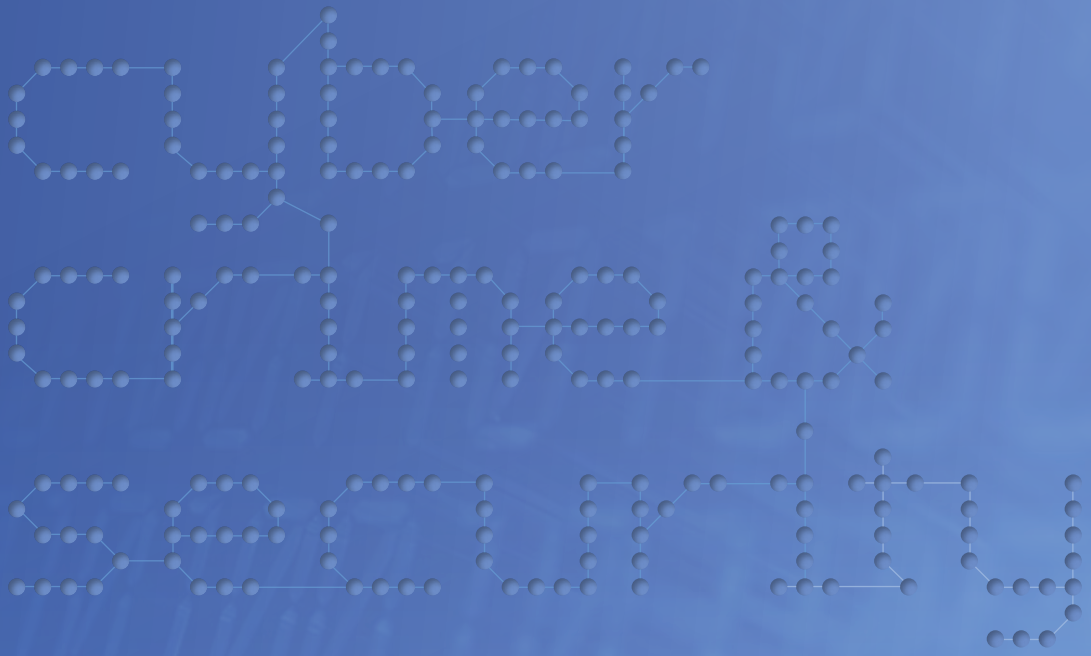
Australian Government



CYBER CRIME & SECURITY SURVEY REPORT 2013

PROTECTING OUR NATIONAL INTERESTS ONLINE

CERT AUSTRALIA

FOREWORD

MALICIOUS CYBER ACTIVITY IS ON THE INCREASE – AND EVERY BUSINESS WITH AN ONLINE PRESENCE IS AT RISK. THIS MAY INVOLVE THE LOSS OF CRITICAL DATA AND CONSUMER CONFIDENCE, AS WELL AS PROFITS

CERT Australia is at the forefront of the Australian Government's support in helping protect Australian businesses from cyber attacks, and providing assistance on request.

The annual survey is an important part of CERT Australia understanding the cyber threat environment, so we can continue providing businesses with the best cyber security advice and support possible.

For example, findings from the survey indicate that the most vulnerable part of a business to cyber threat was the internal network. This may include a range of system vulnerabilities, such as weaknesses in authentication, unused and unpatched services, as well as insecure devices – all of which make it easier for unauthorised access to the network.

If cyber criminals do gain access to a network, this leaves a business open for exploitation. One of the primary ways to do this is through targeted emails, or 'spear phishing', reported as the main cyber security incidents experienced.

Another interesting finding was that the main motivation for a cyber attack was deemed to be a competitor seeking commercial advantage. This aligns with the cyber threat of most concern to businesses, which is theft or breach of confidential information or intellectual property.

One finding of potential concern is that businesses reported no compromises of mobile devices. Yet recent reports from leading IT security companies state there has been a large increase in mobile malware attacks.

I encourage all businesses to read this report, note the range of vulnerabilities identified, and address the areas for improvement.

I would also like to thank the businesses that took the time to respond to the survey – it takes a partnership approach between business and government to boost Australia's cyber resilience.

Dr Carolyn Patteson
Executive Manager, CERT Australia

ISBN: 978-1-925118-22-3

Use of the Coat of Arms

The terms under which the Coat of Arms can be used are detailed on the It's an Honour website (www.itsanhonour.gov.au).

Contact us

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

Commercial and Administrative Law Branch
Attorney-General's Department
3–5 National Cct
BARTON ACT 2600
Call: 02 6141 6666

Email: copyright@ag.gov.au

CONTENTS

THE 2013 CERT AUSTRALIA CYBER CRIME AND SECURITY SURVEY WAS DESIGNED AND CONDUCTED TO OBTAIN A BETTER UNDERSTANDING OF HOW CYBER INCIDENTS ARE AFFECTING THE BUSINESSES THAT PARTNER WITH CERT AUSTRALIA

These are the businesses that form part of Australia's systems of national interest, including critical infrastructure. They underpin the social and economic wellbeing of the nation and deliver essential services, including banking and finance, communications, energy, resources, transport and water.

The findings from this survey build on the baseline data from the *2012 CERT Australia Cyber Crime and Security Survey*. The findings provide a more comprehensive picture of the current cyber security measures businesses have in place, the recent cyber incidents they have identified, their reporting of them, and their concerns about cyber threats.

The findings also identify potential vulnerabilities and areas where organisations can make improvements to strengthen their cyber resilience.

Responses were received from 135 partner businesses. Importantly, they are continuing to take cyber security seriously. This is essential for individual businesses and their clients, as well as the industry sector, and the business community more broadly.

Overall, organisations have good cyber security measures in place, including policies and standards, as well as a range of technologies and mitigation strategies. Of note, 79% of organisations report they are implementing the *Top 4* mitigation strategies released by the Australian Signals Directorate (ASD). However, the use of application whitelisting (one of the *Top 4*) as a mitigation strategy is relatively low.

It is important that strong cyber security measures are in place, as there has been an overall increase in the number of cyber security incidents identified by organisations – from 56 organisations in 2012 to 76 organisations in 2013.

Most of the incidents were in the form of targeted emails, followed by virus or worm infection and trojan or rootkit malware. This is consistent with the finding that respondents viewed cyber security incidents to be targeted at their organisation, rather than random or indiscriminate.

Of concern, 61% of organisations do not have cyber security incidents identified on their risk register. This may be linked with the identified need for management and CEOs to improve their IT security skills and practices – and perhaps awareness.

Of note, the number of organisations that chose not to report cyber security incidents to an outside agency has increased – from 44% in 2012 to 57% in 2013.

Responses 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.

This finding reinforces the need for CERT Australia and other agencies to actively promote the benefits of reporting cyber security incidents.

> IMPORTANTLY, BUSINESS IS TAKING CYBER SECURITY SERIOUSLY

KEY FINDINGS

Findings from the survey reveal a range of concerns and potential vulnerabilities

- 61% of organisations do not have cyber security incidents identified in their risk register
- 13% of organisations using Windows XP did not have plans to migrate to other software before April 2014
- only 27% of organisations had increased expenditure on IT security in the previous 12 months – a decrease of 25% from 2012
- 16% of organisations have no staff dedicated to IT security, and the majority (72%) of large organisations (200+ employees) only have small IT security areas (1-5 full time staff)
- 42% of organisations with a physical presence in other countries do not consider the internationally connected networks within their organisational IT security posture.

Areas for improvement have also been identified

- 95% of respondents think general staff need to improve their IT security skills and/or practices
- 91% of respondents think management need to improve their IT security skills and/or practices
- more than 60% of respondents think IT staff, the CEO and the board of directors need to improve their IT security skills and/or practices
- the main internal factors that contributed to cyber security incidents were staff errors and/or omissions (57%) and poor security culture (50%)
- the main external factors that contributed to cyber security incidents were targeted attack (51%) and third party risks and/or vulnerabilities (49%).

TRENDS – 2012 TO 2013

The following table provides the survey findings from 2012 and 2013 that are directly measurable. These findings are referenced throughout this report.

Finding	2012	2013	change
Number of organisations that identified cyber security incidents on their networks	22%	56%	↑ of 34%
Number of organisations that increased expenditure on IT security	52%	27%	↓ of 25%
Number of organisations applying IT security standards & frameworks	64%	83%	↑ of 19%
Number of organisations using the standard ISO 27001	50%	83%	↑ of 33%
Number of organisations using the standard PCI DDS	20%	42%	↑ of 22%
Number of organisations using cryptographic controls	25%	60%	↑ of 35%
Number of organisations with a forensic plan in place	12%	25%	↑ of 13%
Number of IT security staff with vendor certifications	50%	60%	↑ of 10%
Number of IT security staff with at least five years' experience working in IT security	35%	79%	↑ of 44%
Percentage of respondents who identified the need for general staff to improve their IT security skills &/or practices	70%	95%	↑ of 25%
Percentage of respondents who identified the need for management to improve their IT security skills &/or practices	70%	91%	↑ of 21%
Percentage of respondents who identified the need for boards of directors to improve their IT security skills &/or practices	48%	62%	↑ of 14%
Number of organisations not reporting cyber security incidents to an outside agency	44%	57%	↑ of 13%

THE 2013 CYBER CRIME AND SECURITY SURVEY WAS CONDUCTED BY AUSTRALIA'S NATIONAL COMPUTER EMERGENCY RESPONSE TEAM, CERT AUSTRALIA (THE CERT)

The CERT is the primary point of contact in the Australian Government for cyber security issues affecting major Australian businesses.

The CERT is part of the Commonwealth Attorney-General's Department, with offices in Canberra and Brisbane. It is a trusted source of information and advice on cyber security issues. It is not a regulator, its services are free, and it does not compete with commercial services in the market.

The CERT also works in the Cyber Security Operations Centre, sharing information and working closely with the Australian Security Intelligence Organisation, the Australian Federal Police, and the Australian Signals Directorate.

In addition, it is part of the global network of CERTs in both business and government, and leverages those relationships to protect Australian business.

These partnerships with government agencies and international counterparts mean the CERT is very well connected and informed, so it is best placed to help businesses protect themselves from cyber attacks.

From late 2014, CERT Australia will be co-located within the Australian Cyber Security Centre with other operational cyber security agencies.

One of the challenges the CERT faces is gaining a better understanding of the impact of malicious online activity and how well businesses are placed to respond.

While there are an increasing number of cyber crime and security incidents, the true extent of these threats is difficult to determine.

To help understand what is happening on this front, the inaugural *CERT Australia Cyber Crime and Security Survey* was conducted in 2012.

As the cyber picture is constantly changing, the CERT is conducting annual national surveys to look for trends over time. This assists the Australian Government to develop an informed understanding about cyber security issues affecting the nation.

THE 2013 SURVEY aims to build on the baseline findings from 2012 and form a more comprehensive understanding of how cyber incidents are affecting the businesses that partner with the CERT.

In line with the 2012 survey, the 2013 survey aims to gain a picture of the

- business – general description
- current cyber security measures in place
- recent cyber security incidents identified, and
- reporting of cyber security incidents.

Additional questions were included in the 2013 survey to gain a more comprehensive understanding of each of the above categories. Further, the 2013 survey seeks to understand business concerns about cyber threats.

The survey was produced and conducted by the CERT and was hosted online by WebSurvey. It consisted of 26 questions, both closed and open ended.

To ensure the most accurate and informed responses were obtained, questions were asked to be completed by the Chief Information Officer and/or an IT security officer in each organisation.

Respondents were assured that all answers are anonymous.

> CERT AUSTRALIA IS GAINING A BETTER UNDERSTANDING OF THE IMPACT OF MALICIOUS ONLINE ACTIVITY

INDUSTRY SECTOR

Responses were received from 135 organisations, from more than 12 industry sectors. The greatest representation was from defence (24%), followed by energy (16%), banking and finance (13%), government (12%), and other (11%).

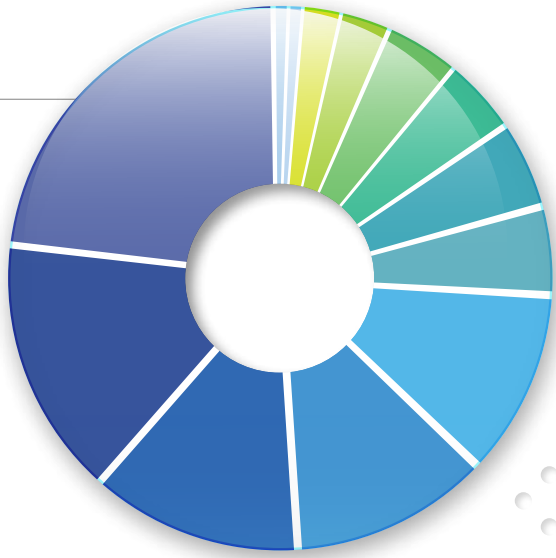
NOTE

- 'defence' refers to defence contractors or members of the defence industry security program (DISP)
- 'government' refers mostly to government-business enterprises (ie critical infrastructure), and
- 'other' includes businesses in legal services, airport management, gaming/ media and entertainment, and software development.

Figure 1 provides a breakdown of the sectors that responded to the survey.

FIGURE 1

DEFENCE	23%
ENERGY	16%
BANKING & FINANCE	13%
GOVERNMENT	12%
OTHER	11%
MANUFACTURING	5%
COMMUNICATIONS	5%
WATER	4%
MINING RESOURCES	4%
TRANSPORT	3%
HEALTH	2%
FOOD	1%
RETAIL	1%



CONTRACT TO GOVERNMENT

Around half the responding organisations (56%) contract or provide services to government. These organisations may therefore be responsible for protecting their own information and government information.

SIZE OF THE BUSINESS

Most respondents (74%) were from large organisations (200+ employees), with 20% being from medium sized organisations (20 – 200 employees), and 6% being from small organisations (less than 20 employees).

> RESPONDENTS ARE AWARE OF THE NEED FOR IT SECURITY STAFF TO KEEP THEIR SKILLS AND KNOWLEDGE UP TO DATE

CYBER SECURITY INVOLVES THE PREVENTION AND DETECTION OF THE UNAUTHORISED ACCESS, USE OR IMPAIRMENT OF AN ORGANISATION'S NETWORK DATA OR SYSTEMS

To maximise cyber resilience, modern organisations layer security defences for their IT systems to reduce the chance of a successful attack. This concept is known as defence-in-depth and seeks to manage risk with multiple defensive strategies, so that if one layer of defence turns out to be inadequate, another layer will hopefully prevent a full breach.

The multiple defence mechanisms layered across an organisation's network infrastructure protect data, networks, and users. A well-designed and implemented defence-in-depth strategy can help system administrators identify internal and external attacks on a computer system or network.

IT SECURITY AREA

Results indicate that 84% of responding organisations have IT security areas. Of those, 89% have internal IT security teams, and 11% outsource their IT security.

Whether internal or outsourced, 74% of the IT security areas are reportedly small (1 -5 full time equivalent staff), 5% are medium (5 – 15 full time equivalent staff) and 5% are large (15+ full time equivalent staff).

Of concern, 16% of respondents reported their organisation did not have an IT security area – with no staff dedicated to this role.

Also of note, most of the large organisations (72%) have small IT security areas.

INTERNATIONAL PRESENCE

Findings indicate that 65% of responding organisations are based solely in Australia, while 35% have a physical presence in other countries.

Of those with a physical presence in other countries, 42% do not consider the internationally connected networks as part of their IT security posture.

This finding is of concern, as all organisations with a physical presence and IT network in other countries need to consider internationally connected networks as part of their IT security posture.

IT SECURITY POLICIES

Organisations were asked what type of IT security policies they use.

Results indicate that basic security policies are being applied by the majority of surveyed organisations.

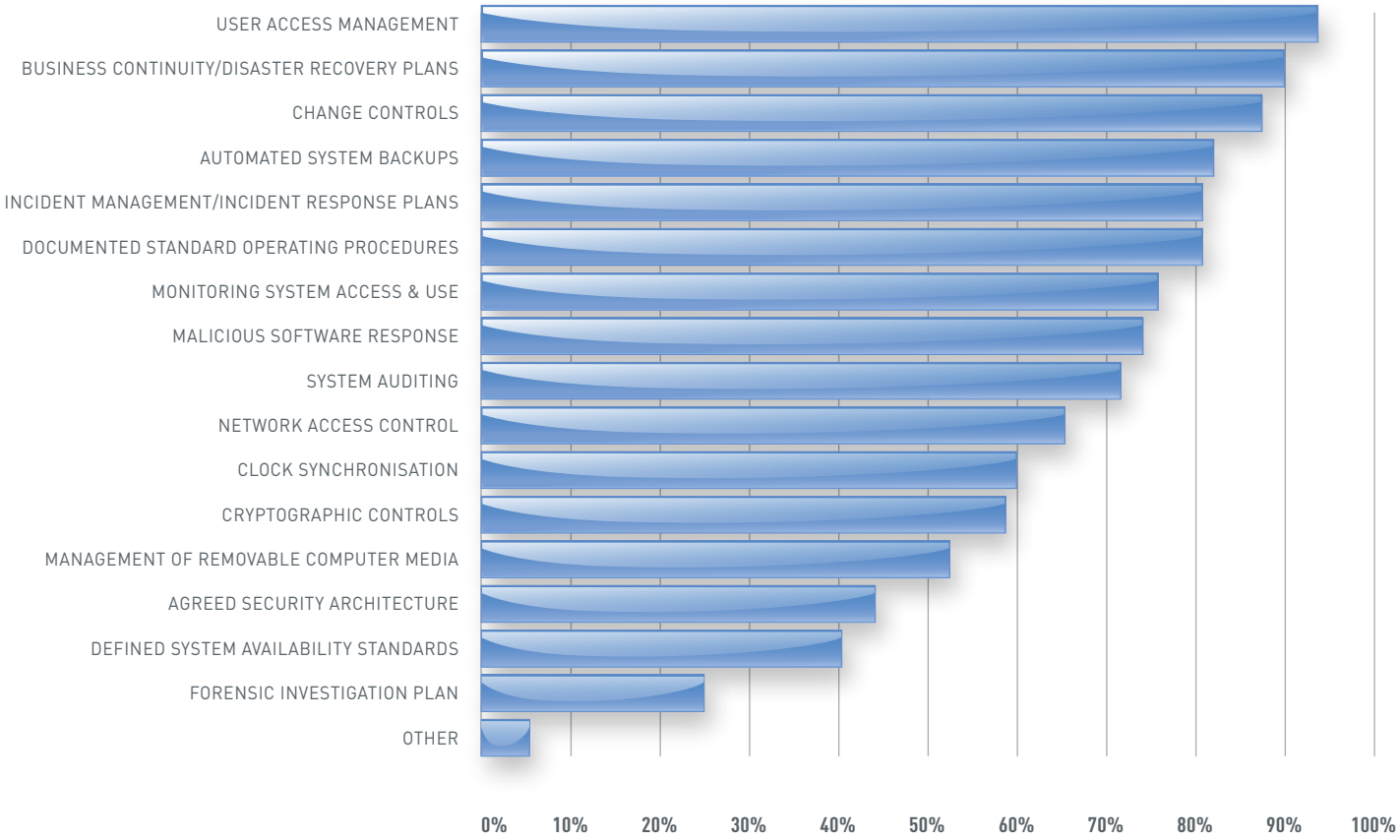
For example, 94% deploy user access management, 90% have business continuity/disaster recovery plans, 87% use change control, 82% have automated system backups, 81% have documented standard operating procedures, and 81% have an incident management or response plan.

While the majority of organisations report they have these security policies, there are also areas for improvement. For example, less than 60% of respondents use cryptographic controls, and around 50% of respondents have plans in place for the management of removable computer media, such as USB memory drives.

In addition, only 25% of respondents reported having a forensic investigation plan. These plans help monitor use of the IT systems, provide mechanisms to recover lost data, and provide ways to protect information on systems.

Figure 2 provides a breakdown of security policies being used by responding organisations.

FIGURE 2 – breakdown of security policies being used



COMPARISON WITH THE 2012 CYBER CRIME AND SECURITY SURVEY RESULTS

The 2013 findings are similar to those of the 2012 survey.

In 2012, the majority of organisations reported applying basic security policies. These included user access management, system backups, documented standard operating procedures and external network access control.

In 2012, the areas for improvement also included having plans in place for the management of removable computer media, using cryptographic controls and having a forensic plan.

Comparison of results does indicate some improvement in the application of IT security policies, with an increase in the number of organisations using cryptographic controls (from 25% in 2012 to 60% in 2013) and having a forensic plan in place (from 12% in 2012 to 25% in 2013).

IT SECURITY STANDARDS

When asked if their organisation uses external IT security standards or frameworks

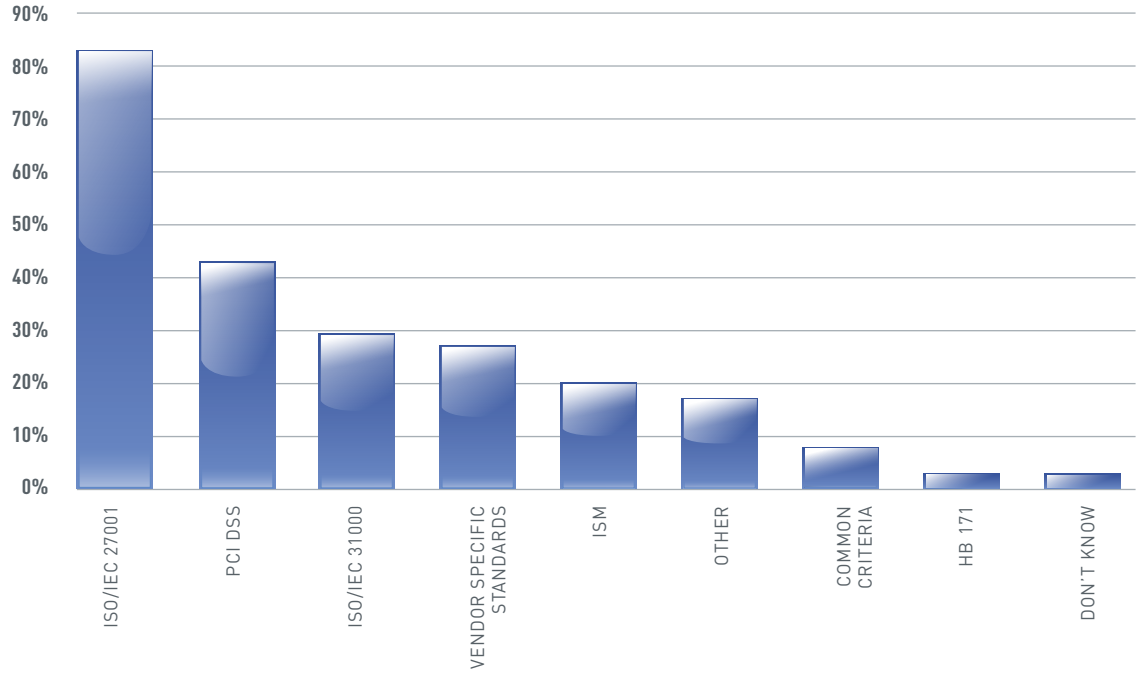
- 83% of respondents reported 'yes'
- 13% of respondents reported 'no'
- 4% of respondents reported they 'did not know'.

Of the organisations that use external IT security standards or frameworks, most use ISO/IEC 27001 (83%), followed by PCI DSS[1] (42%), ISO/IEC 3100 (29%) and vendor specific standards (27%).

Figure 3 provides a breakdown of the external standards being used by responding organisations.

[1]This is the IT security standard commonly used by organisations using credit card data.

FIGURE 3 – breakdown of external standards being used



COMPARISON WITH THE 2012 CYBER CRIME AND SECURITY SURVEY RESULTS

The 2013 findings differ in some respects from those of the 2012 survey.

Comparison of results indicates an increase in the application of IT security standards and frameworks.

There has been an overall increase in the number of organisations applying IT security standards (from 64% in 2012 to 83% in 2013), and a decrease in the number of organisations that do not apply IT security standards (from 25% in 2012 to 13% in 2013).

Specifically, there has been an increase in the number of organisations using ISO 27001 – from 50% in 2012 to 83% in 2013. This standard states it is mandatory for management to examine their organisation's IT security risks to form a risk mitigation system, and to ensure that the controls applied are current for the needs of the business.

The number of organisations adhering to the Payment Card Industry Data Security Standard (PCI DDS) has also increased – from 20% in 2012 to 42% in 2013.

RISK REGISTER

When asked if the threat factor of cyber security incidents had been identified in their organisation's risk register

- 39% of respondents reported 'yes'
- 61% of respondents reported 'no'.

This finding is of concern and indicates an area for improvement, as all organisations should factor the risk of a cyber security incident into their business continuity planning.

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 a better understanding of the threat landscape, so they can develop stronger mitigation strategies to protect their systems.

Management within organisations also need to ensure that, to be truly resilient in relation to the spectrum of risks that could affect their organisation, cyber security incidents have been factored into the risk register, and appropriate measures are taken to mitigate those risks.

IT SECURITY TECHNOLOGIES

Organisations were asked what type of IT security technologies they use.

More than 90% of respondents reported using anti-spam filters, anti-virus software, traditional firewalls (network based), physical access control, email attachment filtering, remote access VPNs, and operating system patch management.

More than 80% reported using password complexity rules, digital certificates, and web filtering/ content inspection.

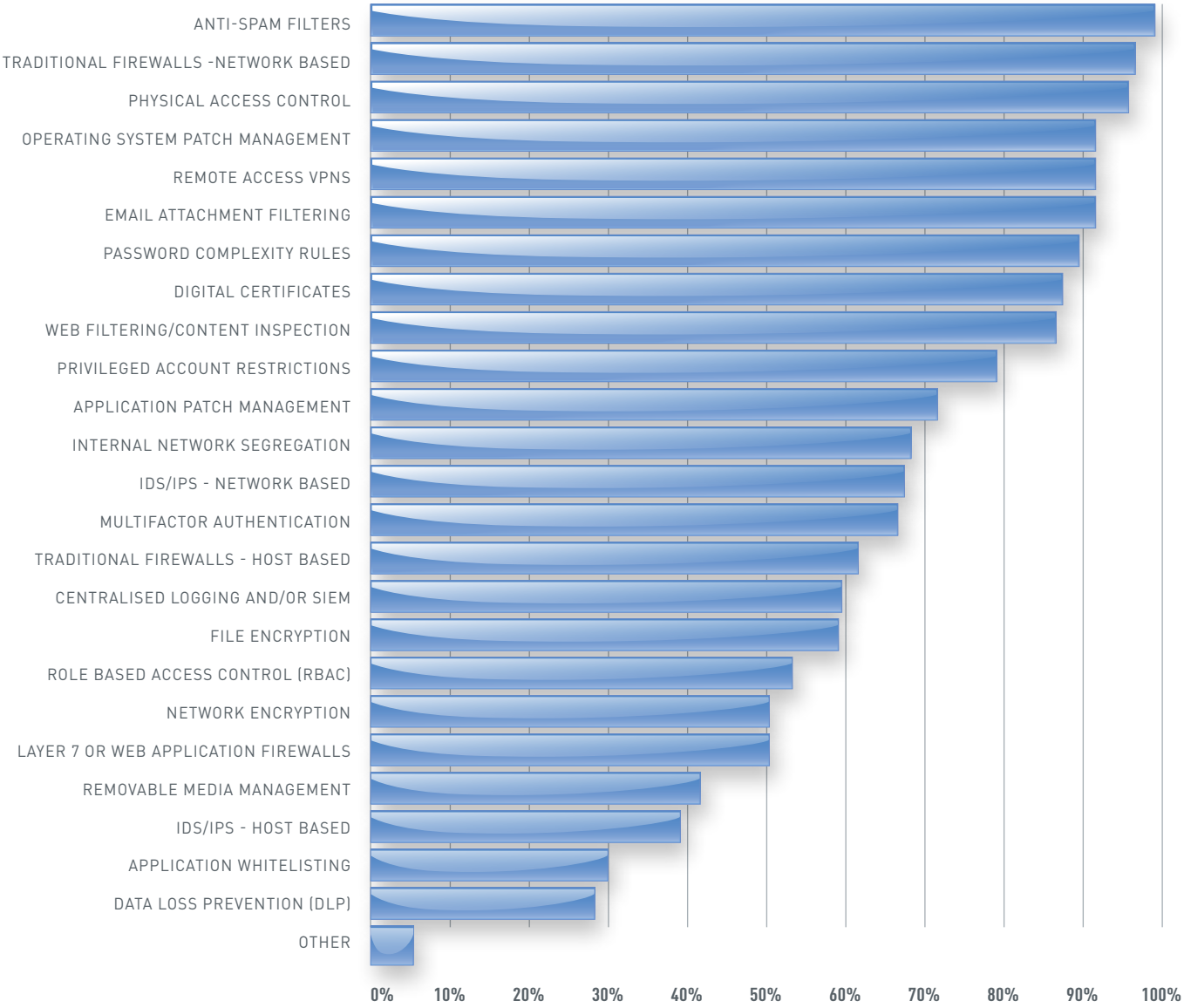
More than 70% reported using privileged account restrictions, and application patch management.

More than 60% also reported using internal network segregation, IDS/IPS (network based), multifactor authentication (such as smart cards, tokens, biometrics), and traditional firewalls (host based).

Only 30% of respondents reported using application whitelisting (one of the *Top 4* mitigation strategies). As ASD states, implementing application whitelisting across an entire organisation can be daunting. As a first step, ASD recommends deployment to high-value and often targeted employees such as executive officers and their assistants.

Figure 4 provides a breakdown of the IT security technologies being used by responding organisations.

FIGURE 4 – breakdown of IT security technologies being used



COMPARISON WITH THE 2012 CYBER CRIME AND SECURITY SURVEY RESULT

The 2013 findings are similar to those of the 2012 survey.

For example, in 2012 more than 90% of responding organisations also reported using antivirus software, spam filters and firewalls. More than 80% also reported using access control and virtual private networks.

While many organisations are using a range of IT security technologies, results from both 2012 and 2013 indicate that some organisations need to strengthen their IT security by adopting a defence-in-depth approach.

IT SECURITY SKILLS AND TRAINING

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

Responses indicate that 79% of organisations have IT security staff with at least five years' experience working in IT security.

More than 65% of organisations have IT security staff with tertiary level IT qualifications.

Around 60% of organisations have IT security staff with either vendor certifications, vendor neutral certifications or who have participated in ad hoc courses.

Findings indicate that 7% of organisations have IT security staff with no form of IT security training or qualification.

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

- 95% of respondents reported this need for general staff
- 91% of respondents reported this need for management
- 66% of respondents reported this need for IT staff
- 63% of respondents reported this need for the CEO
- 62% of respondents reported this need for the board of directors.

COMPARISON WITH THE 2012 CYBER CRIME AND SECURITY SURVEY RESULTS

The 2013 findings differ in some respects from those of the 2012 survey.

Comparison of results indicates an improvement in the IT security skills of IT security staff.

For example, there has been an increase in the number of IT security staff with vendor certifications (from 50% in 2012 to 60% in 2013) and at least five years' experience working in IT security (from 35% in 2012 to 79% in 2013).

However, these results also indicate that some organisations still need to improve the skill set of their IT security staff.

Comparison of results also indicates an increased need for all staff in organisations to improve their IT security skills and/or practices.

For example, an increase in this need was identified for general staff (from 70% in 2012 to 95% in 2013), management (from 70% in 2012 to 91% in 2013), and the board of directors (from 48% in 2012 to 62% in 2013).

Of note, the 2013 survey also asked and identified this need for IT staff and CEOs.

IT SECURITY EXPENDITURE

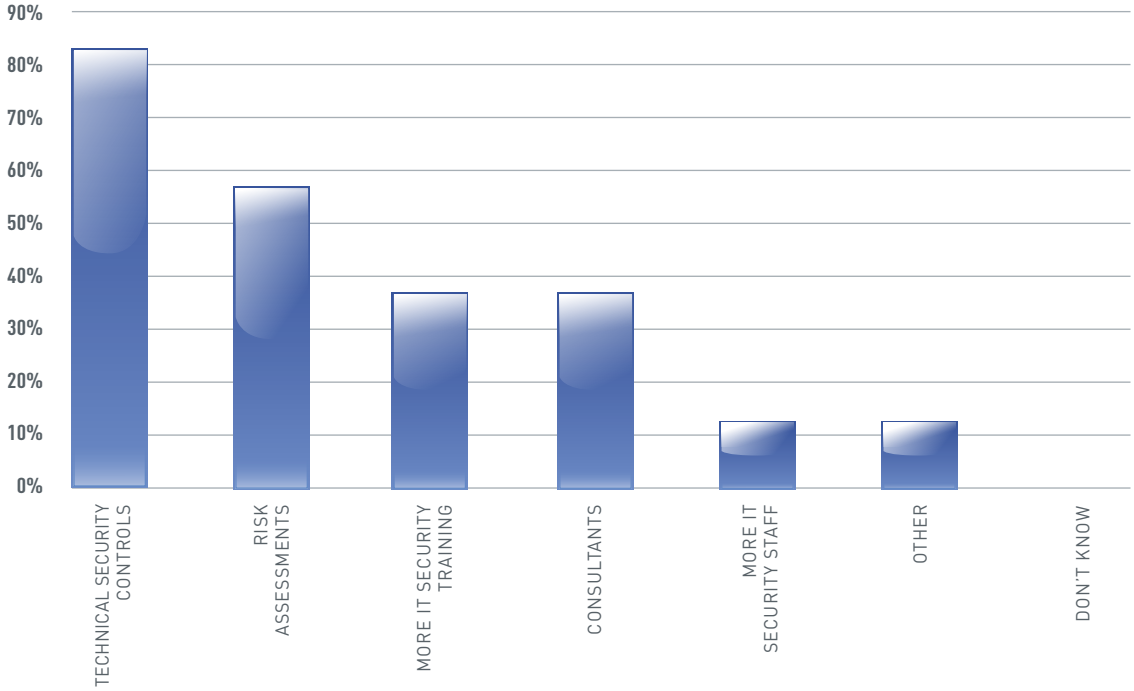
When asked if their organisation had increased expenditure on IT security in the previous 12 months

- 73% of respondents reported 'no'
- 27% of respondents reported 'yes'.

Of those organisations that had increased expenditure on IT security, the majority was on technical security controls (87%), followed by risk assessments (56%). Expenditure was also made on IT security training (38%), consultants (38%) and additional IT security staff (13%).

Figure 5 provides a breakdown of expenditure on IT security.

FIGURE 5 – breakdown of expenditure on IT security



COMPARISON WITH THE 2012 CYBER CRIME AND SECURITY SURVEY RESULTS

The 2013 findings differ from those of the 2012 survey.

Of concern, results indicate a large decrease in expenditure on IT security.

The number of organisations that increased expenditure on IT security decreased from 52% in 2012 to 27% in 2013.

Similarly, the number of organisations that did not increase expenditure increased from 42% in 2012 to 73% in 2013.

The 2013 survey also asked how expenditure was increased, identifying it was mostly on technical security controls (87%).

AUSTRALIAN SIGNALS DIRECTORATE'S TOP 4 STRATEGIES

Respondents were asked if the IT security staff in their organisation are aware of the *Top 4* of the *35 strategies for mitigating cyber intrusions*, released by ASD

- 79% of respondents reported 'yes'
- 16% of respondents reported 'no'
- 5% of respondents reported 'don't know'.

Importantly, results also indicate that respondents who are aware of the *Top 4*, are implementing these mitigation strategies

- 100% patch operating system vulnerabilities
- 98% minimise the number of users with administrative privileges
- 93% patch applications
- 23% use application whitelisting.

The *Top 4* are mandatory for Australian Government agencies, and CERT Australia also advises businesses to use the strategies.

The findings indicate that few organisations use application whitelisting as a mitigation strategy. This is consistent with the finding that only 30% of respondents reported using application whitelisting as a type of IT security technology.

As noted earlier, implementing application whitelisting across an entire organisation can be daunting – but it has significant benefits. As a first step, ASD recommends deployment to high-value and often targeted employees such as executive officers and their assistants.

WINDOWS XP – END OF LIFE

When asked if their organisation uses Windows XP

- 47% of respondents reported 'yes'
- 52% of respondents reported 'no'
- 1% of respondents reported 'don't know'.

When asked if their organisation is aware that technical assistance for Windows XP would no longer be freely available after 8 April 2014

- 97% of respondents reported 'yes'
- 2% of respondents reported 'no'
- 1% of respondents reported 'don't know'.

Of the organisations using Windows XP, the majority (79%) planned to migrate to other software before April 2014.

Of concern, 13% of the organisations using Windows XP did not have plans to migrate to other software before April 2014, and 8% didn't know if their organisation had such IT security plans in place.

Organisations that still use Windows XP after 8 April 2014 are at an increased risk of network vulnerability and compromise, as the software is no longer being supported or patched.

Anecdotal reports indicate that cyber criminals have been 'stockpiling' new XP attacks, waiting for support to end.

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 attacks, as well as why the attacks 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.

NUMBER OF INCIDENTS

Respondents were asked if any cyber security incidents had been identified on their networks in the previous 12 months.

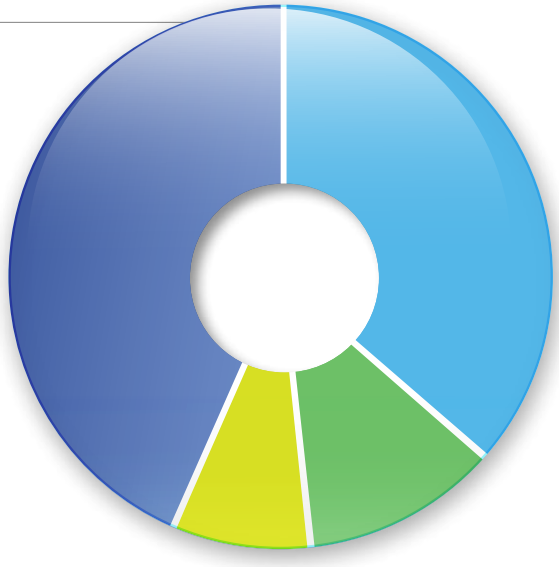
Results indicate that 56% of organisations did identify one or more cyber security incident in the previous 12 months, while 44% did not.

This finding may reflect that a number of cyber intrusions have gone undetected by some organisations, or that their definition of an incident is different. Anecdotal evidence available to the CERT suggests that some businesses are unaware of the full scope of unauthorised activity on their networks.

Figure 6 provides a breakdown of the number of cyber security incidents identified by organisations in the previous 12 months.

FIGURE 6

1 TO 5	35%
6 TO 10	12%
MORE THAN 10	9%
NONE	44%



COMPARISON WITH THE 2012 CYBER CRIME AND SECURITY SURVEY RESULTS

The 2013 findings differ from those of the 2012 survey.

Results indicate an overall increase in the number of cyber security incidents identified by organisations – from 56 organisations in 2012 to 76 organisations in 2013.

This result may indicate an increased awareness or improvement in the ability of organisations to detect cyber intrusions. It may also indicate a preference for organisations to anonymously report experiencing cyber security incidents, such as through this survey.

TYPES OF INCIDENTS

Of the respondents who reported their organisation had identified cyber security incidents in the previous 12 months, they assessed the main types were

- 63% - targeted emails
- 52% - virus or worm infection
- 46% - trojan or rootkit malware
- 35% - theft of mobile devices
- 26% - unauthorised access
- 17% - ransomware
- 17% - distributed denial of service
- 17% - unauthorised access to information from an insider.

These findings may help organisations decide where to place additional resources to protect their information assets.

Interestingly, the main incident identified was targeted emails. These are socially engineered emails that are designed to assist an adversary in gaining a foothold on a network undetected, to extract valuable company or client information.

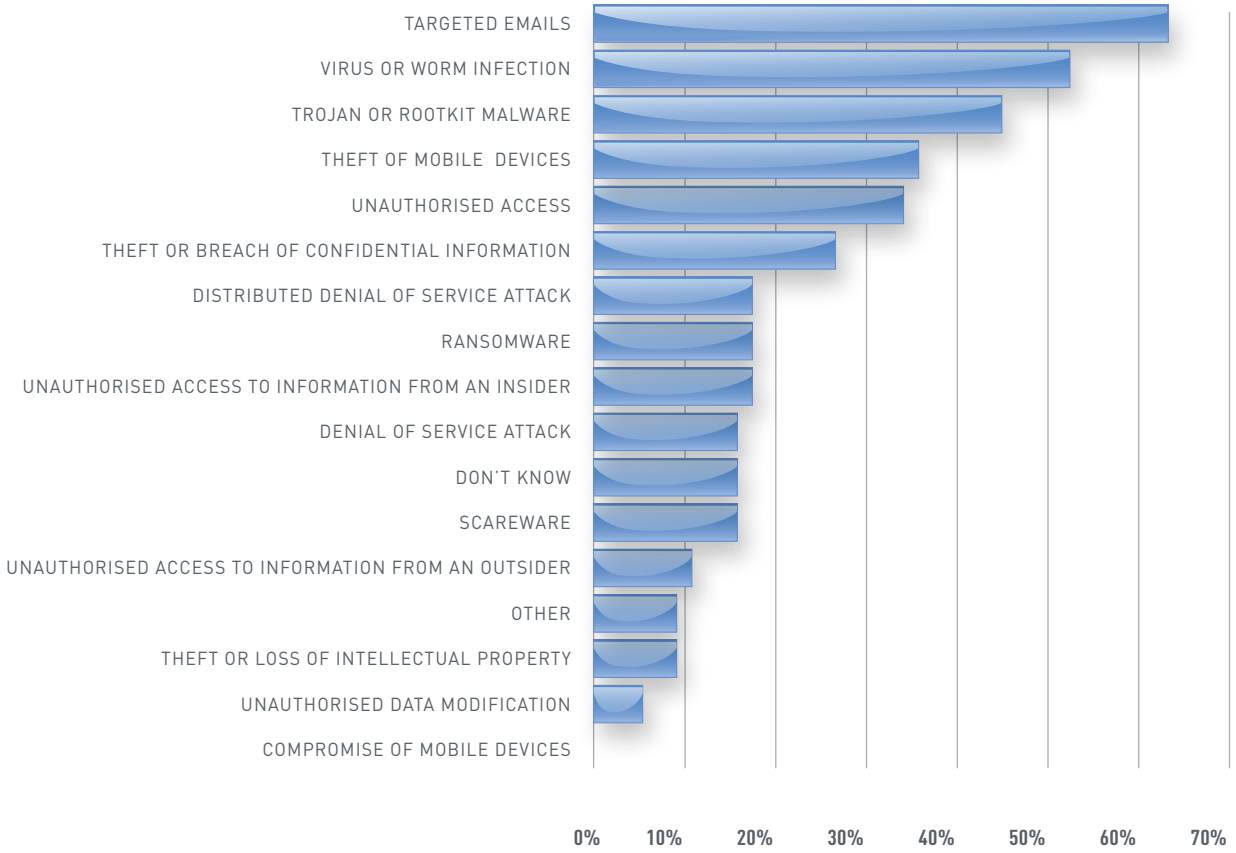
Such 'spear phishing' emails appear to be from a known source – but the links and attached files are designed to by-pass security and create an entry point onto a network.

This method is particularly effective in organisations where cyber resilience is not part of the culture – providing a timely reminder that all staff have a role to play in cyber security.

Also of interest – and concern – is that there were no reports of mobile devices being compromised – yet, recent reports from leading IT security companies state there has been a large increase in mobile malware attacks.

Figure 7 provides a breakdown of the type of cyber security incidents identified by organisations in the previous 12 months.

FIGURE 7 – breakdown of the type of cyber security incidents



COMPARISON WITH THE 2012 CYBER CRIME AND SECURITY SURVEY RESULTS

The 2013 findings are similar to those of the 2012 survey.

In 2012, the main types of incidents identified also included theft of a notebook, tablet or mobile devices, virus or worm infection, trojan or rootkit malware, unauthorised access and denial of service attack.

The 2012 survey did not identify or list 'targeted emails' as a type of incident.

CASE STUDY – COMPROMISED WEBSITES

CERT Australia regularly provides a range of Australian businesses with assistance in cleaning up compromised websites.

It is common for malicious individuals to compromise legitimate websites to facilitate cyber crime.

The compromises are often invisible to users, yet remain harmful to anyone viewing the page, including the owner of the website.

For example, a hacker may infect a website with obfuscated or disguised code, which can download and install malware that records keystrokes on visitors' computers. The hacker can then steal credit card numbers or login credentials for their email accounts, online banking and cloud services.

The owner of a website is responsible for keeping it clean of malware. However, not all website owners are equipped with the technical knowledge and skill to keep their websites secure.

For example in late 2013, CERT Australia contacted a registered domain owner, to report that a small business website had been compromised by malware.

CASE STUDY – COMPROMISED WEBSITES *CONTINUED*

Malware (malicious software) is used to disrupt computer operation, gather sensitive information, or gain access to computer systems. It typically includes viruses, worms, spyware, and trojan horses.

Unsure of how to remediate the website, the domain owner contacted the CERT Australia hotline to discuss the issue and seek further advice.

One of CERT Australia's technical advisors provided guidance on how to detect malicious content on the website, and also a step-by-step action plan on how to clean the website.

This case study highlights how CERT Australia assists Australian businesses in keeping their websites clean and secure, which helps protect the business, its customers and any visitors to the site.

APPARENT MOTIVES OF INCIDENTS

Attribution is always difficult. Where respondents think an attack may have come from, may not be where it actually originated.

Many respondents indicated they did not know the origin of the cyber security incidents experienced. Others attributed the incidents to internal factors such as staff errors and/or omissions and a poor security culture, as well as external factors such as targeted emails.

Respondents who reported their organisation had experienced cyber security incidents in the previous 12 months were asked about the apparent motives or reasons for the attacks.

In priority order, the main apparent motives were

- competitor seeking commercial advantage
- malicious damage
- using the system for further attacks
- personal grievance
- issue motivated/hacktivism
- other (including carelessness, lack of attention and negligence)
- don't know
- illicit financial gain
- random or indiscriminate.

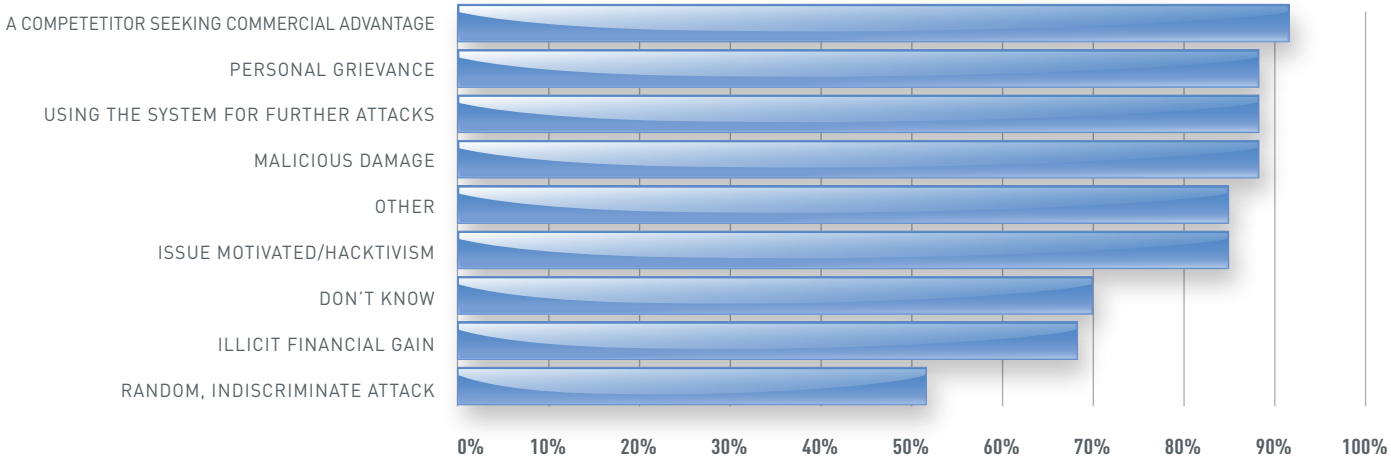
The main motive for attack – a competitor seeking commercial advantage – relates to the theft of intellectual property. There are a range of actors involved in this form of cyber crime – some benefit directly, while others sell the information.

Whatever the motive or reason for a cyber attack, it is important that an organisation understands enough about the incident to determine

- the vulnerabilities on their network
- what data may have been accessed, and
- what needs to be done to increase the protections of their network.

Figure 8 provides a breakdown of the apparent motives or reasons for the cyber security incidents experienced by organisations in the previous 12 months.

FIGURE 8 – breakdown of apparent motives for cyber security incidents



COMPARISON WITH THE 2012 CYBER CRIME AND SECURITY SURVEY RESULTS

The 2013 findings are similar to those of the 2012 survey.

In 2012, respondents also viewed cyber security incidents to be targeted at their organisation, indicating a shift from previous views or conceptions that most attacks are random or indiscriminate.

Whether targeted or random, building organisational resilience to cyber security incidents requires constant awareness and action.

> CERT AUSTRALIA ASSISTS AUSTRALIAN BUSINESSES IN KEEPING THEIR WEBSITES CLEAN AND SECURE

CONTRIBUTING FACTORS TO THE INCIDENTS

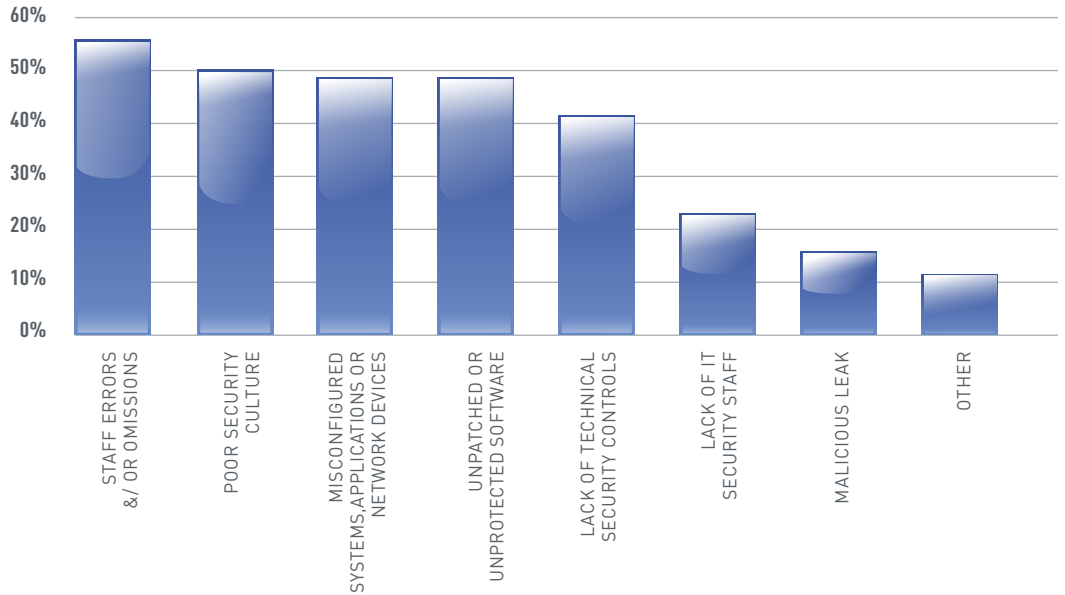
Respondents were asked what internal factors may have contributed to the cyber security incidents identified by their organisation in the previous 12 months.

The main factors were staff errors and/or omissions (57%), followed by poor security culture (50%), unpatched or unprotected software (48%) and misconfigured systems, applications or network devices (48%).

Lack of technical security controls (41%) and lack of IT security staff (22%) were also considered to be contributing factors.

Figure 9 provides a breakdown of the internal factors that may have contributed to the cyber security incidents experienced by organisations in the previous 12 months.

FIGURE 9 – breakdown of internal factors contributing to cyber security incidents

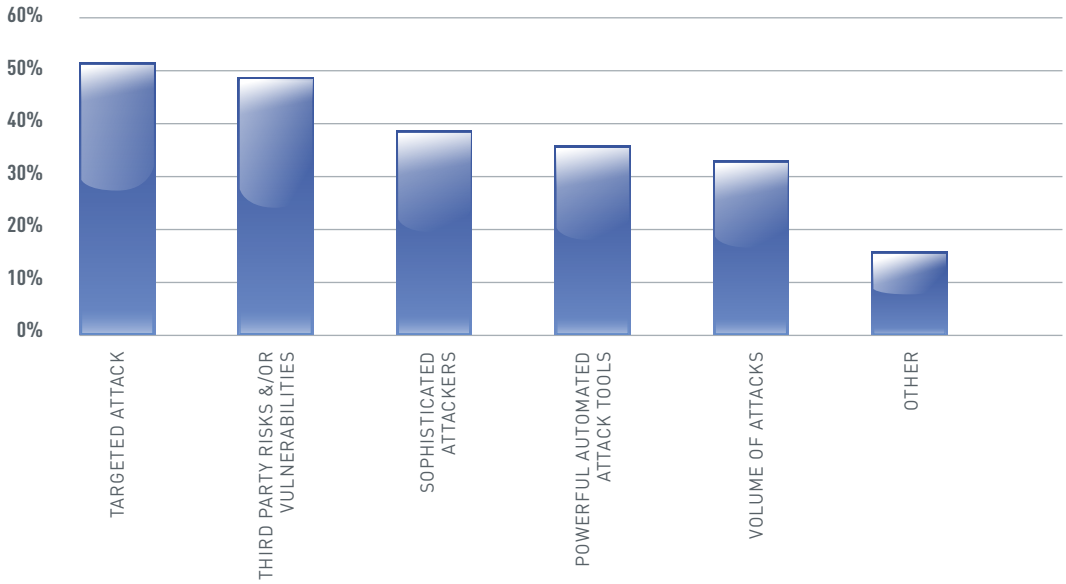


Respondents were also asked what external factors may have contributed to the cyber security incidents experienced by their organisation in the previous 12 months.

The main factors were targeted attack (51%), followed by third party risks and/or vulnerabilities (49%), sophisticated attackers (38%), powerful automated attack tools (36%) and volume of attacks (31%).

Figure 10 provides a breakdown of the external factors that may have contributed to the cyber security incidents experienced by organisations in the previous 12 months.

FIGURE 10 – breakdown of external factors contributing to cyber security incidents



COMPARISON WITH THE 2012 CYBER CRIME AND SECURITY SURVEY RESULTS

The 2013 findings are similar to those of the 2012 survey.

In 2012, the main contributing factors also included the use of powerful automated attack tools, unpatched or unprotected software, misconfigured systems, applications or network devices, sophisticated attackers, lack of technical security controls and poor security culture.

It is encouraging that businesses recognise both internal and external factors can contribute to cyber security incidents.

This highlights the need for organisations to have comprehensive cyber security measures in place and to look out for a range of vulnerabilities.

CASE STUDY – INTERNATIONAL ASSISTANCE

Early in 2014, CERT Australia was contacted by a large Australian financial institution, requesting assistance regarding three phishing websites.

While the websites looked to be authentic, they were fraudulent. They were set up (most likely by financially motivated cyber crime gangs) to look like the institution's website in order to steal customer login credentials (usernames and passwords).

Once criminals have valid login credentials, they can hack into accounts and transfer funds to other accounts. Many also sell the information to other cyber criminals.

Understandably, the financial institution was keen to have the phishing websites taken down.

As the sites were hosted in a foreign jurisdiction, the organisation required assistance from CERT Australia, which has strong links with its international counterparts.

CERT Australia confirmed that the phishing websites were still online and then contacted the national computer emergency response team in the foreign jurisdiction, requesting that the sites be taken down.

CASE STUDY – INTERNATIONAL ASSISTANCE *CONTINUED*

The foreign national CERT reported the phishing websites to the relevant internet service providers for action and remediation – and they were taken down.

This case study is a good example of how CERT Australia's international partnerships help protect Australian businesses.

As Australia's national computer emergency response team, CERT Australia participates in a number of international cyber security communities and has established cooperative agreements with a range of other national CERTS.

For example, CERT Australia has a direct working relationship with government, business and academic CERTS around the world, through the Forum for Incident Response and Security Teams (FIRST).

CERT Australia is also a member of the International Watch and Warning Network (IWWN) and the Asia Pacific CERT (APCERT) Organisation.

> CERT AUSTRALIA'S INTERNATIONAL PARTNERSHIPS HELP PROTECT AUSTRALIAN BUSINESSES

RESPONDENTS WHO STATED THEIR ORGANISATION HAD EXPERIENCED CYBER SECURITY INCIDENTS IN THE PREVIOUS 12 MONTHS (56% OF RESPONDING ORGANISATIONS) WERE ASKED ABOUT REPORTING THE INCIDENT

REPORTING OF INCIDENTS AND TO WHOM

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

Results indicate that 57% of respondents did not report cyber security incidents to any outside agency, and 9% did not know if the incidents were reported.

The remaining respondents (34%) did report cyber security incidents – to either CERT Australia and/or as mandatory reporting to a regulator, and/or to law enforcement.

FIGURE 11

REASONS FOR NOT REPORTING

Respondents who did not report cyber security incidents were asked why. The main reasons were

- 44% - 'there are no benefits of reporting'
- 44% - 'other'
- 20% - 'the attackers probably wouldn't get caught &/or prosecuted'
- 16% - 'did not know'
- 12% - 'negative publicity for the organisation'.

'Other' reasons for not reporting included that the incidents and the consequences were minor, and that the incidents were reported internally and managed by corporate policy.

COMPARISON WITH THE 2012 CYBER CRIME AND SECURITY SURVEY RESULTS

The 2013 findings are similar to those of the 2012 survey.

In 2012, just under half the respondents had not reported cyber security incidents. Their reasons also included there being no benefits of reporting, that the attacker probably wouldn't get caught and/or prosecuted, and that the incidents were minor.

Comparison of results indicates a decrease in the number of organisations reporting cyber security incidents to an outside agency – from 54% in 2012 to 34% in 2013.

These findings reinforce the need for the CERT and other agencies to actively promote the benefits of reporting cyber security incidents.

The CERT works on a partnership and trust basis with business, and encourages the voluntary and timely reporting of cyber security incidents. This allows the 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 the CERT is held in the strictest confidence.

To report an incident, phone the hotline 1300 172 400 or email **info@cert.gov.au**

The CERT has also produced a one page guide for business, on investigating cyber security incidents. It outlines the key considerations and actions that businesses need to take, if a cyber security incident is to be investigated by law enforcement.

The guide is available at **www.cert.gov.au/faq**

> THESE FINDINGS REINFORCE THE NEED FOR THE CERT AND OTHER AGENCIES TO ACTIVELY PROMOTE THE BENEFITS OF REPORTING CYBER SECURITY INCIDENTS.

ALL RESPONDENTS WERE ASKED A SERIES OF QUESTIONS ABOUT THE CYBER ACTORS AND THREATS OF MOST CONCERN TO THEIR ORGANISATION, AND THE RESPONSES TO CYBER THREATS THEY CONSIDER MOST IMPORTANT

This information aims to ascertain areas of future concern, to assist with understanding the trending of cyber security incidents.

This information will also help the CERT in providing the most valuable services and advice to business partners.

CYBER ACTORS OF MOST CONCERN

In terms of their organisation, respondents were asked which cyber actors concern them the most.

These are not necessarily the actors that have been involved in previous cyber security incidents – but are of future concern to organisations.

The main actors are

- 59% - issue motivated groups or hacktivists
- 54% - organised criminal syndicates
- 52% - trusted insiders
- 43% - individuals
- 42% - the intelligence services of some foreign governments
- 6% - other (included business competitors and disgruntled employees).

These findings indicate that issue motivated groups or hacktivists are of most concern.

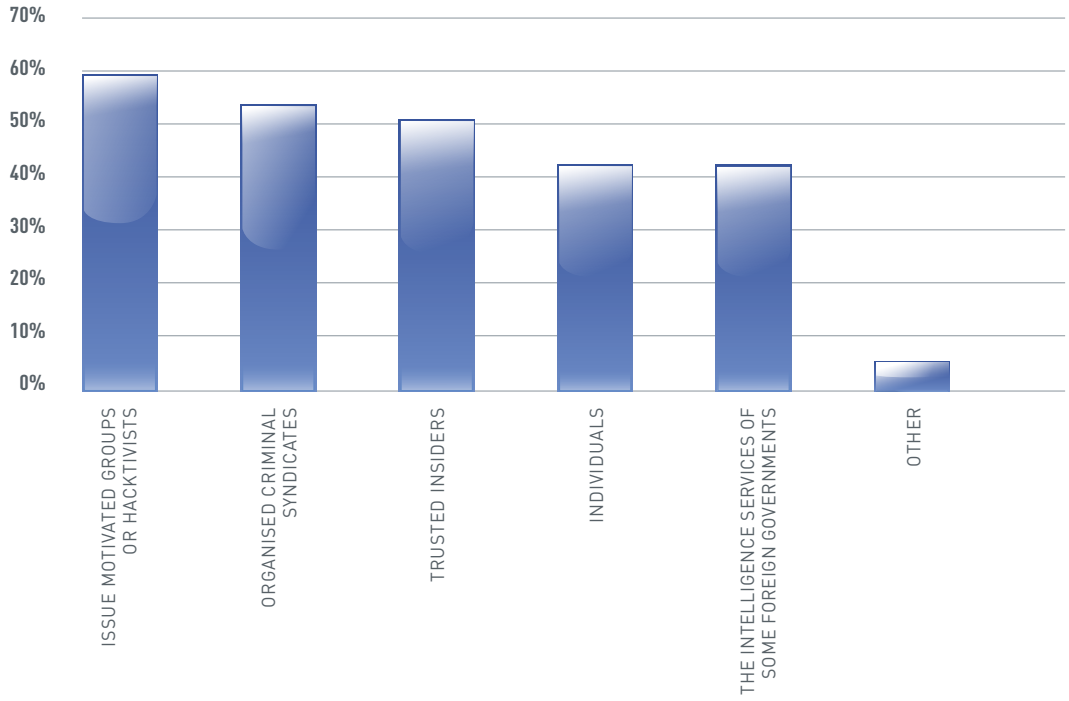
If targeting critical infrastructure, these actors could cause significant harm and disruption, not only to the organisation but to the broader social and economic wellbeing of the nation.

While traditional attacks by this category of cyber actors has involved defacement and distributed denial of service attacks, more recent activity has also involved domain name system (DNS) redirection.

Organised criminal syndicates and trusted insiders also rated highly as cyber actors of concern.

Figure 12 provides a breakdown of the cyber actors of most concern to organisations.

FIGURE 12 – breakdown of cyber actors of most concern



CYBER THREATS OF MOST CONCERN

In terms of their organisation, respondents were asked which cyber threats concern them the most.

The main threats are theft or breach of confidential information (68%), unauthorised access (67%), unauthorised access to information from an outsider (65%) and unauthorised access to information from an insider (51%).

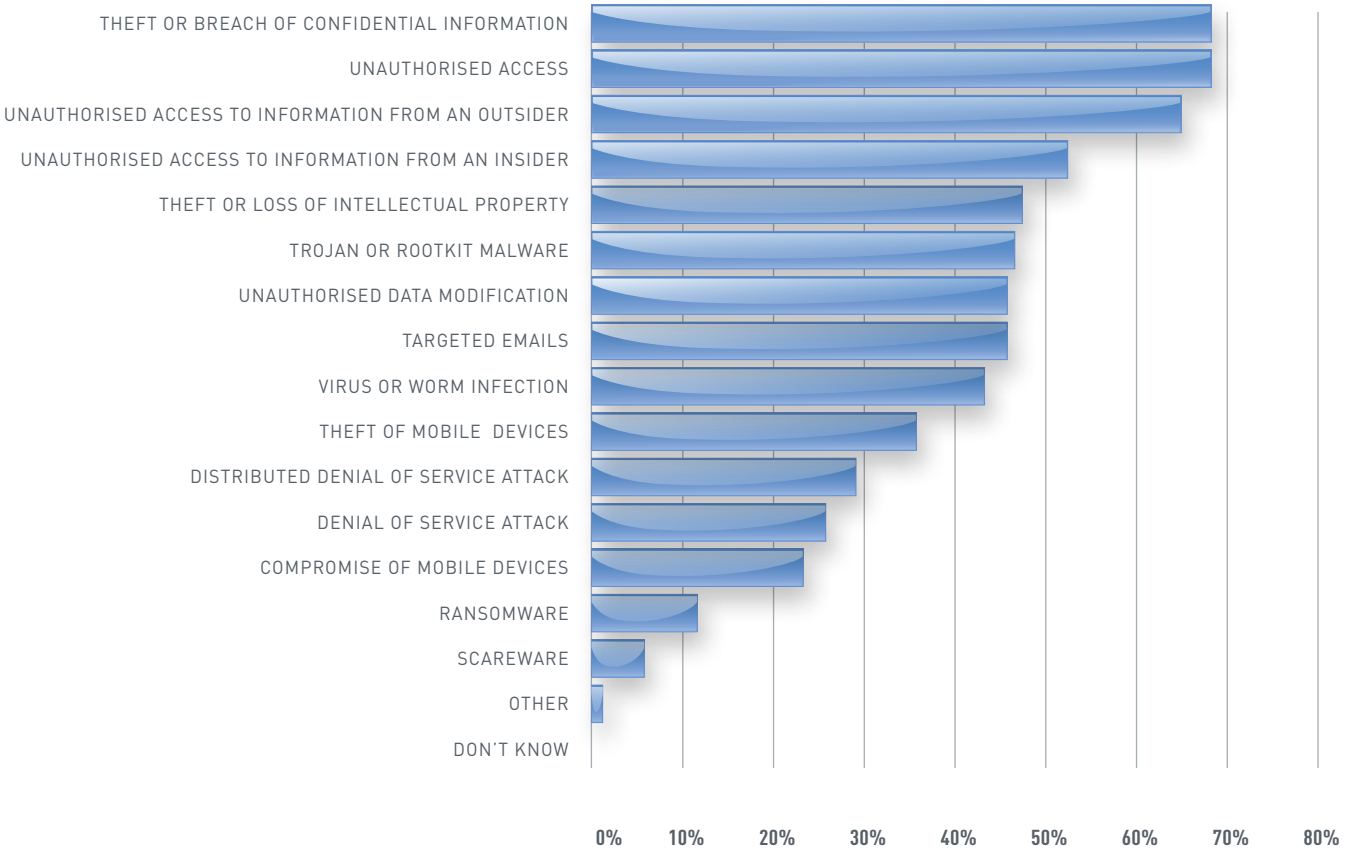
These threats are followed by theft or loss of intellectual property (48%), trojan or rootkit malware (47%), targeted emails (46%), unauthorised data modification (46%), virus or worm infection (43%) and theft of mobile devices (36%).

These findings indicate a range of cyber threats are of concern to organisations. Theft or breach of confidential information and unauthorised access to information – from both insiders and outsiders – appear to be of most concern.

Interestingly, targeted emails are of concern although perhaps not to the extent they should be, as findings from this survey indicate this was the main type of cyber security incident experienced by organisations. A successful targeted email is often the precursor to theft or breach of confidential information and a number of other listed consequences of cyber threats.

Figure 13 provides a breakdown of the cyber threats and consequences of most concern to organisations.

FIGURE 13 – breakdown of cyber threats of most concern



VULNERABLE PARTS OF ORGANISATIONS

Respondents were asked which parts of their organisation are most vulnerable to cyber threats.

The main vulnerability reported is the internal network (51%), followed by externally facing systems (45%), public website (43%), mobile devices being compromised (35%), remote access (34%), mobile devices being stolen (34%) and gateway environment (31%).

These vulnerabilities were followed by concerns about vulnerabilities in supervisory control and data acquisition (SCADA) systems (23%), partner networks (22%) and cloud (22%).

Findings indicate that protecting an organisation's internal network, or methods of accessing that network is of paramount importance to the majority of respondents.

An internal network may have a range of system vulnerabilities, such as weaknesses in authentication, unused and unpatched services, as well as insecure routers and switches – all of which make it easier for unauthorised access to the network.

If cyber criminals do gain access to a network, it is open for exploitation. This aligns with the finding that targeted emails, or 'spear phishing', were the main cyber incidents experienced by organisations.

Interestingly, mobile devices being compromised is considered a vulnerability. This is inconsistent with the earlier finding, which indicates organisations did not experience this type of cyber security incident – refer to figure 7 (0% of mobile devices being compromised).

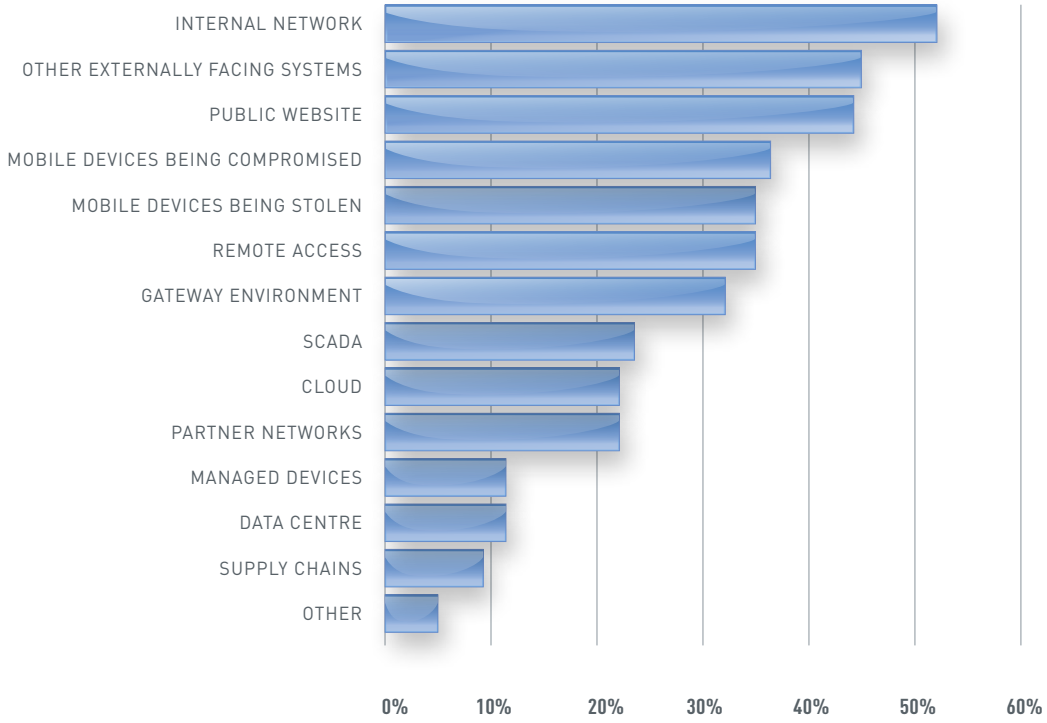
The findings also indicate that organisations have a range of cyber security vulnerabilities, highlighting the need for comprehensive cyber security and risk management plans and procedures.

For example, while the vulnerability of SCADA systems was considered to be relatively low, the consequences of a compromise to these and other industrial control systems may be severe – over and above that of other compromises.

SCADA systems are used in much of the critical infrastructure that underpins essential services, such as those delivered by the water, electricity, communications, gas and transport sectors. They also perform major roles in the manufacturing and resource sectors.

Figure 14 provides a breakdown of the parts of organisations most vulnerable to cyber threats.

FIGURE 14 – breakdown of parts of organisations most vulnerable to cyber threats



THE MOST IMPORTANT RESPONSES TO CYBER THREATS

Respondents were asked what they thought were the most important responses to cyber threats.

The main responses were senior leadership support (76%), training (72%), technical controls (64%), culture change (59%) and procedural controls (53%).

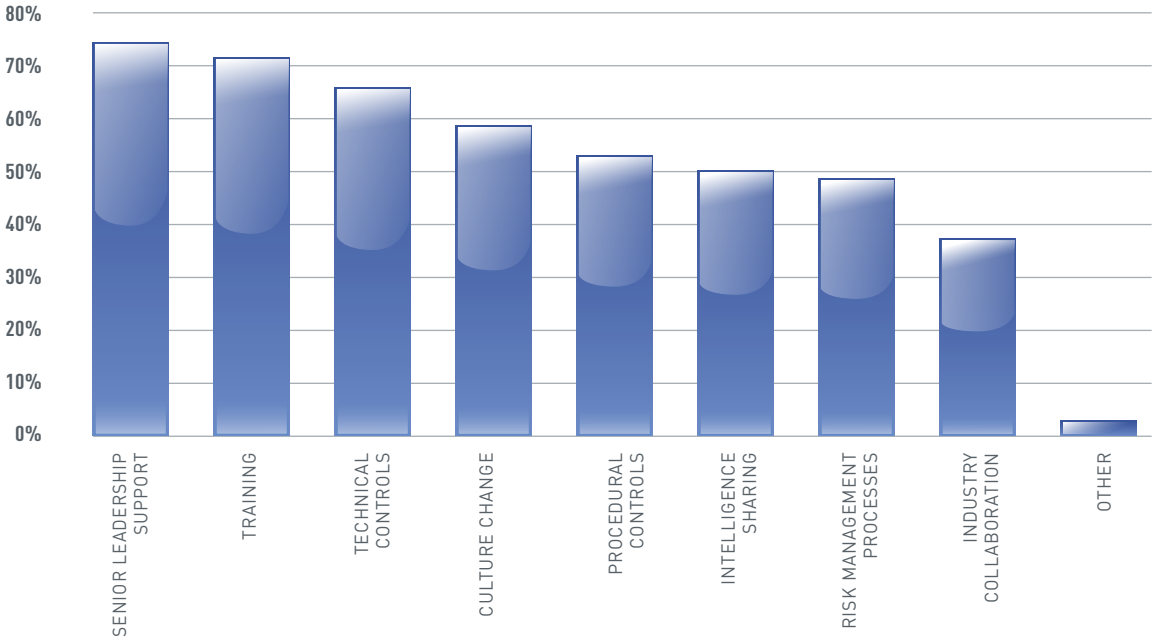
These were followed by intelligence sharing (50%), risk management processes (48%) and industry collaboration (39%).

These findings indicate that an organisation's social and behavioural responses, as well as technical responses are important for cyber security.

Of note, senior leadership support, training and culture change were identified as priorities.

Figure 15 provides a breakdown of the most important responses to cyber threats.

FIGURE15 – breakdown of most important responses to cyber threats



AS AUSTRALIA'S NATIONAL COMPUTER EMERGENCY RESPONSE TEAM, THE CERT WORKS TO ENSURE THAT ALL AUSTRALIANS AND AUSTRALIAN BUSINESSES HAVE ACCESS TO INFORMATION ON HOW TO BETTER PROTECT THEIR INFORMATION TECHNOLOGY ENVIRONMENT FROM CYBER BASED THREATS AND VULNERABILITIES

The CERT is the primary point of contact for cyber security incidents impacting on Australian networks.

The CERT is keen to highlight and reinforce the importance of business taking cyber security seriously. This not only means being aware of cyber threats but also putting effective controls and safeguards into practice. In Australia, it's now publicly acknowledged that cyber operations are one of the most rapidly evolving threats to our national security.

The CERT encourages business to be prepared before an incident occurs. This involves a business knowing its network, understanding the value of its information, and understanding how both are protected.

The CERT also encourages business to understand what constitutes normal behaviour on its network. By knowing this, the business is more likely to detect unusual behaviour.

Being prepared before an incident occurs also involves having operational relationships in place with those who can assist, such as the CERT and law enforcement agencies. Having such contacts already established helps with the efficient and effective sharing of information for prevention – and if necessary, mitigation.

Reporting incidents to the CERT is important. It allows the CERT to make sure that businesses receive the right help – all information provided to the CERT is held in the strictest confidence.

The CERT is the entry point into government for Australian businesses. It works in the Cyber Security Operations Centre, sharing information and working closely with the Australian Security Intelligence Organisation, the Australian Federal Police, and the Australian Signals Directorate.

In addition, it is part of the global network of CERTs in both business and government, and leverages those relationships to protect Australian business.

These partnerships with government agencies and international counterparts mean the CERT is very well connected and informed, so it is best placed to help businesses protect themselves from cyber attacks.

From late 2014, CERT Australia will be co-located within the Australian Cyber Security Centre with other operational cyber security agencies.

The CERT is also a strong point of referral, which can lead to some very positive outcomes in terms of resolution and prosecution.

As such, the important messages for businesses are to

- continue taking cyber security seriously by implementing effective controls
- partner with the CERT before an incident occurs, and
- report cyber incidents to the CERT.

To report an incident

- call the CERT Australia hotline on **1300 172 499**, or
- email **info@cert.gov.au**

GUIDANCE FROM THE CERT

Be prepared before an incident occurs.

Make cyber security part of your risk management and resilience structures and planning.

Train your staff to use good cyber security practices as part of their daily work.

The CERT recommends

- patching applications and operating systems
- limiting the number of users with administrative privileges
- using multifactor authentication for critical systems, and
- using strong passwords/passphrases.

The CERT has also developed a publication on the top cyber security tips for small to medium business – available at **www.cert.gov.au/advice**

In addition, it advises businesses to consider the 35 strategies for mitigating cyber intrusions released by ASD – refer to **www.asd.gov.au/infosec/top35mitigationstrategies.htm**

CASE STUDIES

The case studies in this report provide examples of how partnering with government through the CERT enhances the cyber security of Australian networks.

Australian Government