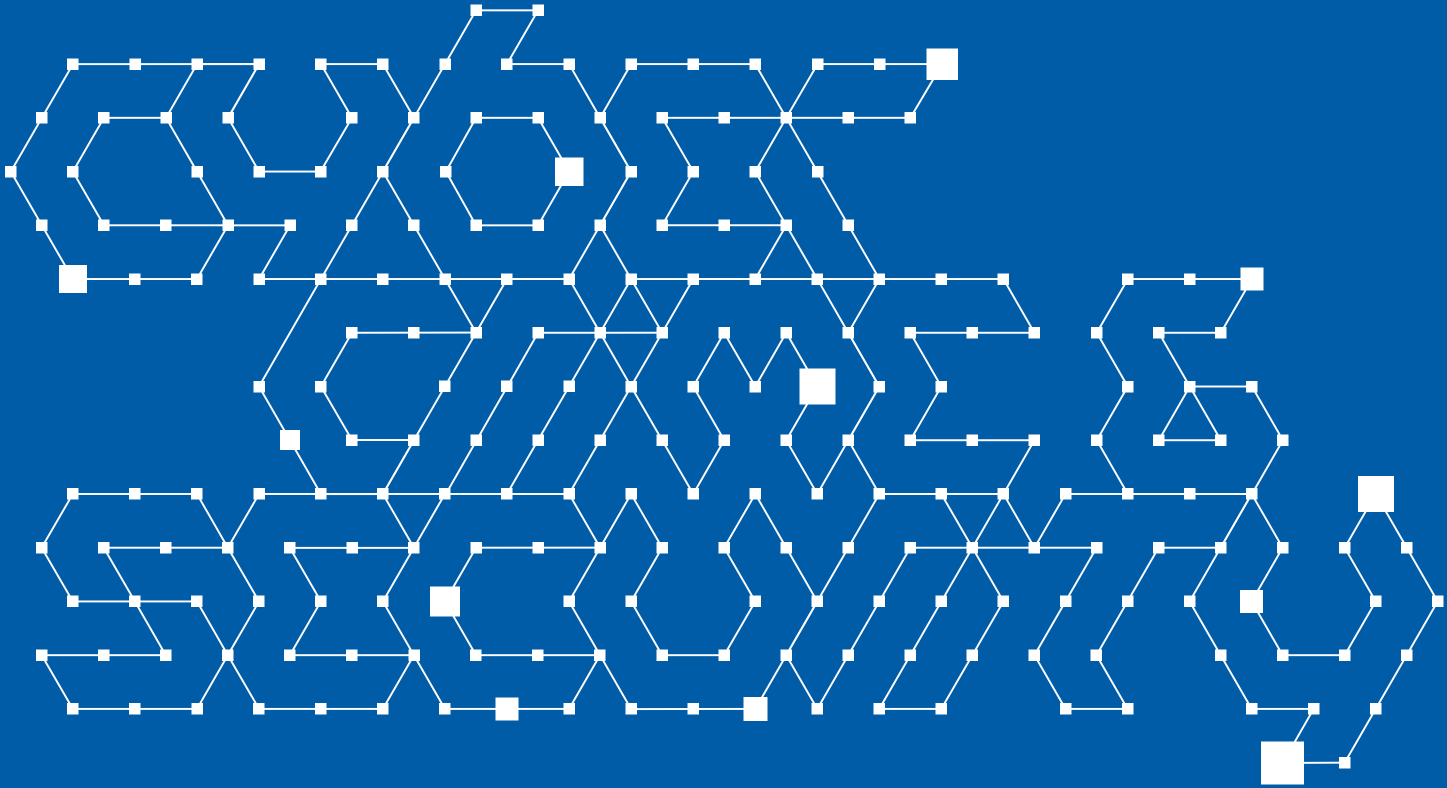
Australian Government



CYBER CRIME & SECURITY SURVEY REPORT 2012_

CERT Australia

AUSTRALIA'S NATIONAL
COMPUTER EMERGENCY RESPONSE TEAM

CIS
Centre for Internet Safety

ACKNOWLEDGEMENTS

CERT Australia and the CIS would like to acknowledge the following contributors to the production of this report: CERT Australia's partner organisations in industry, Online Research Unit, and CRE8IVE.

ISBN: 978-1-922017-03-1

MINISTERIAL FOREWORD_

Australia's way of life is now integrally linked with the internet. The internet provides a global means of communication and interaction that underpins much of our lives – for government, business and individuals.

But while the internet offers a huge range of opportunities, it also brings risks associated with criminal and malicious activity that seeks to exploit those who use it. In particular, the activities and transactions conducted by business online require diligence to ensure that Australia maximises the opportunities offered by the digital economy.

The Australian Government takes cyber security very seriously. CERT Australia stands at the forefront of the Australian Government's support to business in best preparing it to defend against cyber attacks on their systems and networks – attacks that can affect us all.

In July 2012, my predecessor wrote to the CEOs of some 450 businesses that are CERT Australia's stakeholders to ask them to participate in CERT Australia's first *Cyber Crime and Security Survey.* This survey, conducted in partnership with the Centre for Internet Safety at the University of Canberra, is an important step in gaining a better understanding of the impact of malicious online activity targeting Australian business and how well we are placed to respond.

There have been numerous international reports published on these issues in other countries, but to date there has been a paucity of equivalent information specific to Australia. This survey goes some way towards addressing that gap, contributing to a clearer picture of the cyber crime and security environment in Australia.

Of course, this picture is constantly changing, reflecting the complex and evolving nature of cyber crime and security threats. I am therefore pleased that the survey will be an annual event, with the input from business continuing to build on previous survey results.

I would like to thank the businesses that took the time to respond to the first survey.

The survey is yet another demonstration of the value of the partnership between Australian business and the Australian Government, particularly through CERT Australia, in protecting against cyber threats.

Mark Dreyfus QC, MP
Attorney-General of Australia

CONTENTS_

EXECUTIVE SUMMARY_

IMPORTANTLY, BUSINESS IS TAKING CYBER SECURITY SERIOUSLY

The 2012 Cyber Crime and Security Survey: Systems of National Interest was designed and conducted to obtain a better understanding of how cyber incidents are affecting the Australian businesses that form part of Australia's systems of national interest, including critical infrastructure.

These businesses and industries 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 provide a picture of the current cyber security measures these businesses have in place; the recent cyber incidents they have experienced; and their reporting of them. These findings also provide baseline data from which the results of future annual surveys can be compared, to help ascertain overall trends.

Importantly, business is taking cyber security seriously. This is paramount for the security of the individual organisation and its clients, as well as the industry sector, and the business community more broadly. However, the survey results also indicate that many organisations are not confident that cyber security is sufficiently understood and appreciated by staff, management and boards.

In terms of cyber security incidents, more than half the organisations considered attacks on their organisation to be targeted. This indicates a shift from previous views or conceptions, that most attacks are non-targeted or indiscriminate. And while the majority of attacks were reported to come from external sources, the fact that 44% originated from within organisations serves as a reminder that internally-focused cyber security controls and measures are also important.

Reporting of cyber security incidents – which is critical to the effectiveness of the government-business partnership – clearly requires further attention. The CERT needs to articulate to business the benefits of reporting cyber security incidents to CERT Australia and to law enforcement, and that all information provided to the CERT is held in the strictest confidence.

KEY FINDINGS

The key findings for this survey include:

- over 90% of respondents deployed firewalls, anti-spam filters and anti-virus software
- two-thirds of respondents had documented incident management plans, however only 12% had a forensic plan
- nearly two-thirds of organisations used IT security related standards
- over two-thirds of respondents had staff with tertiary level IT security qualifications. Over half had vendor IT security certifications, whilst just under half had non-vendor IT security certifications
- over 20% of organisations know they experienced a cyber incident in the previous 12 months, with 20% of these organisations experiencing more than 10 incidents.

Of the organisations which know they experienced cyber incidents:

- 17% suffered from loss of confidential or proprietary information, 16% encountered a denial-of-service attack, and 10% financial fraud
- 44% reported the incident to a law enforcement agency, whereas only 13% sought a civil remedy through action from legal counsel
- 20% chose not to report the matter to a law enforcement agency because of the fear of negative publicity
- the most common responses as to why incidents were successful, were that they used powerful automated attack tools, or exploited unpatched or unprotected software vulnerabilities or misconfigured operating systems, applications or network devices
- over half of all organisations have increased their expenditure on IT security in the previous 12 months.

OVER 90% OF RESPONDENTS DEPLOYED FIREWALLS, ANTI-SPAM FILTERS AND ANTI-VIRUS SOFTWARE

INTRODUCTION_

THE 2012 CYBER CRIME AND SECURITY SURVEY: SYSTEMS OF NATIONAL INTEREST WAS COMMISSIONED BY AUSTRALIA'S NATIONAL COMPUTER EMERGENCY RESPONSE TEAM, CERT AUSTRALIA (THE CERT), PART OF THE FEDERAL ATTORNEY-GENERAL'S DEPARTMENT.

This report provides analysis of the findings, and identifies areas for further exploration or improvement which may be addressed in future surveys. As there was a strong response rate of almost 60% for this inaugural survey, the findings are considered to be representative of this particular sample. The strong response rate also indicates a good level of trust between the CERT and its business partners.

Established in 2010, the CERT works with the Australian business sector – primarily the owners and operators of systems of national interest. These are the businesses that underpin the social and economic wellbeing of the nation and the economy, such as banking and finance, communications, energy, resources, transport and water.

The CERT provides cyber security threat and vulnerability information to help these businesses manage risk, as well as providing support with incident response. The CERT is also a member of the Cyber Security Operations Centre and the global CERT community. By using its government, international and industry networks, the CERT seeks to provide the most effective and timely advice and assistance possible.

ABOUT THE SURVEY_

The survey was designed to obtain a better picture of how cyber incidents are affecting the businesses that partner with the CERT. It was produced by the Centre for Internet Safety at the University of Canberra. More information on the Centre can be found at www.canberra.edu.au/cis. The Centre was created to foster a safer, more trusted internet by providing thought leadership and policy advice on the social, legal, political and economic impacts of cybercrime and threats to cyber security. The survey was hosted by the Online Research Unit.

Participating organisations were asked that an appropriate person complete the survey, and were assured that all responses are anonymous.

The survey consisted of 24 questions, both closed and open ended, to ascertain:

- business description
- types of IT security used
- types of cyber security incidents experienced, and
- industry reporting of incidents.

RESPONDENTS_

THE STRONG RESPONSE RATE OF ALMOST 60% REFLECTS THE TRUSTED RELATIONSHIP CERT AUSTRALIA HAS WITH ITS BUSINESS PARTNERS

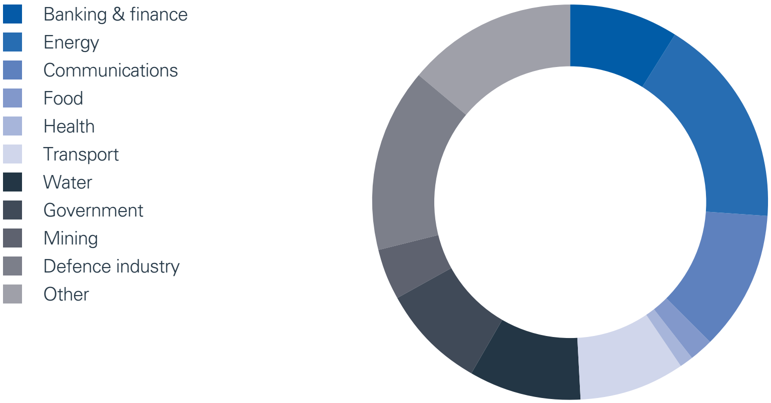
Of the almost 450 organisations contacted, responses were received from 255, which is approximately 60%. This is a strong response rate and reflects the trusted relationship the CERT has with its business partners. It also reflects the willingness of business to participate in a survey that will help government and improve understanding of the cyber security threat environment in Australia.

INDUSTRY SECTOR

More than 11 industry sectors responded, with the greatest representation being from energy (17%), defence industry (15%), communications (12%), banking and finance (9%) and water (9%).

Figure 1 provides a breakdown of the sectors – with 'government' referring to state-owned enterprises and 'other' referring to companies from aviation/aerospace, business services and insurance.

FIGURE_01 – BREAKDOWN OF RESPONDENTS BY INDUSTRY SECTOR



TRUSTED INFORMATION SHARING NETWORK

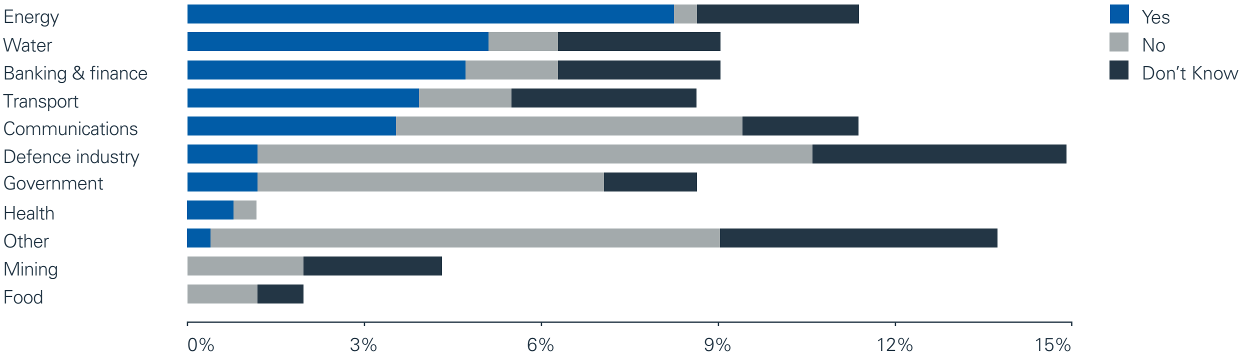
The Trusted Information Sharing Network for Critical Infrastructure Resilience (TISN) is led by the Federal Attorney-General's Department. It provides an environment where business and government can share information on security issues relevant to the protection and resilience of critical infrastructure, and the continuity of essential services in the face of all hazards. The TISN has seven main sector groups – banking and finance, communications, food, energy, health, transport and water.

Disruption of Australia's systems of national interest or critical infrastructure could have a range of serious implications for business, governments and the community. It is vital that owners and operators of these important organisations, both in the private and public sector, are able to plan for, withstand and respond to a broad range of threats, including cyber attacks from outside and inside their organisation.

One third of respondents reported their organisation to be a member of the TISN. This included organisations from banking, energy, communications, transport and water. This provides a mostly representative picture of the TISN sectors that partner with the CERT. One third of respondents reported their organisation was not a member of the TISN, while one third of respondents did not know if their organisation is a member.

Figure 2 provides a breakdown of industry sectors, according to whether or not the respondent identified the organisation as being a member of the TISN.

FIGURE_02 – BREAKDOWN OF INDUSTRY SECTORS IDENTIFYING AS MEMBERS OF THE TISN



SECURITY OF IT SYSTEMS_

Security of IT systems centers on preventing and detecting the unauthorised access to or use of IT systems or impairment of those systems. To achieve such security, modern organisations layer security defences in 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 of defence 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 TECHNOLOGY

Organisations were asked what type of computer security technologies they used. More than 90% of respondents reported using antivirus software, spam filters, and firewalls. More than 80% also reported using access control and virtual private networks (VPNs).

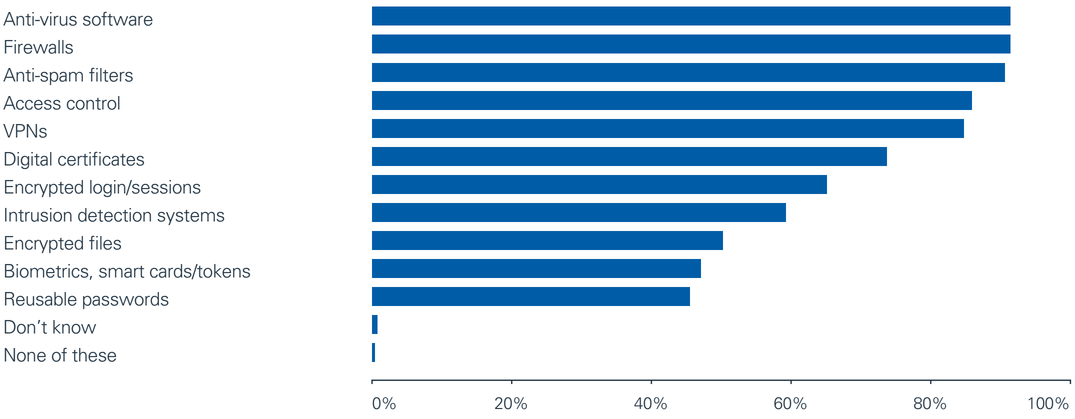
IT security technology such as firewalls and spam filters are not always effective in preventing or detecting sophisticated attacks, so security techniques are increasingly incorporating the use of intrusion detection systems (IDS). Almost 60% of respondents reported using a type of IDS.

Almost half the respondents also reported deploying reusable passwords and multifactor authentication technologies such as biometrics, smartcards and tokens.

These results indicate that some organisations may need to strengthen their IT security, by adopting a defence-in-depth approach.

Figure 3 provides a breakdown of the security technology being used by respondents.

FIGURE_03 – BREAKDOWN OF SECURITY TECHNOLOGY USED



BASIC SECURITY POLICIES ARE BEING APPLIED BY THE MAJORITY OF SURVEYED ORGANISATIONS

IT SECURITY POLICY

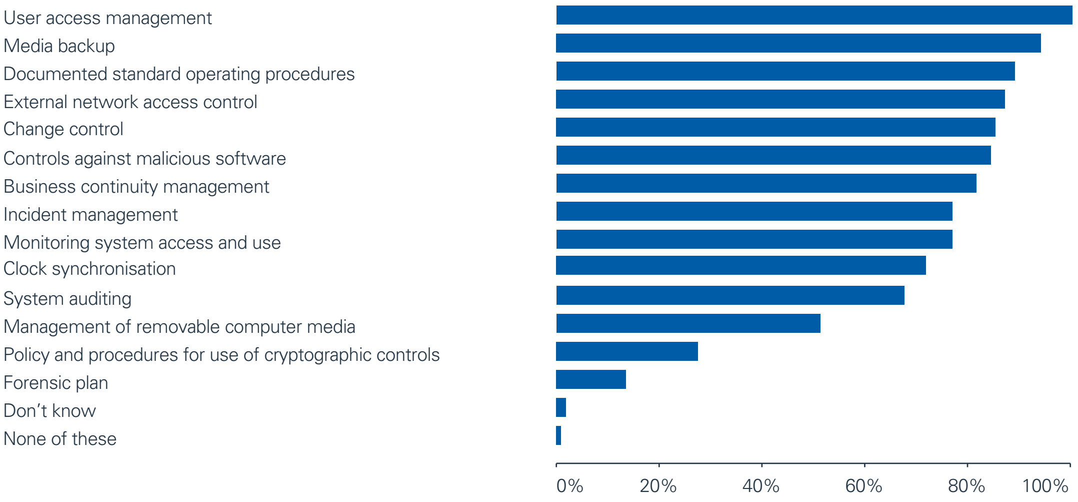
According to respondents, basic security policies are being applied by the majority of surveyed organisations. For example, 84% deploy user access management, 79% perform media backup, 75% use documented standard operating procedures, and 73% have external network access control.

Results indicate there are areas for improvement. For example, less than 50% of respondents have plans in place for the management of removable computer media, such as USB memory drives, and less than 25% have policies and procedures in place for using cryptographic controls.

In addition, less than 12% of respondents reported having a forensic plan in place. These plans help monitor use of the ICT systems, provide mechanisms to recover lost data, and provide ways to protect information on systems.

Figure 4 provides a breakdown of the security policies being used by respondents.

FIGURE_04 - BREAKDOWN OF SECURITY POLICIES IN PLACE



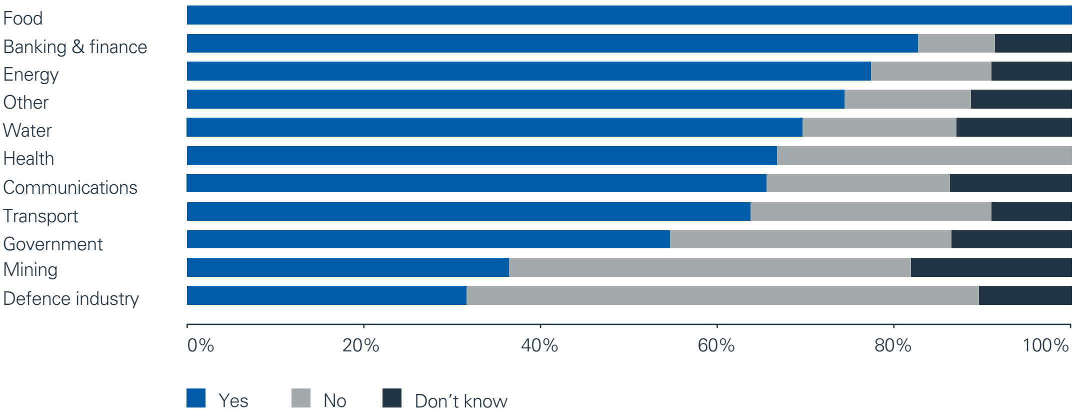
IT SECURITY STANDARDS

Overall, 64% of respondents reported their organisation did apply IT security standards or guidelines.

Of the remaining respondents, 25% reported their organisation did not apply IT security standards or guidelines, and 11% did not know. These findings are a concern and warrant future investigation.

Figure 5 provides a breakdown of industry sectors and their use of IT security standards or guidelines.

FIGURE_05 – BREAKDOWN OF INDUSTRY SECTORS AND STANDARDS



IT'S IMPORTANT TO TAKE CYBER SECURITY SERIOUSLY… LAYER SECURITY DEFENCES IN IT SYSTEMS

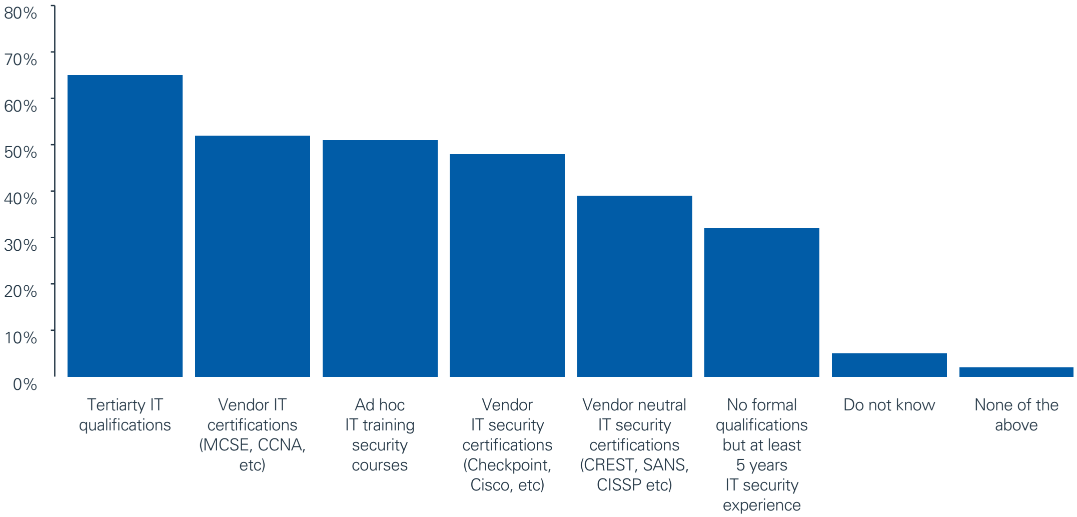
Of the respondents who reported their organisation did apply some form of IT security standard, almost 50% followed or used as a guide, the ISO 27001. This standard states it is mandatory for management to examine their organisation's IT security risks to form a risk mitigation system, and to ensure that the controls applied are current for the needs of the business.

Of this same subset of respondents, just over 20% reported their organisation adhered to the Payment Card Industry Data Security Standard (PCI DDS). This is the IT security standard commonly used by organisations using credit card data. In addition, just over 15% used a vendor specific standard.

IT SECURITY QUALIFICATIONS

Responses indicated that 65% of participating organisations had IT security staff with tertiary level IT qualifications. More than 50% of participating organisations had IT security staff with some type of vendor based IT certifications. Almost 35% of participating organisations had IT security staff with no formal training, although most of these staff had more than five years working in the IT security industry.

FIGURE_06 – IT SECURITY QUALIFICATIONS OF IT STAFF



These findings indicate that some organisations may need to improve the skill set of their IT security staff.

This was supported by the additional finding that 55% of respondents thought their organisation needs to do more to ensure their IT security staff have an appropriate level of qualification, training, experience and awareness.

These findings indicate that respondents are aware of the need for IT security staff to keep their skills and knowledge up to date – which is essential, as cyber threats are constantly evolving.

Respondents also thought their organisation needs to do more to ensure other staff have an appropriate level of IT skill and awareness:

- 70% of respondents reported this need for general staff
- 70% of respondents reported this need for management, and
- 48% of respondents reported this need for their board of directors.

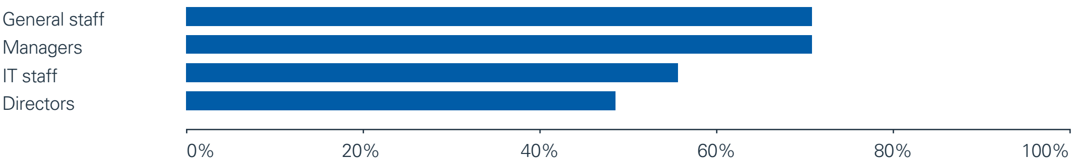
These findings indicate that respondents are aware that cyber security is a shared responsibility. Even where networks are secure at the perimeter, security is dependent on all staff being aware of vulnerabilities such as phishing attacks. This is a method used to penetrate organisations without needing to breach IT security defences, by attempting to get staff to divulge information and provide access – unwittingly – to corporate systems.

These findings also indicate that many organisations are not confident that cyber security is sufficiently understood and appreciated by staff, management and boards.

Figure 7 provides a breakdown of organisational staff and respondents' views on the need for the organisation to do more to ensure they have an appropriate level of IT security skill and awareness.

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

FIGURE_07 – BREAKDOWN OF STAFF AND NEED TO ENSURE APPROPRIATE IT SECURITY SKILL



CYBER INCIDENTS_

RESPONDENTS WERE ASKED ABOUT THE TYPES OF CYBER SECURITY INCIDENTS THEIR ORGANISATION HAD EXPERIENCED...

Respondents were asked about the types of cyber security incidents their organisation had experienced in the previous 12 months, as well as possible motives for the attacks, and why the attacks may have been successful.

A cyber security incident was classified as an electronic attack that harmed the confidentiality, integrity or availability of the organisation's network data or systems.

FIGURE_08 - ORGANISATIONS THAT EXPERIENCED ONE OR MORE CYBER INCIDENTS

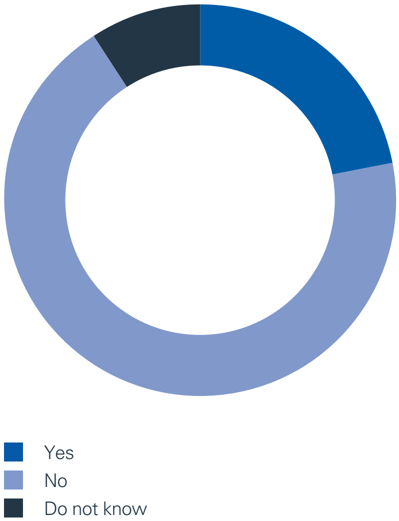
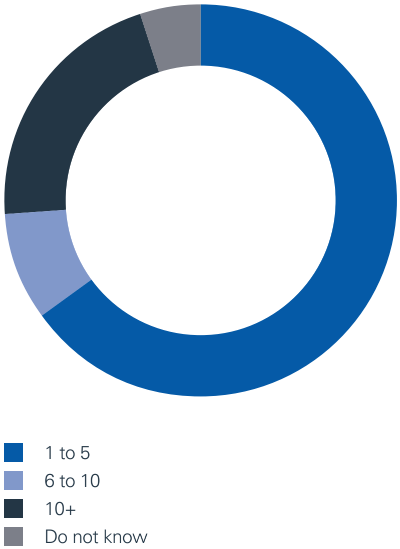


FIGURE_09 - BREAKDOWN OF NUMBER OF INCIDENTS EXPERIENCED



NUMBER OF INCIDENTS EXPERIENCED

When asked if their organisation had experienced a cyber security incident in the previous 12 months:

- 69% of respondents reported ‘no’
- 22% of respondents reported ‘yes’, and
- 9% of respondents reported they ‘did not know’.

While these results indicate the majority of organisations did not experience a cyber incident in the previous 12 months, this may more accurately reflect that a number of cyber intrusions have gone undetected by some organisations. Anecdotal evidence available to the CERT suggests that some businesses are unaware of the full scope of unauthorised activity on their networks.

The CERT is also aware of hesitation from organisations to report a cyber security incident. This may be for a variety of reasons – some are concerned that the information they report may lead to negative publicity and/or regulatory scrutiny, others don’t consider reporting to be worthwhile.

Of the respondents who reported their organisation had experienced an incident in the previous 12 months:

- 65% reported experiencing one to five incidents
- 21% reported experiencing more than 10 incidents
- 9% reported experiencing six to 10 incidents, and
- 5% did not know how many incidents had been experienced.

Figure 9 provides a percentage breakdown of the number of cyber security incidents experienced by organisations in the previous 12 months.

THESE FINDINGS MAY HELP ORGANISATIONS DECIDE WHERE TO PLACE ADDITIONAL RESOURCES TO PROTECT THEIR INFORMATION ASSETS

TYPES OF INCIDENTS EXPERIENCED

Of the respondents who reported their organisation had experienced a cyber incident in the previous 12 months, the main types reported were:

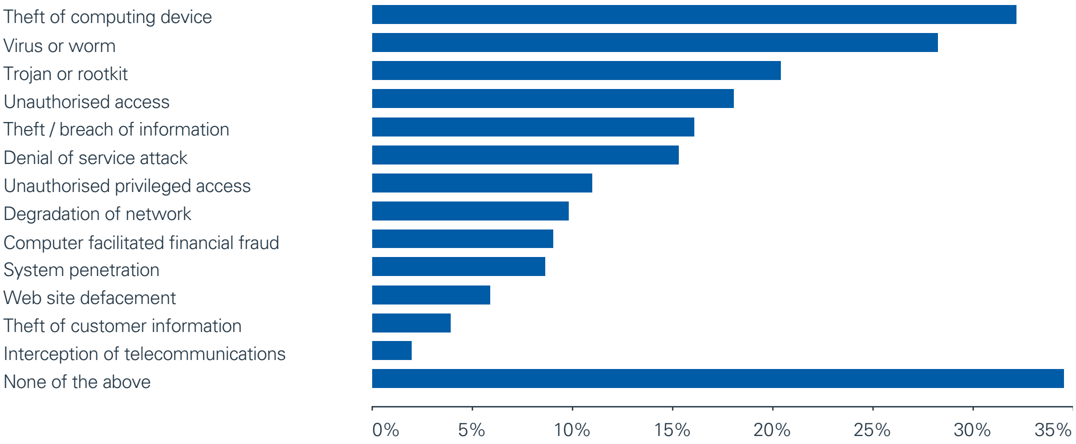
- theft of a notebook, tablet or mobile devices – 32%
- virus or worm infection – 28%
- trojan or rootkit malware – 21%
- unauthorised access – 18%
- theft or breach of confidential information – 17%, and
- denial-of-service attack – 16%.

These findings may help organisations decide where to place additional resources to protect their information assets. The high percentage of physical computing assets being stolen highlights the need for physical security measures to be included in an organisation's security risk management plan.

Interestingly, although respondents were provided with 13 specific types of incident from which to choose – 34% of respondents reported the incidents their organisation had experienced were 'none of the above'. As the types of incident were comprehensively listed, this finding may be due to the respondent not knowing what type of incident was actually experienced.

Figure 10 provides a breakdown of the type of cyber security incidents experienced by organisations in the previous 12 months.

FIGURE_10 – BREAKDOWN OF TYPE OF INCIDENTS EXPERIENCED



Of the respondents who knew they had suffered electronic attack, 71% reported they had been subject to between 1 and 5 external attacks, whilst 44% reported they had been subject to between 1 and 5 internal attacks. Many companies spend the majority of their IT security budget on protection from external attacks. But the figures above serve as a reminder that internal controls and measures are also important, to ensure that internal risks are also managed. Should they have sufficient motivation – financial, personal or cause-related – internal employees, whether they are permanent or casual staff or contractors, can have access to sensitive information and the opportunity to understand critical systems and exploit potential weaknesses in security.

BUILDING RESILIENCE TO CYBER SECURITY INCIDENTS REQUIRES CONSTANT VIGILANCE BY IT SECURITY STAFF

MOTIVES FOR THE ATTACKS

Respondents were asked what they thought the motives for the incidents were. The highest suspected motive was non-targeted unsolicited malicious damage (17%), followed by indiscriminate attack (almost 16%).

Interestingly, more than half the respondents viewed the attacks to be targeted at their organisation – with motives being illicit financial gain (15%), hactivism (9%), using the system for further attacks (9%), using the system for personal use (6%), being from a foreign government (5%), personal grievance (5%), and being a competitor (4%).

This finding indicates a shift from previous views or conceptions, that most attacks are non-targeted or indiscriminate.

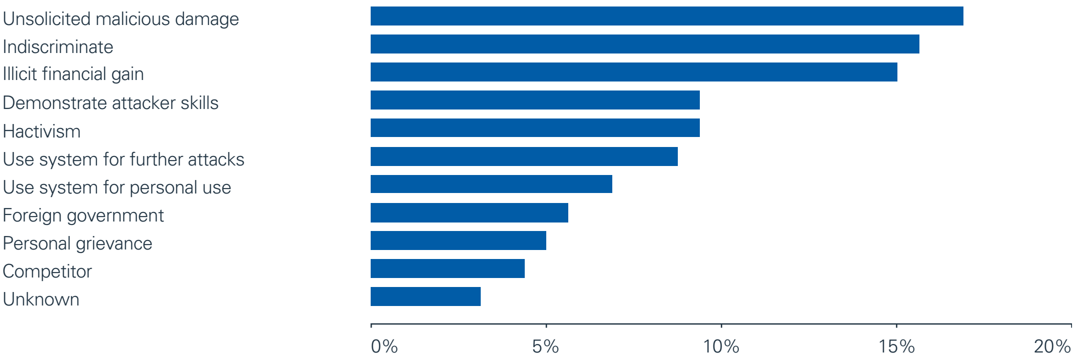
Either way, building resilience to cyber security incidents requires constant vigilance by IT security staff, in order to create and apply current and efficient risk treatments.

Attribution is always difficult. Where respondents think an attack may have come from, may not be where it actually came from. What's important is that an organisation understands enough about attacks so they can work out:

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

Figure 11 provides a breakdown of suspected motives for cyber security incidents experienced by organisations in the previous 12 months.

FIGURE_11 – BREAKDOWN OF MOTIVES FOR INCIDENTS EXPERIENCED



CASE STUDY – RANSOMWARE_

In late September 2012, CERT Australia received a series of calls from more than 25 organisations being targeted by *ransomware*.

The attacks encrypted files on the compromised system and/or locked the victim out of the desktop environment. The attacks also encrypted files in the system backups.

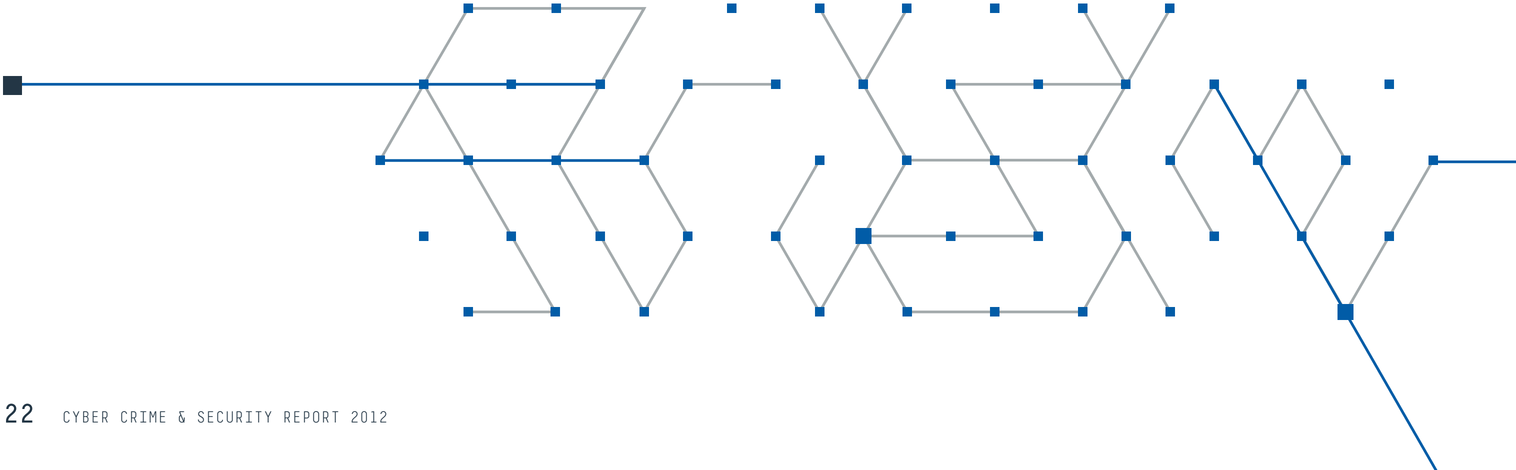
The victims were then asked by the attacker to pay a fine using a payment or money transfer service, to obtain the codes that would unlock the computer and/or decrypt the data.

In some cases, the *ransomware* included scareware, displaying a fake warning screen, claiming that the victim's computer had been associated with criminal activity. This was a tactic to discourage the victim from reporting the attacks to law enforcement agencies or the CERT. For example, one warning screen was set up to look like it was from the Anti Cyber Crime Department of the Federal Internet Security Agency. There is no such agency.

In the majority of cases, the attackers used Microsoft Remote Desktop Protocol as an entry point to the target network. This was possibly using authentication credentials obtained by key loggers, or accessing systems with weak credentials.

The severity of the damage done by the attacks varied across the target organisations. In the worst case scenario reported to the CERT, one victim lost 15 years' worth of critical business data, which is a serious compromise.

THE VICTIMS WERE THEN ASKED BY THE ATTACKER TO PAY A FINE USING A PAYMENT OR MONEY TRANSFER SERVICE...



So how does the CERT help business deal with such attacks?

Firstly, it worked directly with the affected organisation to help it better defend against the attack. Where the organisation had outsourced management of its website, the CERT helped the service provider protect the affected network.

The CERT also worked with law enforcement locally – because of the criminal nature of the activity; Microsoft – to share data and analysis; and international colleagues – as the threat actors or attackers used infrastructure based overseas.

In addition, the CERT identified other organisations in Australia that had not yet reported the activity. It then contacted them to warn the attacks were happening in their sector, and then gave them advice about how to protect their systems.

The CERT also issued a guidance paper on the *ransomware* threat, which was made publicly available on its website.

This case study highlights the nature of CERT Australia's mission – it's all about helping business best prepare for and respond to cyber attacks. It does this by using its government, industry and international partnerships to provide the most useful advice possible – as soon as possible.

> THESE FINDINGS HIGHLIGHT THE NEED FOR ORGANISATIONS TO STAY VIGILANT TO VULNERABILITIES...

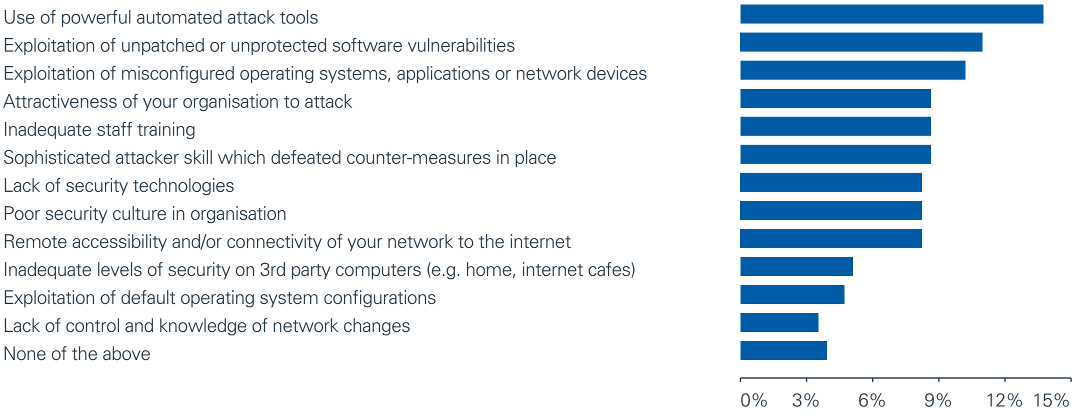
CONTRIBUTING FACTORS TO THE ATTACKS

Respondents were asked what factors they thought may have contributed to the incidents. The highest rated reason was the use of powerful automated attack tools (14%), followed by exploitation of unpatched or unprotected software vulnerabilities (11%), and exploitation of misconfigured operating systems, applications or network devices (10%).

These findings highlight the need for organisations to stay vigilant to vulnerabilities and apply appropriate mitigations – specifically where misconfigured systems are the reason an attack was successful.

Figure 12 provides a breakdown of respondents' views on contributing factors to cyber incidents.

FIGURE_12 – BREAKDOWN OF CONTRIBUTING FACTORS TO INCIDENTS



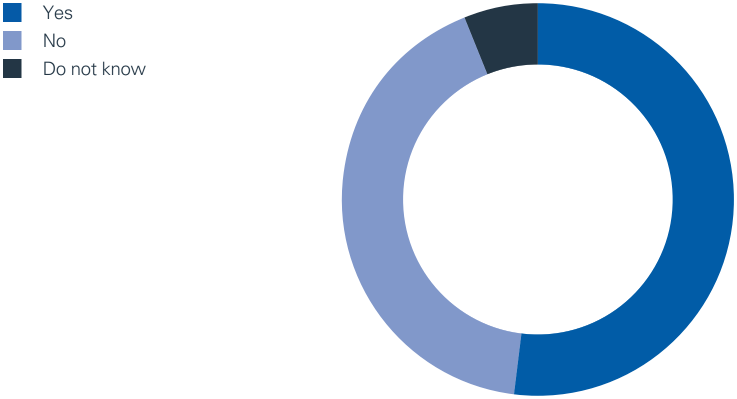
EXPENDITURE ON IT SECURITY

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

- 52% of respondents reported 'yes'
- 42% of respondents reported 'no', and
- 6% of respondents reported they 'did not know'.

52% OF ORGANISATIONS INCREASED EXPENDITURE ON IT SECURITY IN THE PREVIOUS 12 MONTHS

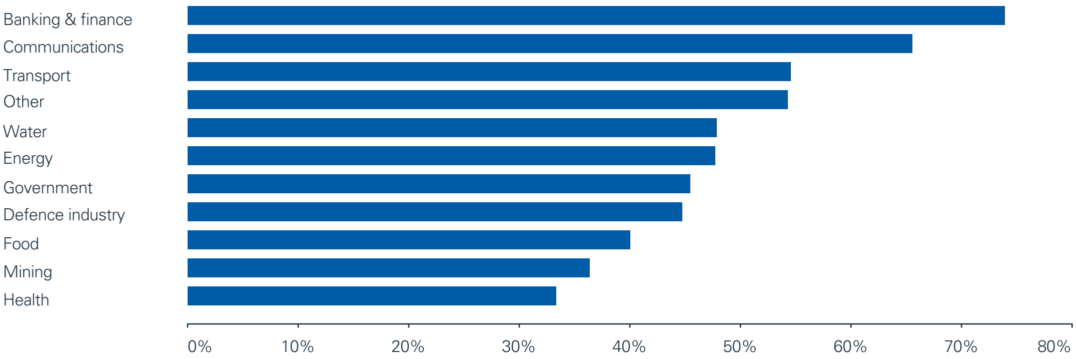
FIGURE_13 – ORGANISATIONS THAT INCREASED EXPENDITURE ON IT SECURITY IN THE PREVIOUS 12 MONTHS



THERE IS A NEED FOR CONTINUAL INVESTMENT IN INFORMATION SECURITY

These findings indicate that more than half of participating organisations are increasing their expenditure in information security. While it is unknown where this expenditure was directed within an organisation, it is a positive step demonstrating the need for continual investment in information security.

FIGURE_14 – BREAKDOWN OF INDUSTRY SECTORS AND INCREASE IN IT EXPENDITURE



REPORTING INCIDENTS HELPS THE CERT & THE GOVERNMENT **UNDERSTAND** NEW TRENDS IN **CYBER·CRIME**

IT'S IMPORTANT TO PARTNER WITH CERT AUSTRALIA BEFORE AN INCIDENT OCCURS

CASE STUDY – DISTRIBUTED DENIAL-OF-SERVICE_

Distributed denial-of-service (DDoS) attacks are one of the most serious threats to organisations with an online presence.

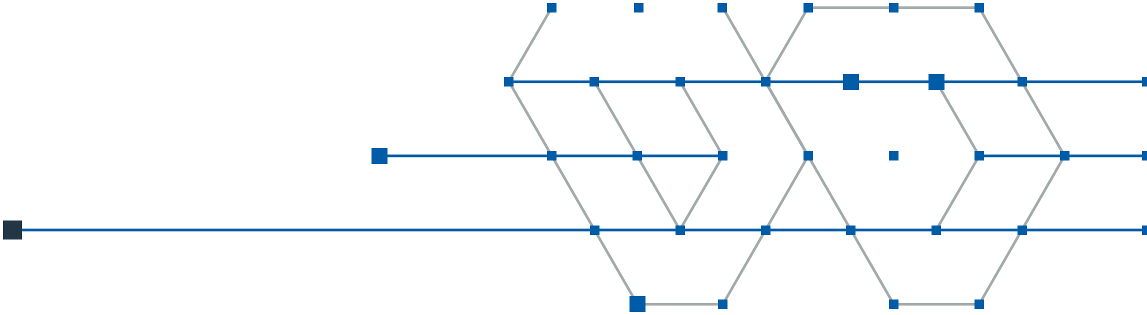
Historically, these attacks had non-financial motivations, aiming to bring attention to certain events or protest specific issues. The more recent trend, however, is for DDoS to be used for extortion.

Early in 2012, CERT Australia received reports from a range of Australian financial companies that were being targeted by extortion-based DDoS attacks. They had been called and threatened with an attack against their website, unless they made a payment.

This type of attack can cause serious problems. It can not only disrupt the company's online activities via its website, it can also stop clients from doing business with them online.

The attackers chose their targets carefully. They combed victim websites for pages that would generate the most processing in order to increase the likelihood of successfully taking down the site. Some websites were brought down by the attack; others had the infrastructure to withstand it.

The CERT located the target list for the attacks and contacted the listed companies. As the attacks were of a criminal nature, the CERT also provided all relevant information to the Australian Federal Police's High Tech Crime Operations for investigation.



The sites which had the ability to mitigate the attack were not targeted for long. With the attacks being financially motivated, the attacker seemed quick to move on to other potential victims. However, if the company communicated with the attacker, the site appeared on the target list for longer periods of time.

The CERT was able to identify the international source of the attacks from a sample of the DDoS traffic provided by one of the companies – this highlights the value of sharing information. The CERT then notified its international counterpart, asking for assistance in having the control hub taken down. The international CERT responded quickly and the host was shut down.

However, as is normally the case with such incidents, the control hub then moved to another internet address and recommenced attacks. The CERT again contacted overseas counterparts to issue further take down requests.

The CERT also continued to follow up with affected companies, providing options and advice on mitigation techniques for possible future attacks. The companies that were most effective in mitigating the attacks had already well-established and tested response procedures in place for dealing with DDoS.

This case study highlights the need for organisations to develop DDoS response plans and test them. By partnering with the CERT – ideally before an incident occurs – business can be better prepared to mitigate cyber attacks.

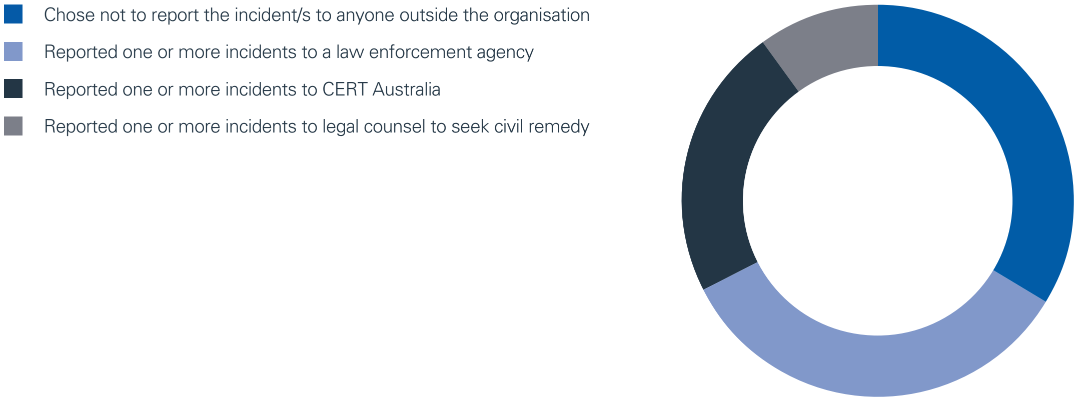
REPORTING OF INCIDENTS_

IT'S IMPORTANT AND NECESSARY FOR BUSINESS TO REPORT CYBER INCIDENTS TO CERT AUSTRALIA... ALL INFORMATION IS HELD IN THE STRICTEST CONFIDENCE

Respondents who indicated their organisation had experienced cyber attacks in the previous 12 months, were asked a range of questions about reporting the incidents.

Just under half the respondents (44%) said they had chosen not to report the incidents to an outside organisation. Of the respondents who did report one or more incidents, 44% were to a law enforcement agency, and 29% were to the CERT.

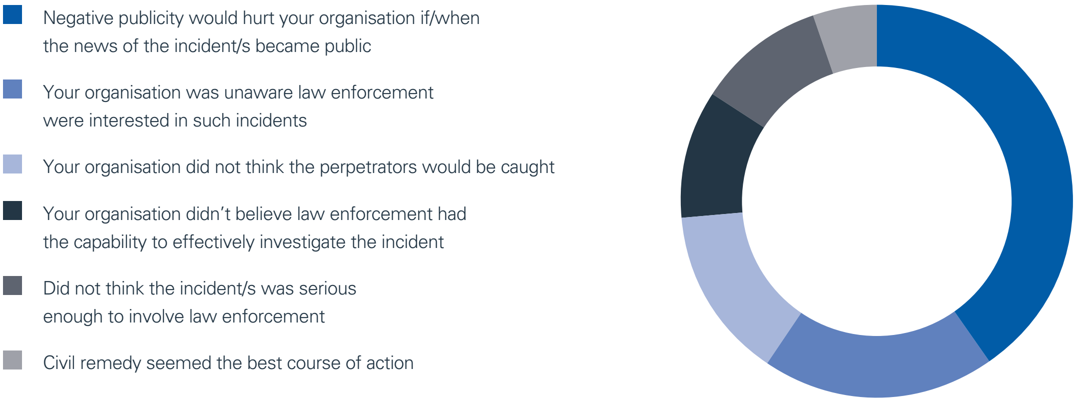
FIGURE_15 – TO WHOM ORGANISATIONS REPORTED A CYBER SECURITY INCIDENT



These findings indicate a high level of caution from organisations in reporting incidents – although they may also reflect the actions of the respondent, rather than the overall practice of the organisation.

When asked why they had chosen not to report a cyber security incident to a law enforcement agency, 74% indicated that they didn't think the incident/s warranted law enforcement intervention. This response may indicate the incident/s suffered by these organisations were of a minor level and/or they were unaware of the threshold level for interest and acceptance for investigation by a law enforcement agency. In addition, 35% of organisations didn't believe law enforcement had the capability to effectively conduct an investigation into the incident, while 26% didn't think the perpetrator would get caught.

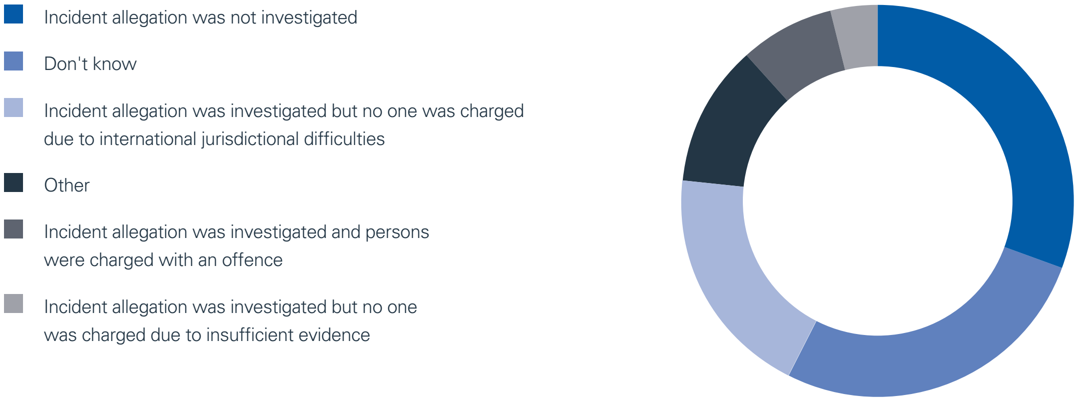
FIGURE_16 – WHY ORGANISATIONS CHOSE NOT TO REPORT A CYBER SECURITY INCIDENT TO A LAW ENFORCEMENT AGENCY



...THE BENEFITS OF REPORTING CYBER SECURITY INCIDENTS TO CERT AUSTRALIA AND TO LAW ENFORCEMENT...

Out of those respondents who did report a cyber security incident to law enforcement, 33% stated that it was their understanding the incident was not investigated and 29% stated they did not know the outcome from the referral, while 8% of matters referred to law enforcement were reported to have resulted in a person being charged.

FIGURE_17 - OUTCOMES OF REPORTING OF A CYBER SECURITY INCIDENT'S TO LAW ENFORCEMENT



These findings highlight that the CERT needs to articulate to business the benefits of reporting cyber security incidents to CERT Australia and to law enforcement, and that all information provided to the CERT is held in the strictest confidence.

CASE STUDY – CRIMINAL INVESTIGATION

In 2009, the Australian Federal Police received information regarding the unauthorised modification of data at a Western Australian government department. The subsequent investigation revealed two males who were contractors to the department, sharing information regarding the illegal access to the departmental computer operating system.

The investigation revealed communications between the two males pertaining to the creation of malicious software and subsequent commands to hack network security controls in an attempt to crack a file and reveal the user-names and passwords of departmental staff.

The AFP executed search warrants at both males' addresses and seized a number of computers and associated media. Both males were subsequently charged with conspiracy to cause an unauthorised modification of data held in a computer, knowing the modification to be unauthorised, and being reckless as to whether the modification impaired the reliability, security or operation, of any such data and the modification is caused by means of a carriage service, contrary to section 11.5(1) and sub-section 477.2(1) of the Criminal Code 1995 (Cth).

Upon appearing at Court, both males pleaded not-guilty to the above offence. Following a trial, they were both found guilty. One of the offenders was sentenced to 30 months imprisonment to be released after having served 10 months and the other to 36 months to be released after having served 12 months, both to enter into a recognisance to be of good behaviour for a period of 20 and 24 months respectively.

ABOUT CERT AUSTRALIA_

THE CERT ENCOURAGES BUSINESS TO BE PREPARED BEFORE AN INCIDENT OCCURS

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 initial 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.

As general guidance, the CERT advises business to use the Top 35 strategies for mitigating cyber intrusions, released by the Defence Signals Directorate (DSD). This list is informed by DSD's experience in operational cyber security, including responding to serious cyber incidents and performing vulnerability assessments and penetration testing for Australian Government agencies. While the first four strategies have the potential to mitigate up to 85% of attacks, this information does need to be tailored to suit the needs and operating environment of each business.

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 necessary and important. It allows the CERT to make sure that businesses receive the right help – and 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 with other key agencies including the Australian Security Intelligence Organisation, the Australian Federal Police and the Defence Signals Directorate. The CERT also works closely and shares information with its international counterparts.

This means the CERT is very well connected and very well informed, which is a great asset in helping businesses protect themselves from cyber attacks. 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