligations.

2 **Figure 2: Motivations for investing in cyber security**



Question: Q16. Please rank the following responses based on the importance to your organisation for investing in cyber security, with 1 being the most important and 7 being least important.

Base: All respondents (113). More resilient organisation (79). Less resilient (34).

When weighing investment in cyber security against other business needs, senior management needs to consider the overall level of cyber risk, their organisation's exposure to such risks, and the potential whole-of-business cost that could be incurred if a serious cyber incident were to occur on their network.

> The costs of compromise can be more expensive than prevention measures.

The costs of compromise can be more expensive than preventative measures. The challenge faced by organisations is getting this balance right.

Looking at the results in Figure 2, two further observations stand out. Firstly, less resilient organisations appear to place more emphasis on productivity, compliance and virus protection compared to more resilient organisations. This is to be expected as, being less resilient, they are more concerned about withstanding factors that have more immediate financial and legal consequences than those with longer term consequences, such as damage to reputation or intellectual property losses. More resilient organisations are likely to have multiple layers of cyber security controls in place, allowing them to focus investment on addressing other concerns. This is explored in greater depth in the following section.

Secondly, when comparing the motivations of all organisations with the cyber incidents they reported experiencing in 2015-16, the results suggest that organisations underestimate the risks posed by viruses.

Organisations may believe the range of controls they have in place adequately protects against threats from malware, and are no longer motivated by this problem. However, types of malware (including worms and viruses) are commonly used as initial vectors to compromise a network, and 42% of organisations surveyed were successfully compromised by malware infection, suggesting it is still an issue. Organisations must maintain protection against threats from malware on an ongoing basis. Not doing so places networks and data at risk.

Planning for and managing cyber security

What does the security posture of partner organisations look like?

The ACSC's 2016 Threat Report highlighted the importance of planning and preparation in relation to cyber security incidents. Effective management of an incident can greatly decrease the severity, scope, and amount of damage — and therefore cost — of a cyber security incident.

Cyber security controls

An organisation's cyber security posture includes all the technical and non-technical policies, procedures and controls that enable it to be protected against cyber threats. Ensuring the right controls are in place for the level of risk the organisation faces is key to cyber resilience.

Survey participants were asked to indicate which of a list of 20 controls their organisation has in place. These controls cover:

- **Planning** — including having a documented IT security or cyber security policy and an incident response plan.
- **People/resourcing** — including cyber security awareness training for staff, having a cyber security incident response team or capability and a security operations centre.
- **Systems** — including identity and access management system, data loss prevention system, intrusion detection or prevention system, security information and event management system and mobile device management system.
- **Processes** — including regular cyber security risk assessments, third party or vendor risk assessments, processes to identify critical systems and data, privileged account management processes, patch management processes, threat and vulnerability scanning and processes to receive regular cyber security threat intelligence.
- **Governance/reporting** — including regular cyber security risk reporting to senior management/the board and external certification to cyber security standards.

As shown in Figure 3, most organisations have a range of these cyber security controls in place, though no specific control has been adopted by more than 86% of all organisations surveyed.

No single mitigation strategy or control is guaranteed to prevent cyber security incidents, which is why ACSC agencies highlight the importance of having multiple layers of controls in place. The prioritisation of various controls and strategies to mitigate cyber threats can, and should, vary according to the context specific to each individual organisation.

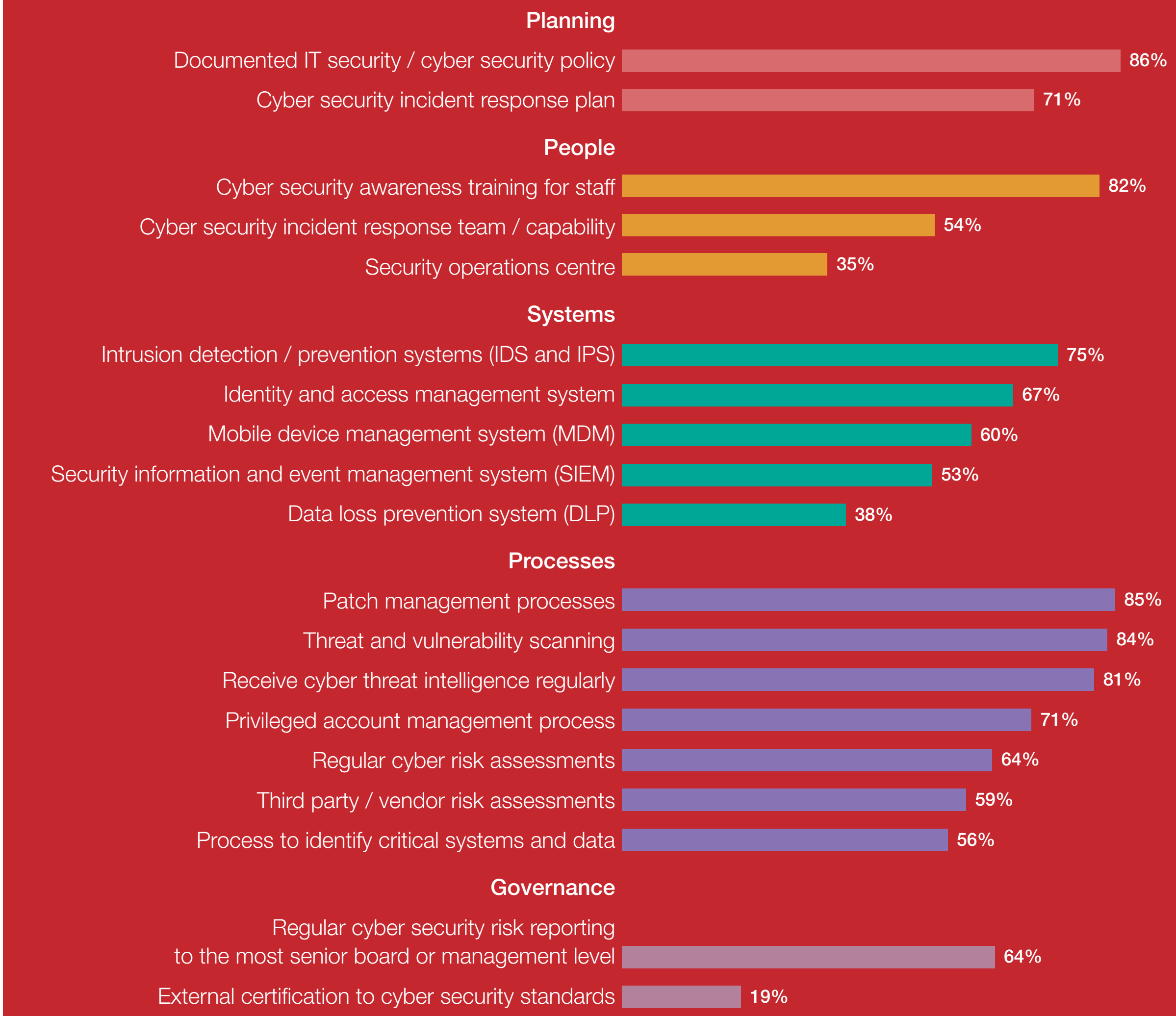
Before selecting which controls to implement, organisations need to understand the value of the data and information they hold, where it is on their network, how it is protected and who has access to it. This knowledge will inform the level of protection that is required and which controls to prioritise.

> …non-technical policies, procedures and human capabilities are as important as technical controls.

Organisations with a more mature security posture will have a solid baseline of protections in place along with other relevant strategies based on the risks to their business. They are more likely to understand that non-technical policies, procedures and human capabilities are as important as technical controls.

Figure 3 shows that organisations are less commonly adopting broader control systems such as data loss prevention systems (38%) and security information and event management systems (53%) or investing in specific cyber security resources (e.g. only 35% have a security operations centre and 54% have a cyber security response team or capability). Least commonly undertaken is external certification to cyber security standards, with only 19% indicating they have this in place.

3 **Figure 3: Cyber security controls in place**



Question: Q17. Which of the following does your organisation currently do or have in place?

Base: All respondents (113).

However, it is important to recognise that there is a large discrepancy in complexity and cost between the controls listed. For example, some options, such as setting up a dedicated security operations centre or gaining external certifications, may be prohibitively costly or disproportionate to the scale of organisation.

Comparing these responses with those from other questions in the survey reveals instances where organisational attitude or exposure to risk may be out of step with the actual controls in place.

In the previous section exploring investment in cyber security, organisations cited a desire to safeguard company owned data and protect customer information as the top factors motivating investment. However, only 56% of organisations report having a process in place to identify critical systems and data. This raises concerns that some of the remaining 44% may have systems and data that are insufficiently secured because they have not been identified as critical. It also highlights the gap between factors of concern and the controls organisations have in place to address such concerns.

Fewer organisations have device management and user access controls in place than allow their staff members to conduct business on personal devices or work remotely. For example, 73% have staff that use personal devices for business reasons, yet only 60% of organisations have a mobile device management system in place.

Similarly, the survey suggests organisations are exposed to unmitigated risks associated with outsourced IT services and systems or networks shared with overseas organisations through a lack of comprehensive checks and future planning.

Almost all (97%) of the surveyed organisations have remote-working staff, yet only 67% have an identity and access management system and only 71% have a privileged account management process.

Looking at the controls according to more or less ‘resilient’ attitudes towards cyber security reveals that organisations that are less resilient attitudinally are also less likely to have the listed cyber security controls in place.

Secure administration

For suggestions on implementing a secure administration environment, visit:

https://www.asd.gov.au/publications/protect/secure-administration.htm

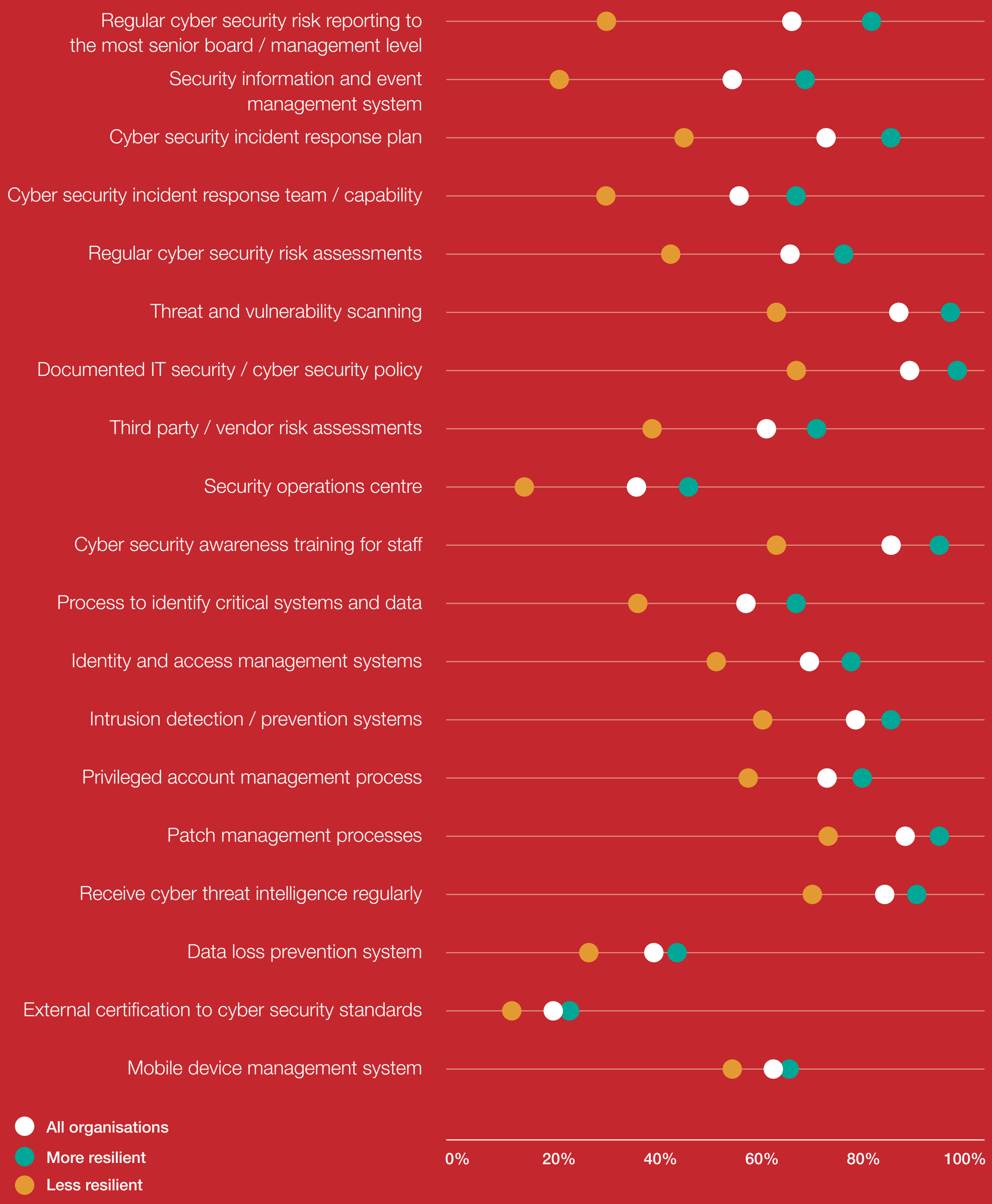
Figure 4 displays a breakdown of organisations displaying more or less resilient attitudes towards cyber security with each of the controls in place. The list of controls is ordered from the option with the largest discrepancy between the groups to the control with the smallest discrepancy. Breaking down responses in this way clearly shows how less resilient organisations have fewer controls in place. No more than 71% of these organisations have adopted any one of the controls, compared with up to 95% of those that are more resilient in attitude.

As previously discussed, this observation reflects that organisations with a more mature security posture will have a solid baseline of protections in place along with a range of other technical and non-technical strategies based on the risks to their business. On average, only four in ten (44%) less resilient organisations will have any of these controls in place.

Further, cyber security reporting at board or senior management level is the control far more likely to be adopted by more resilient organisations, followed by security information and event management systems (SIEMs) and cyber security incident response plans. This reflects a more mature cyber security posture and an understanding that factors such as governance and planning are as important to long-term cyber resilience as purely technical controls.

4

Figure 4: Cyber security controls by resilience level



Question: Q17. Which of the following does your organisation do or have in place?

Base: All respondents (113). More resilient organisation (79). Less resilient organisations (34).

Incident response plans

Having an up-to-date and regularly tested incident response plan is an important factor for effective management of a cyber incident. Results suggest this message is being received, with more organisations than ever putting such plans in place.

Among the organisations surveyed, 71% have a cyber security incident response plan in place compared with 60% in the 2015 ACSC Cyber Security Survey of Major Australian Businesses.

Despite the overall increase, there is still room for improvement.

Fewer than half (44%) of the organisations identified as less resilient have an incident response plan in place. Furthermore, of all organisations that have incident response plans, fewer than half (46%) regularly review and exercise these plans. Fifteen percent either never test it or test it on an ad hoc basis, less than once a year (24%).

As the threat environment continually evolves — with new software, tools, technologies and techniques constantly released — incident response plans must be regularly reviewed and updated in order to remain effective.

How do other organisations approach incident response plans?

Organisations were asked to indicate what their incident response plan covered.

- Guidelines for categorisation of events
- Plans for each major incident type and for different types of data being compromised
- Key tools (e.g. checklists or guides) for use during the response
- Processes for alerting necessary stakeholders, including:

  Board members and senior management

  Affiliates, suppliers or external agencies potentially affected by the incident

  Australian Cyber Security Centre agencies
- Arrangements to regularly review and exercise the plan

Importantly, plans need to consider whole-of-business operations and impacts.

Fewer than half (46%) of all organisations with a plan in place included media or communication response processes. This is concerning considering the need to communicate effectively with affected parties in the event of a compromise, and the real business impacts that can come with reputational damage and a loss of business.

More advice and information is available in the following publications:

Cyber Security Incidents — Are You Ready?
https://www.asd.gov.au/publications/protect/cyber-security-incidents-are-you-ready.htm

Preparing For and Responding to Cyber Security Incidents
https://www.asd.gov.au/publications/protect/preparing_for_cyber_incidents.htm

From top 4 to essential eight

Since 2009 the Australian Signals Directorate (ASD) has produced and regularly reviewed a prioritised list of practical actions organisations can take to make their computers, networks and systems more secure.

Originally known as the *Strategies to Mitigate Targeted Cyber Intrusions*, these mitigation strategies have changed over time to reflect and address cyber threats as they have evolved. In 2017 this guidance addresses targeted cyber intrusions, ransomware and external adversaries with destructive intent, malicious insiders, 'business email compromise' and industrial control systems.

Just as the number and type of strategies are reviewed and changed, so too is the package of top strategies that is prioritised by ASD. These top mitigation strategies, if implemented as a package, offer organisations a baseline that makes it much harder for adversaries to compromise systems.

ASD's easy to remember 'Catch, Patch, Match' Top 4 Mitigation Strategies were recommended to government and industry alike as a package that could address up to 85% of the intrusions responded to by ASD.

Now the Top 4 have evolved into the Essential Eight.

Application whitelisting (catch), patching applications and operating systems (patch) and restrict administrator privileges (match) are still there as top recommendations, but now they are joined by additional steps to prevent malware running, limit the extent of incidents and aid data recovery.

The essential eight

To prevent malware running:

- Application whitelisting
- Patch applications
- Disable untrusted Microsoft Office macros
- User application hardening

To limit the extent of incidents and recover data:

- Restrict administrative privileges
- Patch operating systems
- Multi-factor authentication
- Daily back-up of important data

For more information on the Essential Eight and other *Strategies to Mitigate Cyber Security Incidents* visit: https://www.asd.gov.au/publications/protect/essential-eight-explained.htm

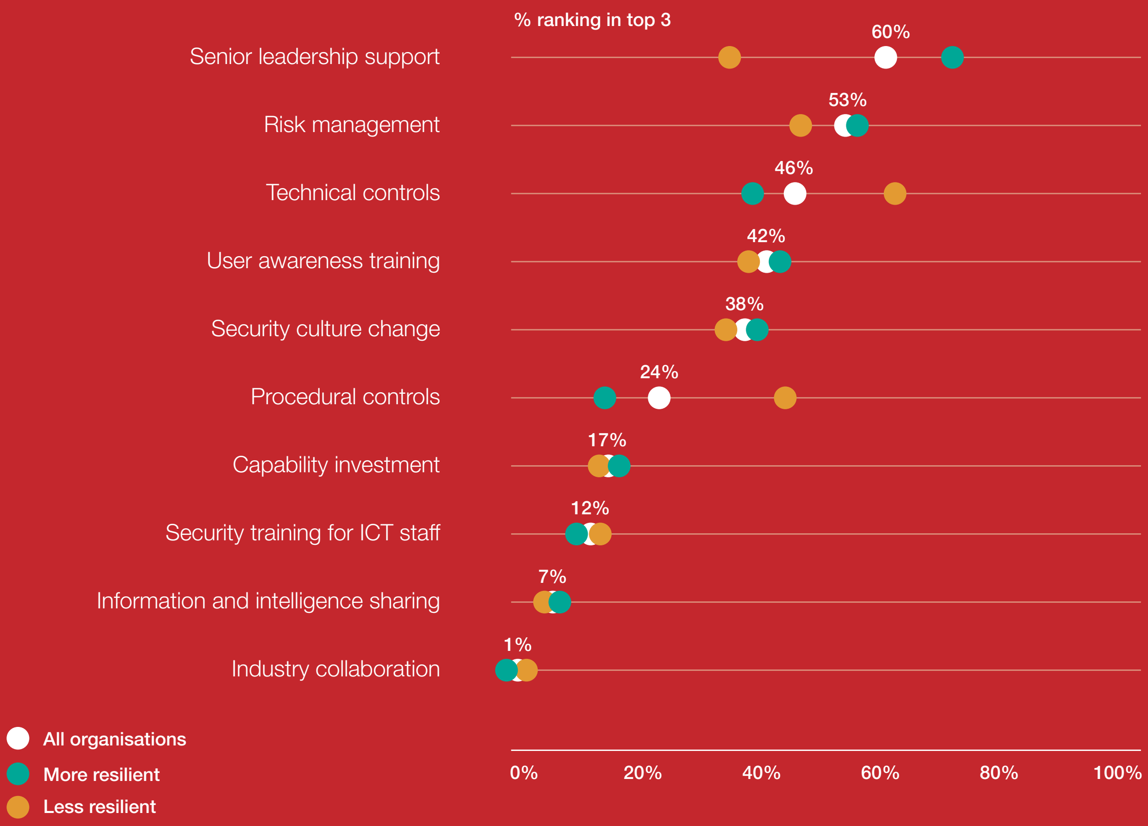
Mitigating cyber security risks

Surveyed organisations were asked to rank a range of factors in terms of their perceived importance to the organisation in mitigating cyber security risks. The results are shown in Figure 5, along with a comparison of the results for organisations that have a more and less resilient cyber security outlook.

Although senior leadership support is the leading factor overall (60%), there is a vastly divergent view of the importance of this factor according to whether an organisation has a more or less resilient attitude towards cyber security.

5

Figure 5: Important factors for mitigating cyber security risks



Question: Q21. Please rank the following responses in terms of their importance to your organisation in mitigating cyber security risks, with 1 being most important and 10 being least important.

Base: All respondents (113). More resilient organisations (79). Less resilient organisations (34).

> …cyber-resilient organisations see senior leadership support by far the most important factor...

More cyber-resilient organisations see senior leadership support as by far the most important factor, while it is the fifth most important factor for less resilient organisations.

A similar, though less pronounced, pattern is observed for risk management, which was the second most important factor in mitigating risk overall (53%). This relates back to the discussion on board-level consideration of cyber security in the section on 'Organisational attitudes and resilience'.

The results in this section reinforce that organisations that have regular, proactive discussions on cyber security at the most senior levels are more resilient and better prepared for cyber threats. Such regular discussions may result in greater buy-in regarding cyber security at senior levels, which may have flow-on effects regarding the prioritisation of investment decisions for cyber security, with a positive effect on the overall level of protection against cyber threats. Regular discussions are also likely to increase awareness of cyber risks at senior levels, fostering an understanding of cyber security as a whole-of-business concern.

More resilient organisations also take a 'defence-in-depth' approach to cyber security, implementing a range of technical and non-technical policies, procedures and controls that enable better protection against cyber threats in the long term.

As previously observed, more resilient organisations typically have a higher number and broader range of technical controls in place and are therefore able to focus on factors that build capability — such as senior leadership support, user awareness training and cultural change — rather than only those that are in response to an immediate concern. In contrast, less resilient organisations were far more likely to rank technical and procedural controls as the most important factors for mitigating cyber security risk.

> ...a 'defence-in-depth' approach to cyber security…enable better protection against cyber threats in the long term.

Interestingly, the factors organisations ranked as most important in mitigating risks were not always the most commonly adopted. For example, cyber security awareness training for staff and procedural controls, such as patching and vulnerability scanning, are widely adopted but ranked lower than other factors such as senior leadership support and risk management in terms of their importance to organisations.

Conversely, 81% of organisations surveyed identified that they regularly receive cyber threat intelligence; however, information or intelligence sharing and industry collaboration were viewed as being the least important factors in mitigating cyber security risks.

This lack of importance placed on information sharing and collaboration, together with security training for ICT staff, is cause for concern for two reasons.

Firstly, the need for sharing actionable and tactically useful indicators has long been understood. The recent move towards security automation and cyber threat intelligence can play a significant role by filtering out the noise created by unsophisticated and untargeted threats, providing insight to the evolution of sophisticated adversary tradecraft, and validating defensive security and response measures.

Secondly, sharing indicators of compromise along with indicators about the vulnerabilities, infrastructure, and tactics, techniques or procedures (TTPs) used by an adversary with other potential targets can increase the costs (time and money) and limit the effectiveness of malicious actors.

For these reasons ACSC agencies, led by CERT Australia, have been increasing their capabilities for sharing niche cyber threat intelligence with key partners across the country.

However, sharing sensitive information requires an existing relationship and degree of trust between parties. This means that organisations and governments need to invest in industry collaboration and building partnerships before an incident occurs, to ensure the foundations exist to facilitate information sharing when it is most needed.

Further, an organisation's ability to effectively utilise such threat intelligence and information relies not only on having the necessary technical tools in place; it also requires operational staff to have the knowledge and capability required to make sense of this data within the context of their own organisation.

Ongoing security training ensures the skills and capability of ICT staff keeps abreast of such developments. Cyber security professionals and network defenders must be as motivated, innovative and agile as malicious adversaries.

> Cyber security professionals and network defenders must be as motivated, innovative and agile as malicious adversaries. ”

Mitigating risks for networks and shared data

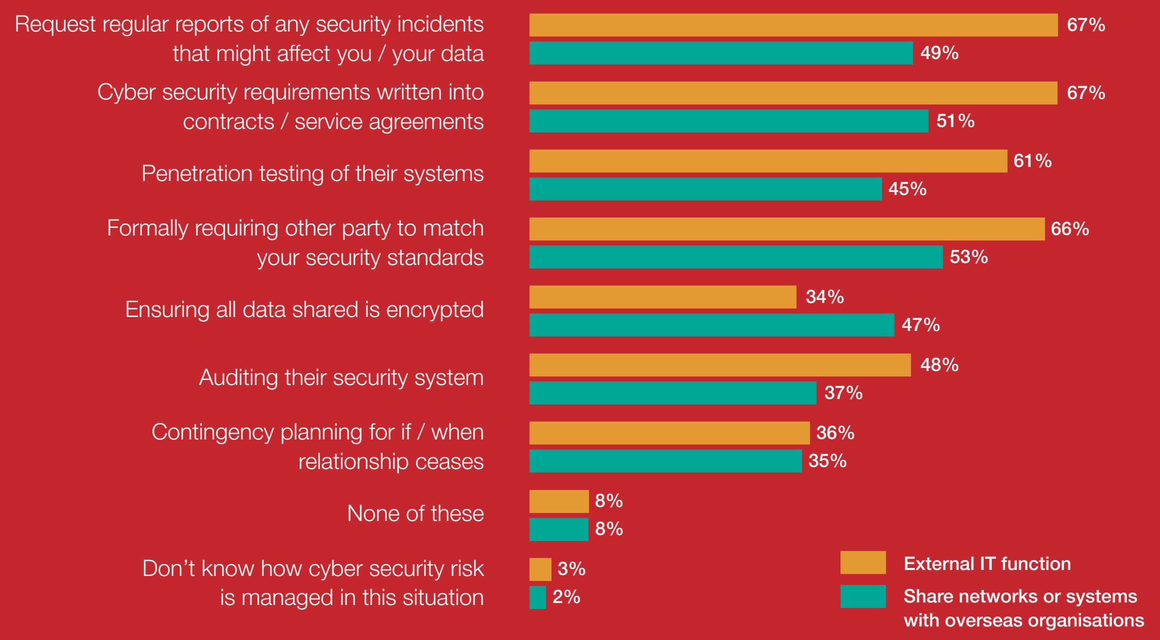
Cyber security risks to data and systems increase the more closely organisations interact with external parties. Of particular concern is the safety of data and networks shared with overseas organisations and the security of systems that are overseen by external IT providers. Not least among these risks is the potential for confidential or sensitive data to be maliciously intercepted or stolen.

Organisations that outsource any element of their IT function and those that share networks and systems with overseas organisations were asked to indicate the processes they use to mitigate the risks associated with these activities. The results are shown in Figure 6 for each activity.

Organisations are more likely to have arrangements in place for networks and shared data with external IT companies than with overseas-based organisations, presumably because the relationship with IT companies specifically focuses on the security of these systems.

Of concern is that only 34% of those organisations with an external IT function, and 47% of those that share networks and data with overseas organisations, ensure that all data shared between the two organisations is encrypted. Further, only around one third (35% and 36% respectively) of organisations have undertaken any contingency planning for if or when the relationship with these external organisations ceases. Eight percent (8%) have not put in place any of the potential risk mitigation strategies.

Figure 6: Mitigating risks for networks and shared data



Question: Q20. Which of the following risk mitigation arrangements do you have in place for?

Base: Those who have: External IT functions (64). Share networks / systems with overseas organisations (49).

Evaluating the effectiveness of cyber security

An organistion's understanding of what is 'normal' activity on its network is one of the most effective ways it can identify any malicious activity. Analytic solutions are important to establish baseline activity in order to detect anomalies and should be regularly tested. Such information is also vital for digital forensics and the ability to successfully investigate and prosecute cyber criminals.

> ...poor logging records and a deficient understanding of the layout of a network can impede the ACSC's ability to assist...

The ACSC 2016 Threat Report noted that factors such as poor logging records and a deficient understanding of the layout of a network can impede the ACSC's ability to assist a victim organisation and increase the duration and costs associated with a compromise.

Furthermore, the AFP has observed a number of examples of organisations not testing what is being logged or retained by analytic agents on their network, resulting in redundant information being compiled.

This survey found that formal evaluation of cyber security is primarily undertaken by the organisations surveyed via active technical testing such as penetration testing, with 72% indicating they do this. Beyond technical testing, 56% have used a specialist advisor or consultant to review their cyber security requirements.

Fewer than half of the organisations surveyed have evaluated their cyber security via any of the other eight potential methods presented in the survey, as shown in Figure 7.

Less direct approaches such as seeking feedback from management or measuring staff awareness are undertaken by 48% and 45% of organisations, respectively. More robust evaluations such as via tabletop exercises, benchmarking against other organisations, formal monitoring against industry standards and measuring trends in incidents and costs are less commonly undertaken.

A very small minority (just 7%) have undertaken return on investment calculations. This is interesting when we know that budgets and bottom lines are very important to Boards.

> A very small minority have undertaken return on investment calculations.

It might be useful for organisations to consider ways to present their Senior Executives with metrics that demonstrate that investment in cyber security helps to protect the bottom line, although this is a complex undertaking and we are not aware of examples where this is happening.

In line with their security posture, less resilient organisations have done far less to formally evaluate their cyber security than more resilient organisations, with 18% not sure or having undertaken none of the activities listed.

7 **Figure 7: Steps taken to formally evaluate cyber security**

	More resilient organisations	Less resilient organisations
Active technical testing (e.g. penetration testing)	77%	59%
Used specialist advisor or consultant to review cyber security requirements	62%	41%
Sought senior management feedback	56%	29%
Monitored levels of regulatory compliance (compliance auditing)	52%	32%
Measured staff awareness	52%	29%
Table top exercises (vulnerability or threat assessment, threat modelling)	49%	21%
Benchmarking against other organisations	38%	15%
Formal monitoring against industry standards	37%	12%
Measured trends in incidents or cost	38%	6%
Return on investment calculations	6%	9%
None of these	3%	9%
Other	3%	3%
Don’t know / not sure	3%	9%

Question: Q27. Which of the following things if any have you done in the last financial year to formally evaluate your organisations cyber security?

Base: All respondents (113). Businesses (68). Government organisations (45). Mature organisations (79). Less mature organisations (34).

Seeking guidance on cyber security threats

The ACSC has a clear and important role to play in providing impartial information, guidance and support to both private sector and government organisations.

> ...the majority of surveyed organisations actively sought out information, advice or guidance from external sources.

During 2015-16, the majority of surveyed organisations (83%) actively sought out information, advice or guidance from external sources.

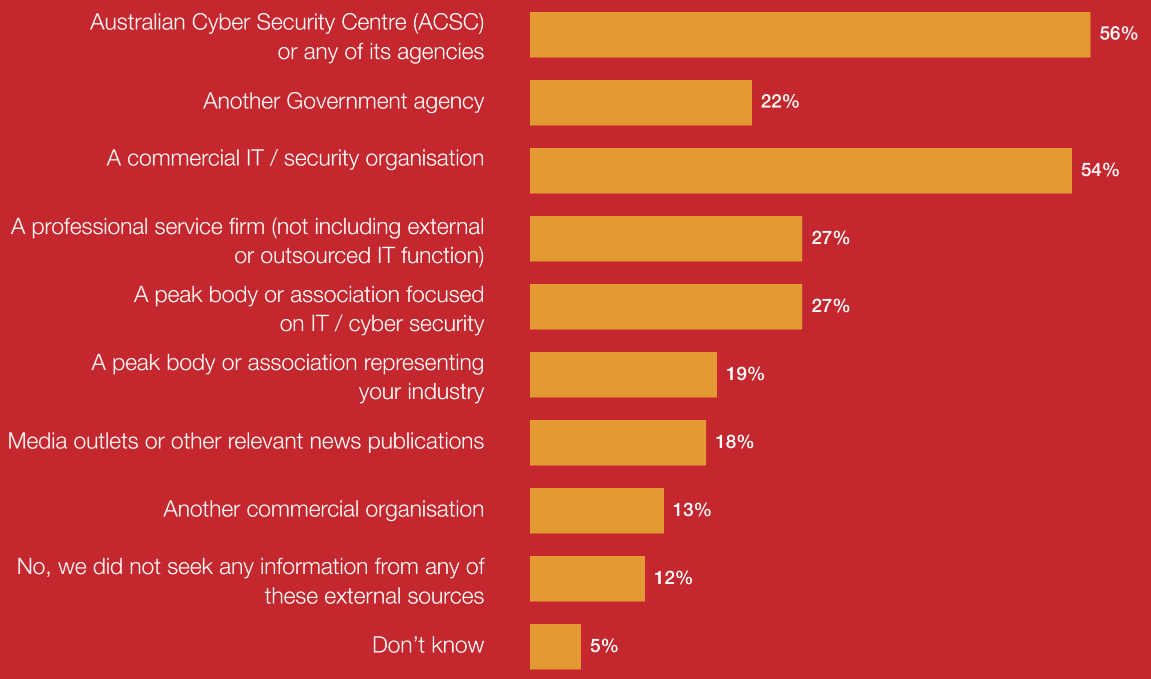
As shown in Figure 8, most organisations used a range of external information sources. While it is unsurprising that government organisations were more likely to seek this type of assistance from government sources (80%), more than half of private sector organisations surveyed (56%) also accessed government sources for cyber security information, advice or guidance.

Interestingly, more cyber-resilient organisations were far more likely than others to have sought out cyber security information, advice or guidance from government sources (75%, compared to 44%). The ACSC and its agencies were the primary source of this information, with 56% of surveyed organisations seeking information, advice or guidance through this channel.

However, organisations are equally reliant on commercial IT/security organisations for information, advice and guidance, with 54% having sought information through this channel in 2015-16.

8

Figure 8: Sought information, advice or guidance on cyber security threats



Question: Q38. Over the 2015–16 financial year, did your organisation seek out any information, advice or guidance on cyber security threats facing your organisation from any of the following external sources?

Base: All respondents (113).

Cyber security incidents experienced in 2015-16

Exploring the nature, frequency and impact of cyber security incidents on Australian organisations

The cyber threat remains ever-present. Most organisations (90%) faced some form of attempted or successful cyber security compromise during the 2015-16 financial year.

Just over half (52%) of all organisations surveyed faced numerous malicious threats on a daily basis — for some threat types up to hundreds of times a day.

In total, 86% of organisations surveyed experienced attempts to compromise the confidentiality, integrity or availability of their network data or system. With just over half (58%) experiencing at least one successful compromise of data and/or systems — up from 50% in the 2015 survey of Major Australian Businesses.

Incidents experienced

In 2015-16, malware and spear email phishing were the most common exploitation methods for successful compromise. Distributed denial of service (DDoS) attempts, although less frequent, were more likely to succeed in disrupting the availability of data or systems and inflict more severe consequences.

Two in five of the organisations experiencing successful breaches were targets of malware infections (42% experienced these, mostly as ransomware or other commodity malware) or email phishing and social engineering fraud (42% experienced this, mostly in the form of impersonation of the organisation's brand or other phishing activity). One in five organisations surveyed experienced successful DDoS incidents (19%) and a similar proportion by another type of compromise (20%).

Almost all organisations faced a range of incidents through email phishing and social engineering fraud, with 84% experiencing attempts of this sort. These were primarily in the form of deception intending to fraudulently obtain a money transfer, or some other phishing activity. A smaller majority also experienced attempts to compromise data or systems through malware (68%).

DDoS attempts or other types of incidents were less common (experienced by 23% and 33%, respectively), but given similar proportions of organisations are successfully impacted by these types of incidents, it appears that these threats are more difficult to fend off. Better preparation to combat DDoS attempts may reduce negative impacts for organisations.

Threat types and definitions

As noted earlier, this survey report sits alongside the ACSC 2016 Threat Report to provide an overview of the cyber threat landscape and how well positioned the Australian Government and organisations are to prevent and respond to such threats.

More information about the types of threats mentioned in this survey report, including definitions and mitigations, are contained in the 2015 and 2016 Threat Reports available from:

https://www.acsc.gov.au/publications

Overall, one third of organisations surveyed experiencing cyber security incidents in 2015-16 was alerted to any of these by a party external to their organisation (33%) and this did not differ by type of organisation or its outlook on cyber security.

For information on preparing for and responding to denial of service activities go to:

https://www.asd.gov.au/publications/protect/preparing-for-responding-to-ddos-activities.htm

9 Figure 9: Cyber security incidents 2015-16 (all surveyed organisations)

Incidents experienced

90% Experienced a cyber security breach or threat that compromised the confidentiality, integrity or availability of network data or systems.

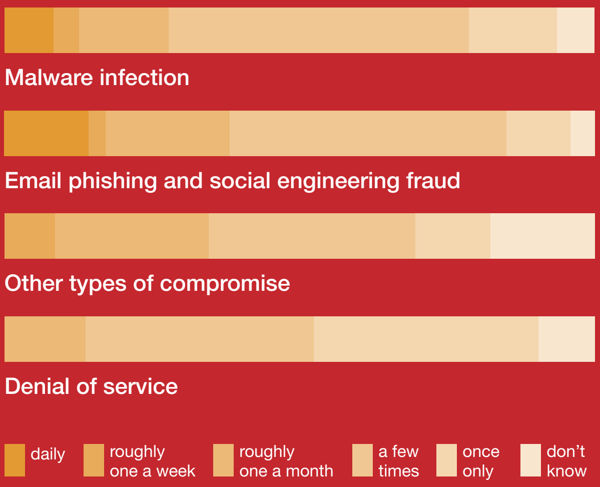
58% Successful incidents

- 42% Malware infection
- 42% Email phishing and social engineering fraud
- 20% Other types of compromise
- 19% Denial of service

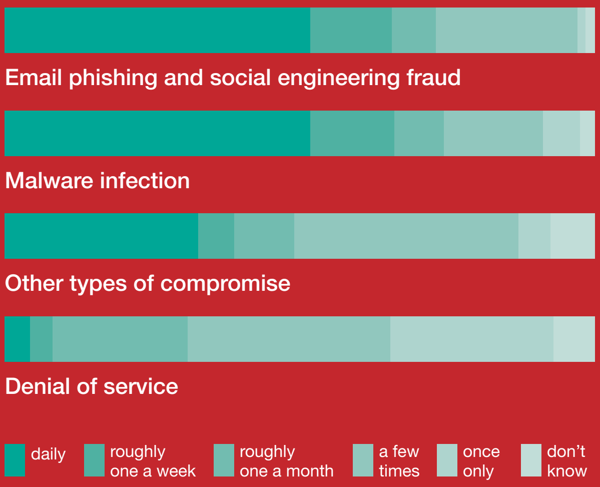
86% Attempts

- 84% Email phishing and social engineering fraud
- 68% Malware infection
- 33% Other types of compromise
- 23% Denial of service

Frequency of incidents



Frequency of attempts



Severity

NOT SEVERE		SEVERE
55%	Email phishing and social engineering fraud	4%
60%	Malware infection	6%
58%	Other types of compromise	5%
42%	Denial of service	23%

Impact

63%	Resources
39%	Financial
13%	Service
9%	Reputation
1%	Other

4% were unaware of any impact

29% experienced none of these

Reporting

38%
reported all incidents to most senior board or management

48%
reported to any external party (34% to ACSC)

45%
did not (39% not serious enough to report, 33% see no benefit)

Frequency of incidents

The organisations surveyed faced numerous malicious cyber threats on a daily basis, many resulting in successful compromises.

Half of the organisations surveyed experienced attempts to compromise data and systems on a daily basis (and even up to hundreds of times a day) through malware (52%) and email phishing (52%), and whilst such attempts were mostly only successful a few times over the year, 9% of organisations indicate having successfully been compromised by malware and 15% by email phishing on a daily basis.

> Half of the organisations surveyed experienced attempts to compromise data and systems on a daily basis... ❞

As noted above, DDoS incidents were less frequent, experienced by 52% once a month or only a few times over 2015-16, while 38% of those that were successfully impacted by them experienced this only once over the year.

Incident severity

Organisations were asked to rate the severity of each type of cyber security incident they experienced on a scale of 1 to 7, where a score of 6-7 was considered severe. The majority of incidents experienced were not rated as severe (giving a rating of 1 or 2 out of 7).

Interestingly, despite being less frequent the impact of DDoS incidents tended to be rated as more severe. Of the organisations who experienced DDoS activity, 23% rated the impact as 6 or 7 out of 7. By comparison, just 6% of organisations or less rated the impact of any other type of incident as severe.

Denial of Service (DOS)

For advice on preparing for and responding to denial of service activities, visit:

https://www.asd.gov.au/publications/protect/preparing-for-responding-to-ddos-activities.htm

Not surprisingly, results varied according to levels of resilience. Less cyber-resilient organisations appeared slightly more likely to experience the impact of malware as 'severe' than more resilient organisations, with 13% of the former rating the severity as 6 out of 7, compared with just 3% of the latter group.

Impact of incidents

Sixty percent (60%) of organisations surveyed experienced tangible impacts on their business as a result of an attempted compromise. When the attempt was successful, the number of organisations that experienced tangible impacts rose to 82%.

The fact that 60% of organisations can point to real business impacts as a result of cyber incidents, despite rating most incidents as relatively low in severity, should give senior managers pause for thought.

The most common consequences reported were related to resources or productivity. Of the organisations that experienced an attempted or successful compromise:

- 56% required additional staff time to deal with the incident
- 35% had staff prevented from doing their work
- 39% felt financial impacts, mainly consisting of further investment required to prevent future incidents (33%) or external repair and recovery costs (11%).

Of concern, almost one in ten (9%) of the organisations characterised as less resilient did not know the impact of cyber security incidents on their organisation, compared to just 1% for more resilient organisations.

More resilient organisations also appear more likely to take note of less direct impacts, with 11% of those subject to threat attempts or compromises noting reputational damage as a result, compared with just 3% of less resilient organisations.

Reporting incidents

Cyber security incidents are commonly reported to the board or equivalent level of organisations, with 86% indicating either all or some of the incidents experienced were reported at this level. Only 9% indicated that no incidents were reported at this level within their organisation.

Reporting to external agencies is less common. Only 48% of organisations experiencing any incident in 2015-16 reported this to an external agency. In particular, reporting by private sector organisations fell from 51% in 2014-15 to just 40% in 2015-16. The main reasons given for not reporting incidents include incidents not being successful, substantial or serious enough (39%), followed by the perception that there are no benefits to reporting (33%).

More needs to be done to raise the value of reporting both attempted and successful incidents as a means to improve the Government's overall understanding of the threat environment. As noted in the ACSC's 2016 Threat Report, the Centre's visibility of cyber security incidents affecting the private sector is heavily reliant on voluntary self-reporting. Although the ACSC is the most common external agency receiving reports (34%), the picture is still incomplete.

As noted earlier in this report, cyber-resilient organisations were far more likely to have sought cyber security information, advice or guidance from government sources. Having an accurate and up-to-date picture of the threat environment is vital for ACSC agencies to assist other organisations who are also at risk. This knowledge would further enable the development of appropriate cyber security advice, incident response assistance and mitigation strategies.

Assistance managing cyber security incidents

Surveyed organisations were asked which sources of assistance they would feel most comfortable approaching if they needed extra help to manage a cyber security incident.

As shown in Figure 10, the majority of organisations indicated they would request help from the ACSC (82%), followed by their own cyber security consultants (55%).

> ” Organisations with a more cyber-resilient outlook were more comfortable approaching their cyber security consultants for additional assistance...

Organisations with a more cyber-resilient outlook were more comfortable approaching their cyber security consultants for additional assistance than less resilient organisations (62%, compared to 3%), which were more likely to approach their managed IT providers (35%, compared to 19%).

As would be expected of partner organisations, eight in ten (82%) were likely to contact the ACSC or any of the agencies for help responding to an incident — rising to 85% for more-resilient organisations. These results validate the importance of the Government's experience and expertise in providing incident response including triage, mitigation and containment.

10 **Figure 10: Most likely contacts for extra help to manage cyber security incident**

	All organisations	More resilient organisations	Less resilient organisations
Australian Cyber Security Centre or any of its agencies	82%	85%	76%
Your cyber security consultants	55%	62%	38%
Managed security service providers	49%	49%	47%
Managed IT providers	24%	19%	35%
Other government agencies	6%	6%	6%
Your cyber insurance broker	4%	5%	0%
Other	4%	4%	3%
Don't know	2%	0%	6%

Question: Q27. Which of the following things if any have you done in the last financial year to formally evaluate your organisations cyber security?

Base: All respondents (113). Businesses (68). Government organisations (45). Mature organisations (79). Less mature organisations (34).

Contact details

Australian government customers, businesses or other private sector organisations with questions regarding this advice should contact the ACSC:

☎ **Telephone:**
1300 CYBER1 (1300 292 371)

Website:
http://www.acsc.gov.au/contact

Australian Government

Australian Cyber Security Centre

PARTNERING FOR A CYBER SECURE AUSTRALIA