Australian Government
Australian Cyber Security Centre

2015 CYBER SECURITY SURVEY: MAJOR AUSTRALIAN BUSINESSES

CERT AUSTRALIA
PROTECTING OUR NATIONAL INTERESTS ONLINE

ACSC
AUSTRALIAN CYBER SECURITY CENTRE

PARTNERING FOR A CYBER SECURE AUSTRALIA


2015

2015 CYBER SECURITY SURVEY:
MAJOR AUSTRALIAN BUSINESSES

978-1-925290-57-8 (Online)

Contact us

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

Attorney-General's Department
3–5 National Cct
BARTON ACT 2600
Email: copyright@ag.gov.au

FOREWORD

THE CYBER THREAT FACING AUSTRALIA IS UNDENIABLE AND UNRELENTING. AN ISSUE THAT ONCE ONLY CONCERNED IT SECURITY PROFESSIONALS NOW EXTENDS TO THE BOARDROOM, TO SHAREHOLDERS AND TO INDIVIDUALS.

CERT Australia, one of the partner agencies in the Australian Cyber Security Centre (ACSC) is the primary point of contact for cyber security issues affecting major Australian businesses. In 2014-15, CERT Australia responded to 11,733 incidents affecting businesses, 218 of which involved systems of national interest and critical infrastructure.

For Australia to continue to be a trusted place in the world to do business, we must understand the cyber threat and implement strong cyber defences.

To understand the current cyber security posture and attitudes of Australian business organisations, the ACSC has conducted its inaugural Cyber Security Survey of major Australian businesses.

The cyber security posture of Commonwealth Government agencies and their networks is addressed in the 2015 ACSC Cyber Security Survey of Commonwealth Government Entities.

The ACSC will use the information gathered from both surveys to inform Australia's cyber security strategies and advice. These aim to increase cyber resilience both within public and private organisations for the cyber security of the nation.

The findings from major Australian businesses show that organisations are taking action to protect their information and networks. However, there is still opportunity to improve Australia's cyber security resilience.

I encourage all organisations to read this report, note the range of threats and vulnerabilities identified and take action to improve their cyber security posture.

Importantly, I would also like to thank all organisations that took the time to respond to the survey—your input is highly valued and will contribute to enhancing Australia's cyber resilience.

Clive Lines
Coordinator
Australian Cyber Security Centre

EXECUTIVE SUMMARY

THE NEED FOR STRONG CYBER SECURITY MEASURES HAS NEVER BEEN GREATER, WITH THE RISE OF SOPHISTICATED AND TARGETED MALICIOUS ACTIVITY AGAINST AUSTRALIA'S NETWORKS.

In this context, the 2015 Australian Cyber Security Centre (ACSC) Cyber Security Survey of major Australian businesses was conducted to obtain a better picture of Australian organisations' understanding of cyber threats and how they are positioned to secure their networks.

These organisations all form part of Australia's systems of national interest. They underpin the social and economic welfare of Australia and deliver essential services including banking and finance, defence industry providers, communications, energy, resources, transport and water.

For trend analysis, the report draws on previous findings from the *2013 CERT Australia Cyber Crime & Security Survey*.

The findings demonstrate that cyber security incidents are still common and recurrent for Australian businesses. Half of the respondents reported experiencing at least one cyber incident that compromised the confidentiality, integrity or availability of a network's data or systems in the last year.

Encouragingly, organisations are applying cyber security measures, including policies and standards as well as a range of technologies and mitigation strategies—with clear improvements (as demonstrated throughout the report).

However, organisations are still being targeted by a broad range of threats—particularly those designed to elicit money. Of note, the number of ransomware incidents reported has drastically increased—four times that of 2013. Most other threat types have remained stable. Ransomware also affected every sector that had experienced a cyber security incident, which demonstrates the indiscriminate targeting and the sophistication of this type of threat.

IT security awareness and practices of general staff appear to have improved since 2013. However, many cyber threats now feature well-crafted socially-engineered emails that make it difficult for the user to determine legitimacy, regardless of training. The rise of these threats could be behind the shift in investment moving away from awareness training toward more technical controls in an effort to prevent the user from having to make a judgement call.

The findings also demonstrate that industry organisations are yet to be convinced of the benefits of reporting incidents. Many industry organisations chose not to report incidents as there was no perceived benefit to them.

Reporting cyber security incidents ensures that appropriate and timely assistance can be provided. It also helps to develop a threat picture and assist other organisations who may also be at risk. Cyber security incident reports are also used for developing new advice, procedures, techniques and training measures to help prevent future incidents.

SECURITY POSTURE

- Only **3%** of respondents do not have an IT Security area. This is a significant improvement from **16%** in 2013.
- **77%** of respondents have cyber security incident response plans in place with **37%** of these regularly reviewing it.
- **56%** of respondents increased expenditure on cyber security in the last 12 months. This is a significant increase from 2013, where only **27%** of respondents reported an increase.
- **82%** of industry organisations use external IT security standards or frameworks.
- **100%** of respondents reported using anti-virus software and all but one respondent reported using network based firewalls.
- Awareness and implementation of ASD's **Top 4** *Strategies to Mitigate Targeted Cyber Intrusions* is good with more than **90%** of respondents having adopted three of the four strategies.

> 50% of respondents have experienced at least one cyber incident in the past year.

INCIDENTS AND THREATS

- **50%** of respondents have experienced at least one cyber incident in the past year.
- Of concern, **8%** of respondents were unsure if they had experienced a cyber incident.
- **92%** of respondents that experienced an incident indicated the threat of the cyber security incident/s had been identified in the organisation's risk register. This is more than double the 2013 finding of **39%**.
- There has been a significant surge in the number of ransomware incidents with four times the number of respondents reporting in 2015 (**72%**) as compared to 2013 (**17%**).
- Ransomware is the threat of most concern amongst respondents (**72%**), followed by theft or breach of confidential information (**70%**) and Advanced Persistent Threats (**66%**).
- The 'trusted insider' was the actor of most concern to respondents (**60%**), followed by 'issue motivated groups or hacktivists' (**55%**).
- **43%** of respondents did not report cyber incidents to anyone with the main reason given as **"...no benefits of reporting"**.

THE 2015 AUSTRALIAN CYBER SECURITY CENTRE (ACSC) CYBER SECURITY SURVEY IS COMPRISED OF TWO REPORTS, ONE FOCUSED ON MAJOR AUSTRALIAN BUSINESSES AND ONE FOCUSSED ON COMMONWEALTH ENTITIES AND AGENCIES.

This report focusses on findings from major Australian businesses.

The 2015 ACSC Cyber Security Survey was designed to obtain a collective view of Commonwealth and business' understanding of the cyber threat and how they are positioned to defend their information and networks.

The survey was conducted over a four week period and responses were provided by Chief Information Officers or Information Technology Security Advisors.

Separating the major businesses data from the Commonwealth data is reflective of the different operating environments of these two groups.

Commonwealth agencies have a mandatory requirement to adhere to cyber security standards under the *Australian Government Information Security Manual (ISM)*. The Australian Signals Directorate (ASD) conducted this part of the survey and analysed the data for Government consideration.

Industry data was collected from major Australian businesses that partner with CERT Australia, and that underpin the social and economic welfare of Australia and deliver essential services including banking and finance, defence industry providers, communications, energy, resources, transport and water[1]. CERT Australia works on a trust basis with these businesses and provides support to increase cyber resilience.

This component of the survey was hosted online through an online survey platform and provided complete anonymity for industry respondents.[2]

[1] 2% of business respondents identify as government critical infrastructure owners and operators. For the purpose of the survey they will be grouped with the business/industry findings, not with Commonwealth Government organisations.

[2] The industry component of the survey was approved by the Statistical Clearing House in accordance with Government best practice: Australian Government Statistical Clearing House Approval Number: 02452 – 01.

OVERVIEW OF RESPONDENTS

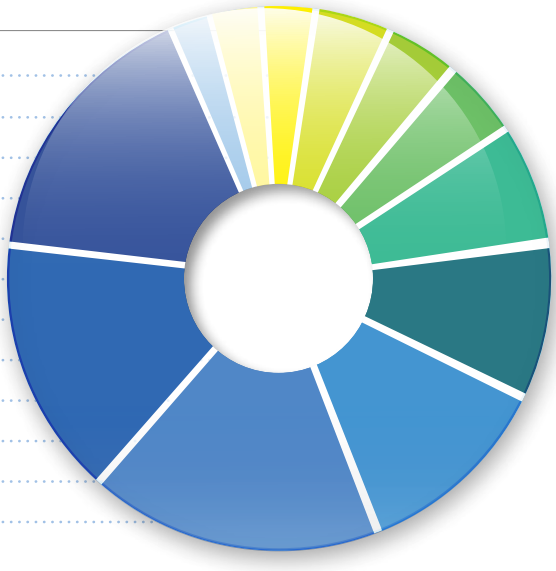
ORGANISATION TYPE

The 2015 ACSC Cyber Security Survey: Major Australian Businesses was completed by 149 respondents, from more than 12 industry sectors. The greatest representation was from the defence industry sector[3] at 18%, followed by the energy sector at 17%, and the banking and finance sector at 11%.

Figure 1 – breakdown of the sectors that responded to the survey.

FIGURE 1

DEFENCE INDUSTRY[3]	18.0%
OTHER	17.0%
ENERGY	17.0%
BANKING & FINANCE	11.0%
COMMUNICATIONS	9.0%
WATER SERVICES	8.0%
MINING AND RESOURCES	5.0%
TRANSPORT	4.0%
GOVERNMENT	4.0%
RETAIL	3.0%
HEALTH	3.0%
MANUFACTURING	2.0%



Note:

- 'Other' mainly included local government, entertainment, media and legal services.
- 'Government' refers to organisations that identified themselves as government, principally government-business enterprises or government owned/operated critical infrastructure.

[3] Includes Defence contractors and Defence Industry Security Program (DISP) members.

SIZE OF THE ORGANISATION

Most of the respondents (67%) were from large organisations (200+ employees), 23% were from medium size organisations (21-199 employees) and 10% were from small organisations (less than 20 employees).

Figure 2 – breakdown of the size of respondent organisations.

FIGURE 2

SMALL (< 20 EMPLOYEES)	10.0%
MEDIUM (20 - 199 EMPLOYEES)	23.0%
LARGE (200 + EMPLOYEES)	67.0%

IT SECURITY AREA

97% of respondents have an IT Security area. Of those, 56% have an internal IT Security team, 3% outsource and 39% use a mix of internal and outsourced services.

Only 3% of industry respondents reported that they do not have an IT Security area. This is a significant improvement from the previous, *CERT Australia Cyber Crime & Security Survey* conducted in 2013, where 16% of respondents reported their organisation did not have an IT Security area with any staff dedicated to this role.

The majority (54%) of respondents reported having a small IT security area with 1-5 staff members, 13% had medium sized teams with 6-14 staff and 15% had large teams with 15+ staff.

These results are positive, demonstrating a growing appreciation for the importance of cyber security and the role played by IT Security teams.

PRESENCE IN OTHER COUNTRIES

It is essential that all interconnected networks, both domestic and international, are considered as part of an organisation's overall cyber security posture. This includes satellite offices, third party networks and partner networks. A compromise of one network can affect all systems it is connected to and have a significant impact on the organisation.

36% of respondents have a presence outside Australia, and 79% of those are taking their internationally connected networks into consideration regarding their overall cyber security posture. This is a significant improvement when compared to the 2013 finding of 55%.

CONTRACT TO GOVERNMENT

64% of respondents contract or provide services to government. These organisations may therefore be responsible for protecting not only their own information but also government data, including potentially sensitive or national security classified information.

36% of respondents have a presence outside Australia, and 79% of those are taking their internationally connected networks into consideration regarding their overall cyber security posture.

THE SECURITY POSTURE OF AN ORGANISATION IS MADE UP OF A NUMBER OF DIFFERENT ELEMENTS THAT TOGETHER HELP AN ORGANISATION STAY CYBER RESILIENT.

These elements include up-to-date technology, training, policies and procedures and understanding the cyber security risk beyond the immediate network. Many organisations now layer their security defences for maximum effect to ensure if one layer fails against an intrusion, there are multiple layers of protection.

IT SECURITY POLICIES, PROCEDURES OR PLANS

Developing, implementing and regularly reviewing an incident response plan is a key recommendation to maintain cyber resilience.

An effective incident management plan can reduce the severity and duration of an incident by preplanning how it will be managed, allowing an organisation to respond in an efficient, cost-effective manner. It is crucial, however, that organisations regularly review their plans to ensure they continue to be contemporary and effective.

> Implementing a removable media policy allows for the control and accountability of removable media in the workplace to reduce the risk of malware execution and data exposure.

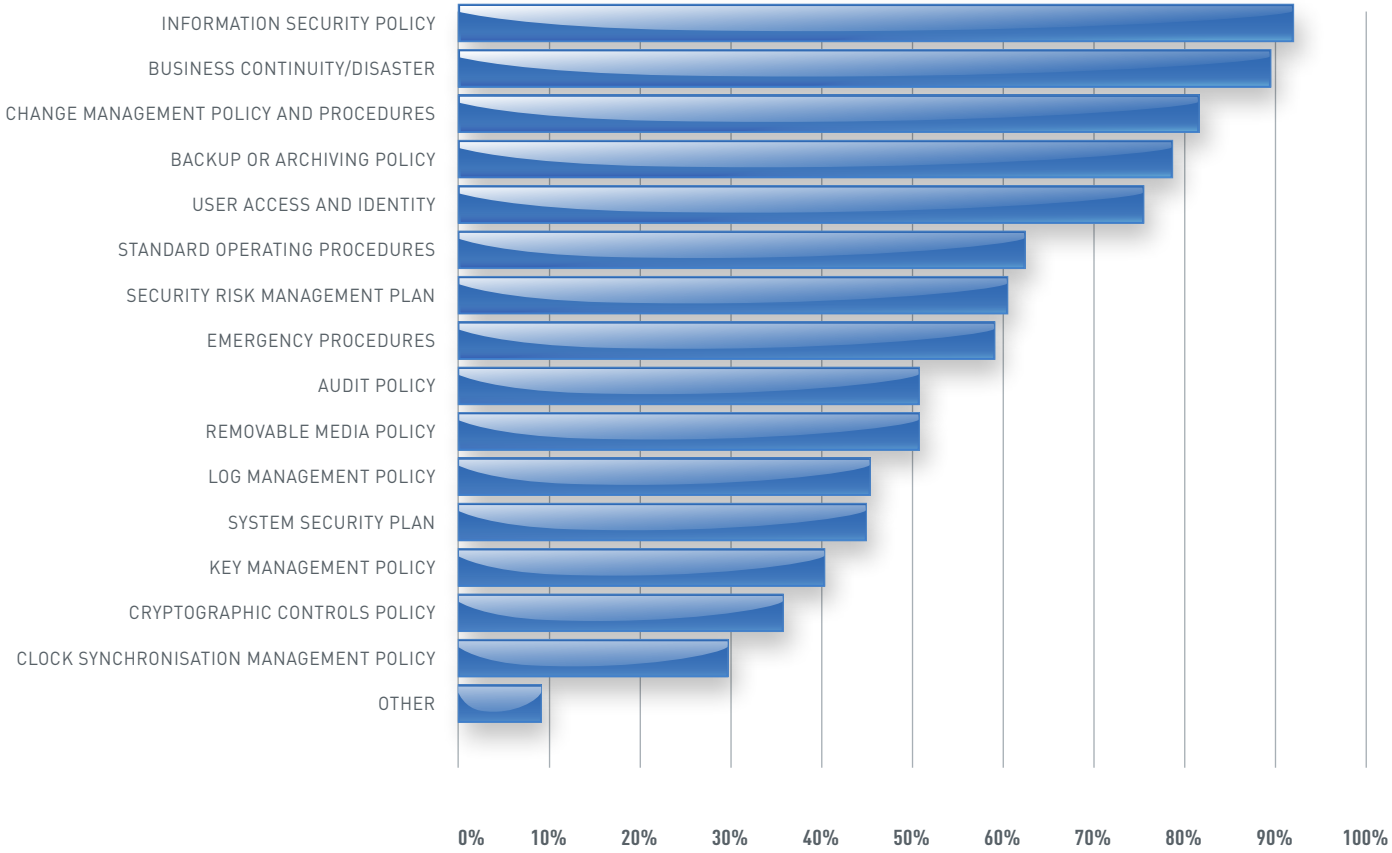
77% of respondents have cyber security incident response plans in place with 37% of these regularly reviewing it.

Industry organisations were asked what other types of IT security policies, plans or procedures they were using.

Basic security policies, plans and procedures are being applied by the majority of organisations. For example, 93% have an information security policy, 89% have business continuity/disaster recovery plans, 87% undertake network monitoring and 78% have a backup or archiving policy.

While the majority of organisations are using some security policies there are areas for improvement. For example, less than half of respondents have a system security plan in place (44%), and only 51% of organisations have a removable media policy.

FIGURE 3 – IT security policies, procedures or plans used by respondent organisations.



IT SECURITY STANDARDS

Industry organisations are encouraged to adopt a risk-based approach to cyber security and aim for best practice with consideration to their sector peers. Standards and frameworks can enable an organisation to identify and prioritise threats and respond efficiently to mitigate vulnerabilities. Organisations can also commit to examining information security risks and implementing a comprehensive suite of information security controls and management processes.

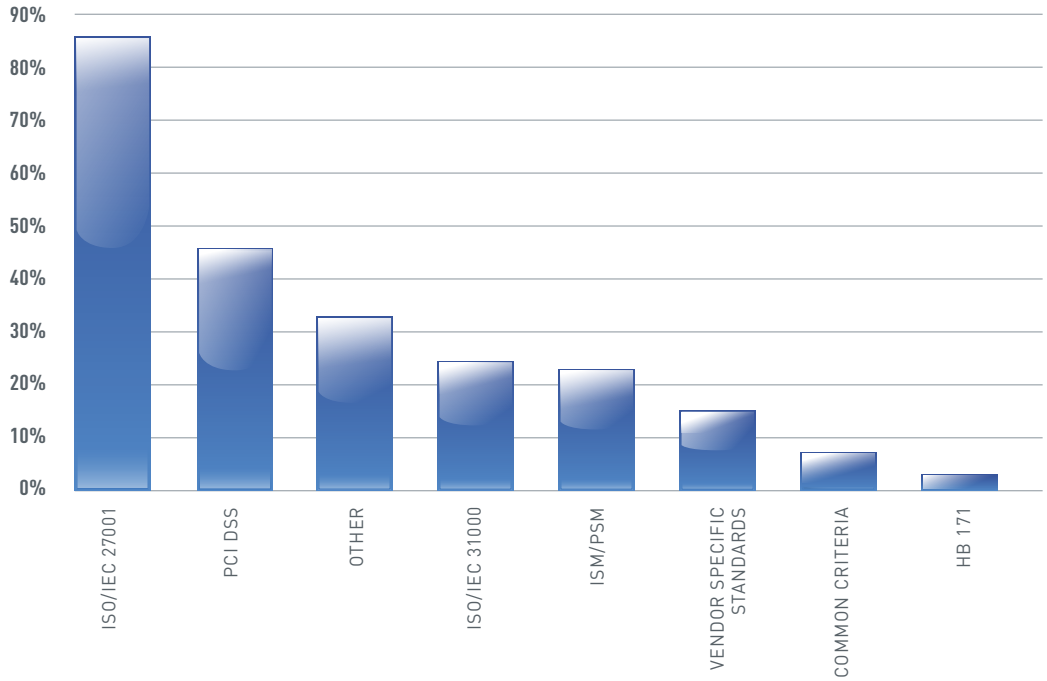
82% of industry organisations use external IT security standards or frameworks.

ISO/IEC 27001 is the most common (85%), followed by Payment Card Industry Data Security Standard (PCI DSS) (46%) and ISO/IEC 31000 (24%). These findings are consistent with 2013 data.

Of the 17%[4] that indicated they were not using external IT security standards or frameworks, just under half were defence contractors or from local government entities. These sectors are subject to requirements under the *Australian Government Information Security Manual* and may not have considered this standard to be 'external'.

It is therefore likely that actual compliance with an external standard or framework is closer to 90%. This demonstrates that businesses are focused on employing a risk based approach for their cyber security posture.

FIGURE 4 – use of IT security standards and frameworks.



[4] 1% did not know.

IT SECURITY TECHNOLOGIES

IT security technologies function as filters, gateways and control points that provide visibility and management of data as it moves through systems and networks.

Respondents were asked which technologies they use to protect their systems and information.

100% of respondents reported using anti-virus software and all but one respondent reported using network based firewalls.

Over 90% of respondents reported using operating system patch management, remote access VPNs, anti-spam filters, physical access control and password complexity rules.

The least used technologies, with less than half the respondents reporting use, included removable media management, application whitelisting, host-based intrusion prevention or detection system, automated dynamic analysis, network encryption and data loss prevention.

The use of these technologies demonstrates organisations are actively working to protect their systems and information. Different technologies will provide a different return on investment and security value for different organisations. It is critically important organisations actively review these technologies to ensure they continue to be effective and suitable for their systems.

IT SECURITY SKILLS AND TRAINING

Having appropriately trained and qualified IT security staff can greatly impact on the cyber security posture of an organisation.

Respondents were asked about the qualifications and training of their IT security staff.

87% of respondents have staff with at least five years' experience working in IT security, while nearly 70% have staff with tertiary qualifications. This is an improvement on the 2013 findings from 79% and 65% respectively.

Over 60% of respondents have staff with either a vendor certificate, vendor neutral certificate, or have participated in ad hoc courses. Only 7% of organisations responded that their IT security staff had no form of formal training or qualification. Both of these findings are consistent with 2013 data.

Respondents were also asked if other staff in their organisation need to improve their IT security skills and/or practices.

The findings for general staff and management are lower than the 2013 findings. As these staff make up the majority of an organisation, this indicates broad improvement across organisations. The need identified for the CEO and board of directors has remained broadly consistent, while interestingly, the need identified for IT staff has risen by 10%, despite the increase in training and qualification. This is perhaps in recognition of the vital role that IT staff play in defending and protecting systems and networks.

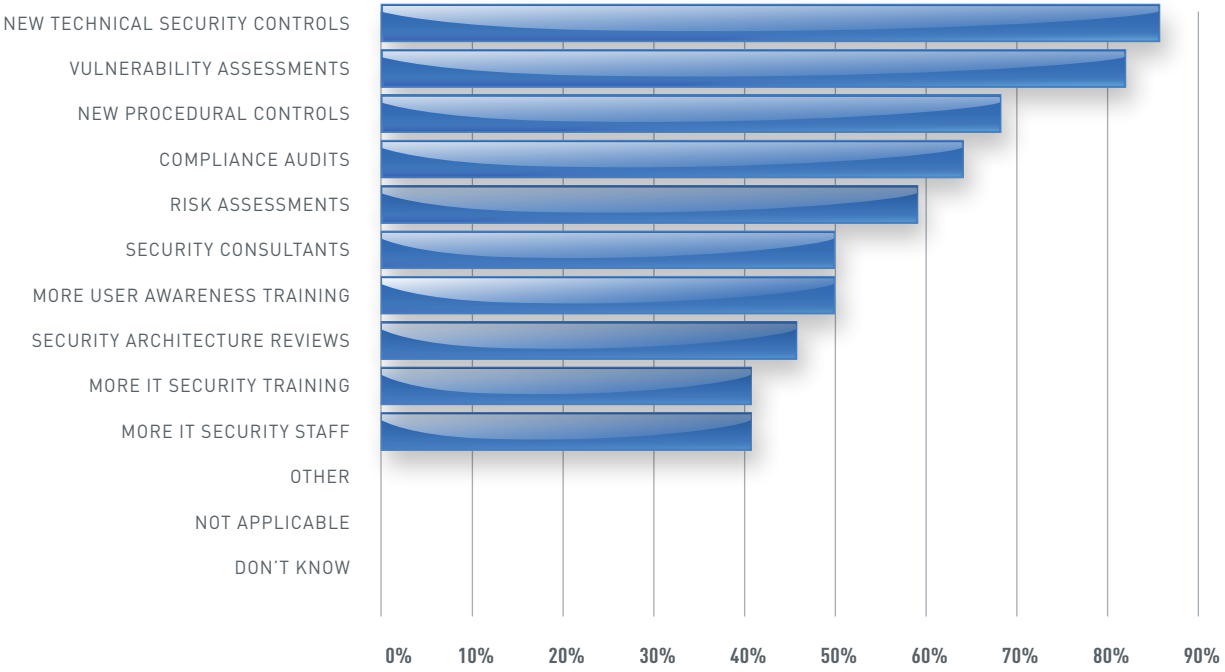
IT SECURITY SKILLS & TRAINING NEEDS	2015	2013	change
Respondents identifying this need for general staff	89%	95%	↓ -6%
Respondents identifying this need for management	83%	91%	↓ -8%
Respondents identifying this need for IT staff	76%	66%	↑ +10%
Respondents identifying this need for the CEO	66%	63%	↑ + 3 %
Respondents identifying this need for the board of directors	62%	62%	0%

CYBER SECURITY EXPENDITURE

Over the last year, 56% of respondents increased expenditure on cyber security. This is a significant increase from the previous *CERT Australia Cyber Crime & Security Survey* conducted in 2013, where only 27% of respondents reported an increase.

Respondents largely saw this increased spending go towards new technical and procedural controls, obtaining vulnerability assessments and compliance audits.

FIGURE 5 – how organisations increased cyber security expenditure.



Of note, while some organisations are actively investing in user awareness training; more are investing in technical controls to prevent the user from having to make a judgement call. This could be attributed to the rise of well-crafted, socially-engineered emails that make it difficult for the user to determine legitimacy, regardless of training.

ADOPTION OF THE AUSTRALIAN SIGNALS DIRECTORATE'S (ASD) TOP 4 MITIGATION STRATEGIES

TOP 4 STRATEGIES TO MITIGATE TARGETED CYBER INTRUSIONS

1. **Application whitelisting** – is designed to protect against unauthorised and malicious programs executing on a computer. It aims to ensure that only specifically selected programs and software libraries (DLLs) can be executed, while all others are prevented from executing.
2. **Patching applications** – applying patches to applications is a critical activity in ensuring the security of systems. Patch or mitigate systems with 'extreme risk' vulnerabilities within two days and use the latest version of applications. This will reduce the chances of malicious intruders taking advantage of vulnerabilities within applications.
3. **Patching operating systems** – applying patches to operating systems is a critical activity in ensuring the security of systems. Patch or mitigate systems with 'extreme risk' vulnerabilities within two days and use the latest version of operating systems. This will reduce the chances of malicious intruders taking advantage of vulnerabilities within operating systems.
4. **Restricting administrative privileges** – administrator accounts are often targeted by malicious actors as they have more privileged access than a normal account. Therefore restricting administrative privileges to operating systems and applications based on user duties, and not web browsing or checking emails on administrator accounts, will reduce the likelihood of compromise.

86% of respondents reported that IT staff in their organisation were aware of ASD's top 4 mitigation strategies. Of those, most are implementing one or more strategies:

- **31%** — have implemented application whitelisting.
- **92%** — patch applications
- **99%** — patch operating system vulnerabilities
- **92%** — minimise the number of users with administrative privileges.

While these results are very positive, it's clear that application whitelisting is not used widely as a mitigation strategy. There has, however, been some improvement on 2013 data where only 23% of respondents reported use.

The main barriers for implementation, as identified by respondents, were financial, cultural and technical constraints.

Anecdotal evidence (collected from other industry engagement activities) shows that while businesses would like to implement application whitelisting, it can be difficult and expensive. Despite this, many businesses have indicated they are attempting or preparing to implement this mitigation strategy.

Implementing application whitelisting across an entire organisation can be a daunting task—however it does have significant benefits. As a first step, ASD recommends deployment to high value and high profile employees such as executive officers and their assistants.

CLOUD-BASED SERVICES

Cloud-based services are increasingly popular with 82% of industry respondents using or planning to use cloud-based services.

Organisations that are not using cloud-base services identified security (50%) and concerns about maintaining business functionality if the cloud services became unavailable (43%) as the main reasons for not adopting cloud services.

CYBER SECURITY INCIDENTS

Respondents were asked about the number and type of cyber security incidents identified on their networks in the previous 12 months. Respondents were also asked about the origin and possible motives for the activity as well as why they may have been successful.

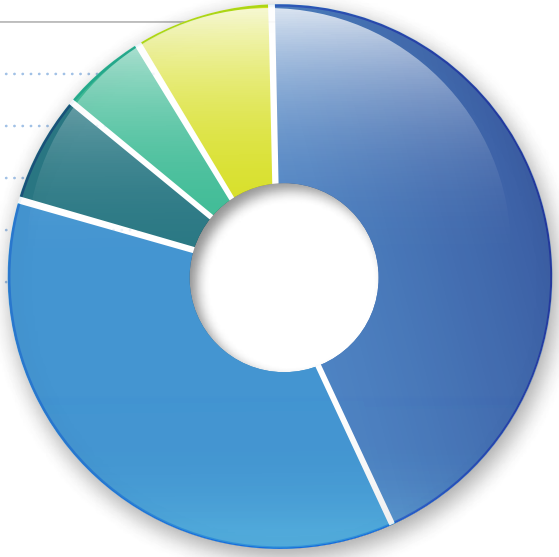
Cyber security incidents were considered to be those that harmed the confidentiality, integrity or availability of a network's data or systems.

50% of respondents reported experiencing one or more cyber security incident/s in the last 12 months, while 42% reported that they had not experienced any incidents.

Figure 6 – breakdown of the number of cyber security incidents experienced.

FIGURE 6

NO	42.0%
YES, 1 TO 5	40.0%
YES, 6 TO 10	6.0%
YES, 10+	5.0%
DON'T KNOW	8.0%



Of concern, 8% of respondents were unsure if they had experienced a cyber security incident.

This finding may reflect that a number of cyber intrusions have gone undetected by some organisations. Anecdotal evidence suggests that some businesses are unaware of the full scope of unauthorised activity on their networks.

Most prevalent types of incidents:

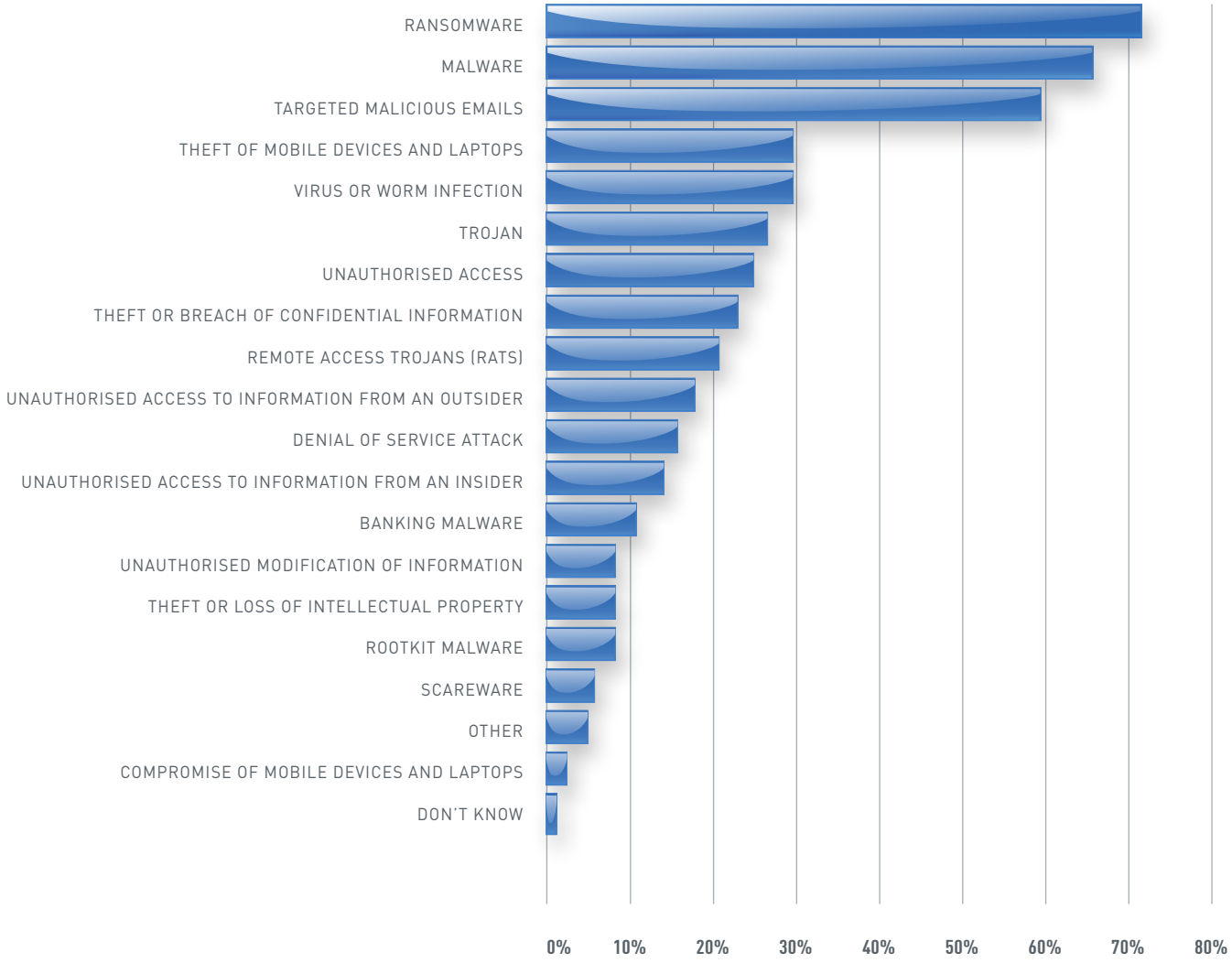
- **72%** — ransomware
- **66%** — malware
- **59%** — targeted malicious emails
- **30%** — virus or worm infection
- **30%** — theft of mobile devices and laptops
- **27%** — trojan
- **20%** — remote access trojans (RATs)
- **25%** — unauthorised access
- **23%** — theft or breach of confidential information
- **17%** — unauthorised access to information from an outsider
- **16%** — denial of service attack
- **14%** — unauthorised access to information from an insider

> The number of ransomware incidents reported has drastically increased—four times that of 2013.

Of note, the number of ransomware incidents reported has drastically increased—four times that of 2013. Most other threat types have remained stable.

Ransomware also affected every sector that had experienced a cyber security incident, which demonstrates the indiscriminate targeting and the sophistication of this type of threat.

FIGURE 7 – breakdown of types of cyber security incidents experienced.



RANSOMWARE

Ransomware refers to extortion through the use of malware that typically locks a computer's content and requires victims to pay a ransom to regain access.

The ACSC 2015 Threat Report states that ransomware campaigns against Australian organisations will continue to be prominent[5].

Many of the incident types use socially engineered emails as the delivery mechanism which makes it very difficult for the user to determine legitimacy. This increased sophistication and targeting can undermine preventative activities such as IT education and awareness programs, making layered security defences critical in mitigating and responding to these threats.

RISK REGISTER

A risk register is used to record any and all identified risks, as well as incidents and analysis of mitigations. This provides IT security teams with an improved understanding of the threat landscape so they can better protect their systems in the future.

Organisations were asked if the threat of the cyber security incident/s they experienced had been identified in the organisation's risk register - with 92% responding yes. Impressively, this is more than double the 2013 survey at 39%.

[5] *Australian Cyber Security Centre 2015 Threat report*, page 24 <https://www.acsc.gov.au/publications/ACSC_Threat_Report_2015.pdf>.

CYBER SECURITY INCIDENT CONTRIBUTING FACTORS

Many internal and external factors can contribute to a cyber incident.

Predominant factors contributing to industry cyber incidents were identified as staff errors or omissions, poor security culture, misconfigured systems, as well as the sophistication and targeting of the incidents.

Survey respondents were also asked what they believe was the motive for the incident/s, with illicit financial gain as the most common motive identified. Financially motivated threats are often broad-based and appeared to affect respondents in most industry sectors. 'Random attack' was also identified as a common motive.

This can be mostly attributed to the increase in ransomware and malware campaigns which utilise indiscriminate targeting for illicit financial gain. It is important to note the difficulty of attribution, and that perception of motive may differ from the reality.

REPORTING

Respondents were asked if the cyber security incident/s had been reported and if so, to whom.

51% of respondents reported cyber security incidents, predominantly to CERT Australia, law enforcement and/or as mandatory reporting to a regulator; while 43% did not report incidents and 6% were unsure if an incident was reported.

Respondents were asked why incidents were not reported.

60% responded that there are 'no benefits of reporting' with 'negative publicity' and 'the attackers probably wouldn't get caught or prosecuted' both at 22%.

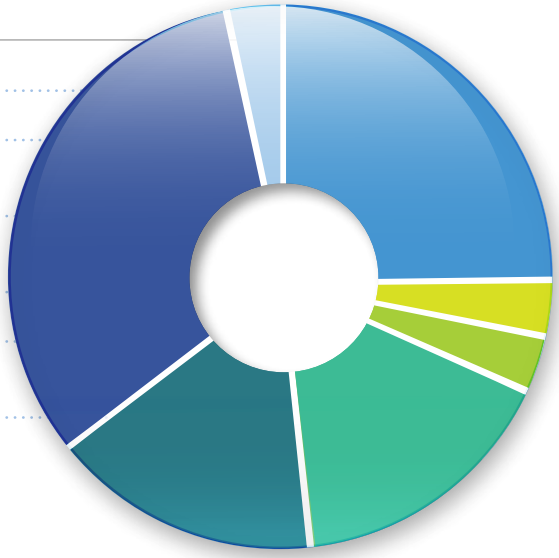
These findings indicate that Australian businesses are yet to be convinced about the benefit of reporting, but also that many incidents are considered too minor to report.

CERT Australia works on a partnership and trust basis with business and encourages the voluntary and timely reporting of cyber security incidents. This allows CERT to form a more accurate view of cyber security threats and make sure that businesses receive the right help and advice. All information provided to CERT is held in the strictest confidence.

Figure 8 – provides a breakdown of whether cyber security incidents were reported.

FIGURE 8

DON'T KNOW	6.3%
YES – TO CERT AUSTRALIA	36.5%
YES - TO THE AUSTRALIAN CYBER SECURITY CENTRE	6.3%
YES - TO THE AUSTRALIAN CYBERCRIME ONLINE REPORTING NETWORK	6.3%
YES – TO LAW ENFORCEMENT	22.2%
YES – MANDATORY REPORTING TO A REGULATOR	22.2%
NO	42.9%



Individuals and businesses can also report instances of cybercrime to the Australian Cybercrime Online Reporting Network (ACORN). Reporting helps develop a better understanding of the cybercrime affecting Australia. By understanding the enablers, we can make it harder and less rewarding to commit cybercrime, therefore making Australia a safer place to do business.

ACORN

ACORN is an accessible and secure method for individuals to report instances of cybercrime. ACORN is designed to make it easier for people to recognise, report and avoid common types of cybercrime. Visit the ACORN website at acorn.gov.au.

CONCERNS AND RESPONSES TO CYBER THREATS

Respondents were asked a series of questions about the cyber threats and actors of most concern to their organisation and the responses to cyber threats they consider most important.

CYBER THREATS OF MOST CONCERN

- **72%** — ransomware or scareware
- **70%** — theft or breach of confidential information
- **67%** — targeted malicious emails
- **66%** — advanced persistent threats (APTs)
- **62%** — unauthorised access to information from an outsider
- **58%** — social engineering
- **56%** — unauthorised access to information from an insider
- **55%** — loss or destruction of information
- **54%** —loss of service ability
- **52%** —virus or worm infection
- **46%** — trojan
- **46%** — unauthorised modification of information
- **40%** — theft or loss of intellectual property
- **40%** — rootkit malware
- **36%** — denial of service attack
- **32%** — compromise of mobile devices and laptops
- **24%** — wire fraud
- **22%** — theft of mobile devices and laptops
- **7%** — other

CYBER ACTORS OF MOST CONCERN

- **60%** — trusted insiders
- **55%** —issue motivated groups or hacktivists
- **54%** — organised criminal syndicates
- **54%** — state based actors
- **45%** — individuals
- **4%** — other

Of note, there were significant concerns regarding insider threat, with 60% identifying trusted insiders as the most concerning cyber actors. Similarly, access to unauthorised information by an insider was rated as a significant threat of concern.

Ransomware topped the industry respondents list of concerns at 72%.

Ransomware was also the most common cyber incident type experienced by industry respondents with 72%.

RESPONSES TO CYBER THREATS

In response to cyber security threats, industry respondents identified a broad collection of factors as being important. The most popular response was user awareness training at 87%.

Closely following were senior leadership support at 79% and technical controls at 75%.

THE AUSTRALIAN CYBER SECURITY CENTRE (ACSC) BRINGS TOGETHER EXISTING CYBER SECURITY CAPABILITIES ACROSS DEFENCE, THE ATTORNEY-GENERAL'S DEPARTMENT - CERT AUSTRALIA, AUSTRALIAN SECURITY INTELLIGENCE ORGANISATION, AUSTRALIAN FEDERAL POLICE, AND THE AUSTRALIAN CRIME COMMISSION, IN A SINGLE LOCATION.

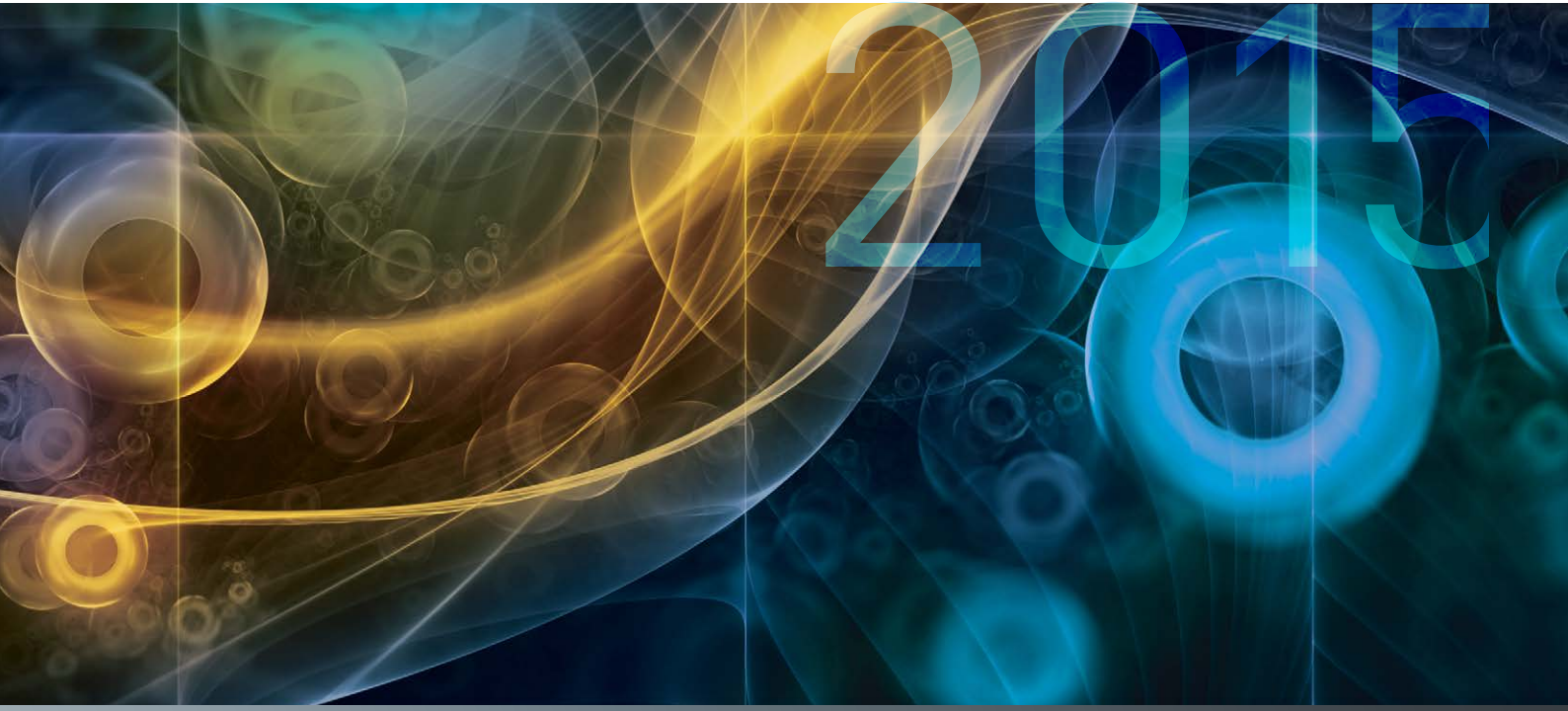
This important Australian Government initiative aims to ensure that Australian networks are amongst the hardest in the world to compromise. The ACSC is a hub for greater collaboration and information sharing with the private sector, state and territory governments, academia and international partners to combat the full range of cyber threats.

CERT Australia is the main point of contact for cyber security issues affecting major Australian businesses. It provides advice and support on cyber threats and vulnerabilities to the owners and operators of Australia's critical infrastructure and other systems of national interest. These businesses and industries underpin essential service delivery across Australia, including banking and finance, communications, energy, resources, transport and water.

2015

Australian Government

Australian Cyber Security Centre



PARTNERING FOR A CYBER SECURE AUSTRALIA