BDO

2016 CYBER SECURITY SURVEY

FOREWORD

Cyber security is a key priority across the Asia-Pacific region and the Australian and New Zealand Governments are taking a proactive approach to ensuring strong cyber security remains a priority in the digital age.

By adopting effective cyber security practices at a national, organisational and personal level, we can help foster economic growth and prosperity in our region, and ensure the businesses and individuals who contribute to it, can do so within a secure cyber environment.

The cyber security landscape is continually evolving. New technologies – such as cloud computing, the Internet of Things and big data – present new channels for adversaries to infiltrate networks. Businesses must work hard to keep up with the pace of change and be resilient to new threats.

Collaboration and international engagement between governments, industry sectors and businesses are vital to building resilience. The private sector owns the majority of a countries digital infrastructure, so the Boards and Executives of businesses – across all sectors – must share responsibility for cyber security with government.

The BDO and AusCERT 2016 Cyber Security Survey is a clear demonstration of the value collaboration can deliver. Research like this is vital to improving our cyber defences and creating solutions to shared problems. The survey report provides insight into, and analysis of, cyber security issues to help inform businesses' cyber investment and risk management decisions. Businesses can use this data to benchmark their current cyber security practices against those of similar businesses, empowering them to improve their understanding and the maturity of their cyber defences.

We encourage businesses to use the survey results as a catalyst for internal discussion and to assess, plan and deploy cyber security measures that are not only fit for purpose, but adaptable to industry demands and future threats.
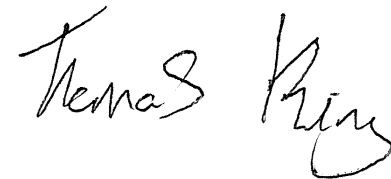
There is no question that Australia and New Zealand are increasingly a target for cybercrime and this is not going to change. The strength of our economies means our systems and data are viewed as incredibly valuable to potential adversaries, so we must act together to address our cyber security threats. Getting cyber security right will allow us to capture more of the opportunities our online world offers.

Working together, informed by insightful research, government and industry can achieve a creative, collaborative and adaptable cyber security future.

Thank you to all the participants and supporters of our 2016 survey. Without your input and honesty, this report would not have been possible.

LEON FOUCHE
NATIONAL LEADER, CYBER SECURITY, BDO

THOMAS KING
GENERAL MANAGER, AusCERT
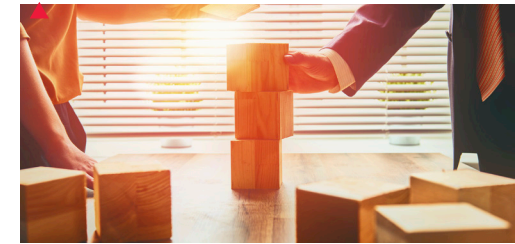
CONTENTS

INTRODUCTION

< 19% OF RESPONDENTS HAVE OR PLAN TO HAVE A SENIOR MANAGEMENT ROLE RESPONSIBLE FOR CYBER SECURITY (I.E. A CHIEF INFORMATION SECURITY OFFICER).

Businesses today understand that protecting their tangible assets is fundamental for survival. When it comes to cyber security, it is no different. Digital assets, such as customer data, intellectual property, financial plans and general ledgers, staff records and payroll data, and transaction logs and machine data are often the building blocks of many modern businesses.

With this in mind, the need for a robust and tailored approach to continually strengthening a business's resilience against cyber risks must be considered as part of its approach to risk management. The size of the business, its industry and its location do not matter – it must be protected.

The first step on the path to cyber resilience is an understanding of risks and the most appropriate way to address them. For many businesses some challenges come as they embark on the first step. The key is knowing what questions should be asked. We've learnt it is the following:

• What are the emerging cyber security threats and vulnerabilities in your industry?
• How do they impact your type of business or industry sector?
• How good are your security controls to defend against these risks?
• Is this within your risk appetite?
• Can you respond effectively to a cyber incident?

These questions are not unique to any specific organisation or industry sector. Every organisation should be in a position to confidently answer them.

BDO and AusCERT have regular conversations with organisations who want to understand industry trends and how their cyber security strategies compare to industry peers. Although there is a lot of industry research and benchmark data available, it is mainly global data focussing on large multinational enterprises.

In August 2016, we collaborated to launch the inaugural 2016 Cyber Security Survey to source local, representative benchmark data of the cyber security strategies of Australian and New Zealand organisations. We received strong support from industry, with more than 400 respondents across a variety of industry sectors.

Drawing upon the intentions of both Australia's Cyber Security Strategy and New Zealand's Cyber Security Strategy, we set out to learn more about the current cyber threat and response landscape, particularly for small and medium sized businesses and the government sector in our region.

The value of the benchmark data we have obtained with industry's support in 2016 is significant. It not only provides a snapshot of the current state of the cyber landscape in Australia and New Zealand, but it also allows businesses to conduct local benchmarking, which we believe is essential for thorough cyber resilience planning.

We intend to build upon this each year, creating what we believe will become a meaningful reference of trend data for Australian and New Zealand businesses to use in their cyber security planning and risk management programs.

47% OF RESPONDENTS HAVE IMPLEMENTED SECURITY AWARENESS TRAINING FOR STAFF.

Respondents by size, based on annual revenue

MORE THAN $250M
18.2%

UP TO $2.5M
35.0%

$2.5M TO $250M
46.8%
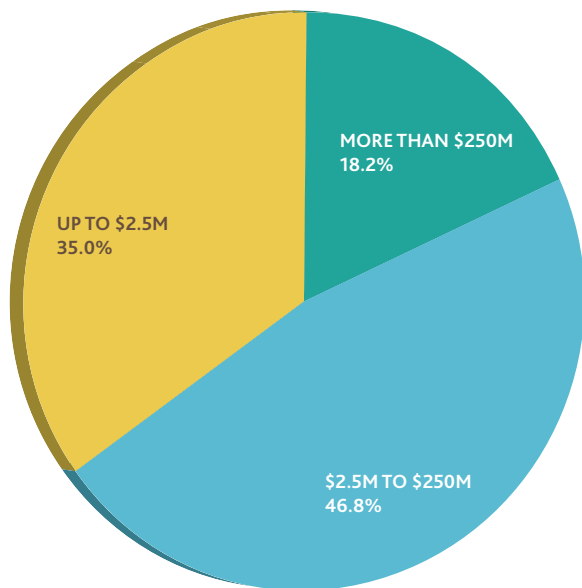
MANY RESPONDENTS HAVE ALREADY TAKEN UP ENDPOINT AND GATEWAY CONTROLS LIKE ANTI-VIRUS (**93%**), WEBSITE AND INTERNET FILTERING (**75%**), AND EMAIL FILTERING TO BLOCK SUSPICIOUS EMAILS (**91%**).

52%

OF RESPONDENTS ARE PERFORMING REGULAR SECURITY RISK ASSESSMENTS, BUT ONLY **49%** REGULARLY REPORT CYBER RISKS TO THE BOARD.

40%

OF RESPONDENTS CAN DETECT SECURITY INCIDENTS, BUT ONLY **21%** HAVE A SECURITY OPERATIONS CENTRE IN PLACE TO INVESTIGATE AND RESPOND TO SECURITY INCIDENTS.

Respondents by location

WESTERN AUSTRALIA 8.6%

SOUTH AUSTRALIA 8.6%

QUEENSLAND 43.2%

NEW SOUTH WALES 17.7%

AUSTRALIAN CAPITAL TERRITORY 4.5%

VICTORIA 16.0%

TASMANIA 1.4%

NORTHLAND 1.7%

AUCKLAND 35.3%

BAY OF PLENTY 4.3%

WAIKATO 17.2%

GISBORNE 2.6%

TARANAKI 1.0%

HAWKE'S BAY 1.7%

MANAWATU - WHANGANUI 1.8%

WELLINGTON 17.2%

CANTERBURY 8.6%

OTAGO 3.4%

SOUTHLAND 5.2%
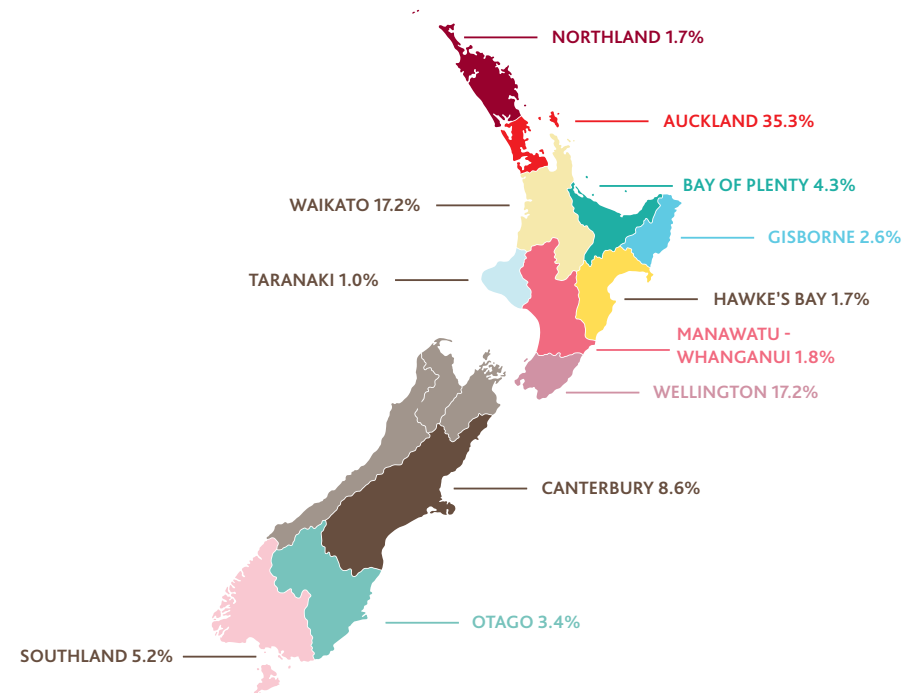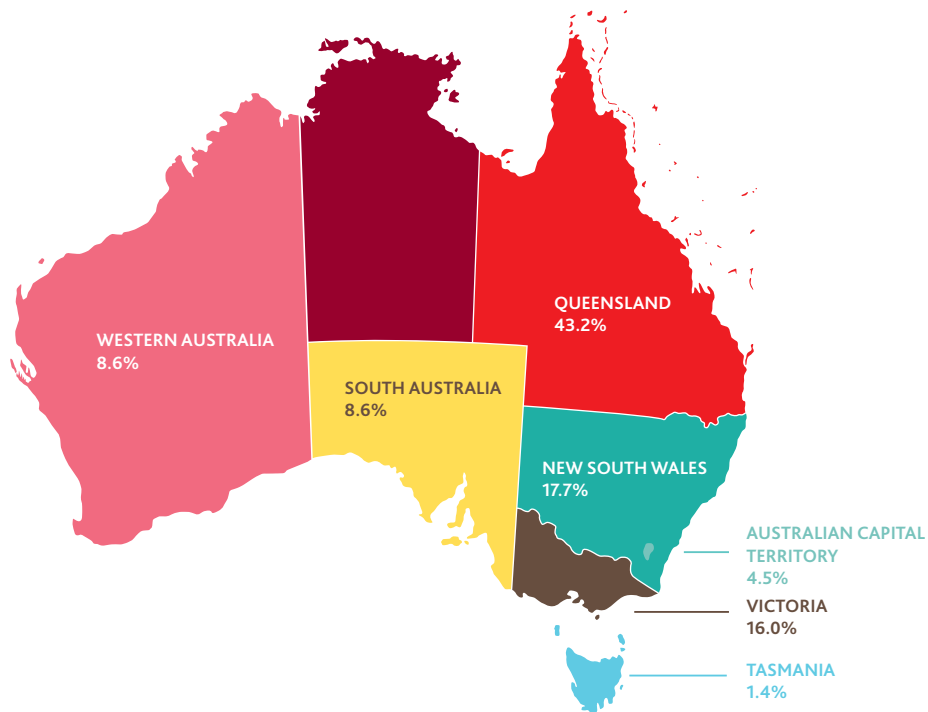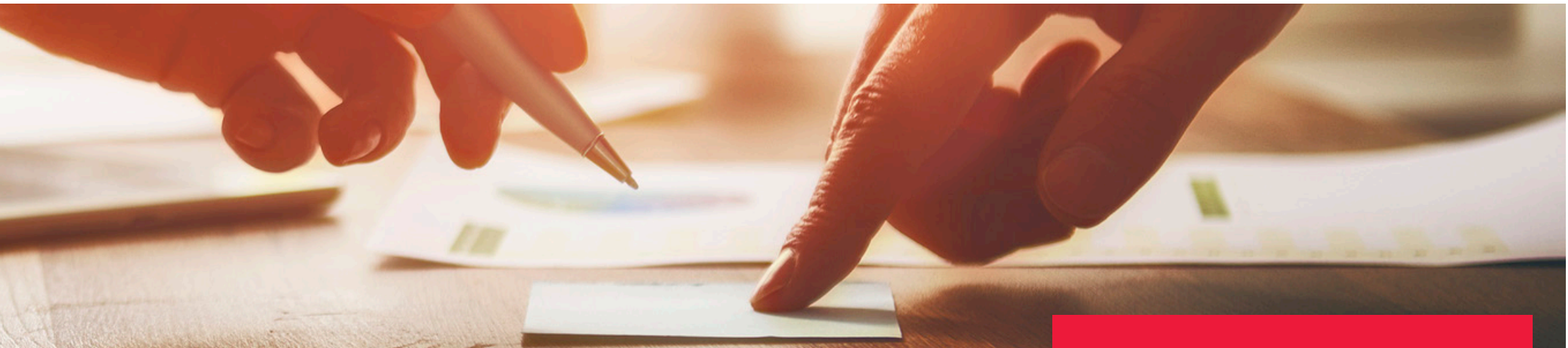
Respondents by industry sector

- ■ WHOLESALE TRADE
- ■ TRANSPORT, POSTAL AND WAREHOUSING
- ■ RETAIL TRADE
- ■ RENTAL, HIRING AND REAL ESTATE SERVICES
- ■ PUBLIC ADMINISTRATION AND SAFETY
- ■ PROFESSIONAL, SCIENTIFIC AND TECHNICAL SERVICES
- ■ OTHER
- ■ MINING
- ■ MANUFACTURING
- ■ INFORMATION MEDIA AND TELECOMMUNICATIONS
- ■ HEALTHCARE AND SOCIAL ASSISTANCE
- ■ FINANCIAL AND INSURANCE SERVICES
- ■ ELECTRICITY, GAS, WATER AND WASTE SERVICES
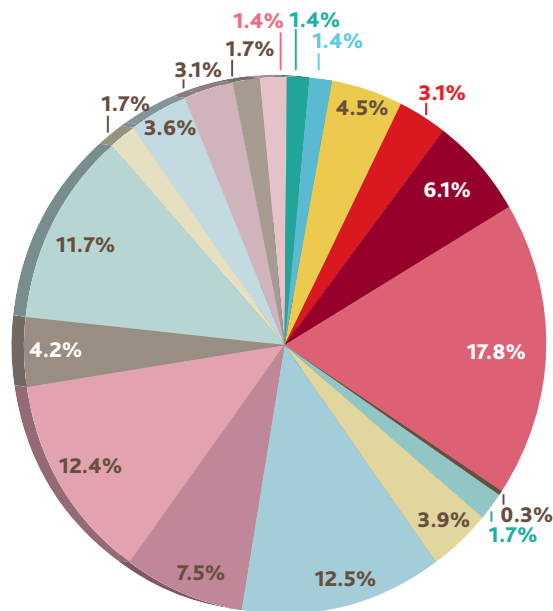
- ■ EDUCATION AND TRAINING
- ■ CONSTRUCTION
- ■ ARTS AND RECREATION SERVICES
- ■ AGRICULTURE, FORESTRY AND FISHING
- ■ ADMINISTRATIVE AND SUPPORT SERVICES
- ■ ACCOMMODATION AND FOOD SERVICES

Pie chart values: 1.4% 1.4% 1.4% 1.4% 1.7% 3.1% 4.5% 3.1% 1.7% 3.6% 6.1% 11.7% 17.8% 4.2% 12.4% 0.3% 1.7% 7.5% 12.5% 3.9%

48%

OF RESPONDENTS HAVE A CYBER INCIDENT RESPONSE PLAN IN PLACE AND ONLY **41%** HAVE A CYBER INCIDENT RESPONSE TEAM OR CAPABILITY IN PLACE TO RESPOND TO INCIDENTS.

44%

OF RESPONDENTS HAVE DEFINED SECURITY STANDARDS FOR CLOUD AND THIRD PARTIES OR SUPPLY CHAIN.

THE INCREASING IMPORTANCE OF CYBER *SECURITY*

Company Boards and Executives are taking an increasingly active interest in the cyber security practices of their businesses. Legislative changes currently on the table, including the *Privacy Amendment (Notification of Serious Data Breaches) Bill 2015*, are contributing to this focus, as is the increased reporting of breaches. In 2016 we have seen a number of high profile data breaches from across the region and globally that have captured the attention of senior management. These events have illustrated very clearly the reputational, operational and financial impacts that a cyber security incident can inflict on an organisation.

Damage to brand and reputation

Consumers are increasingly concerned about their privacy. They are more informed about the impacts of information about them being stolen by criminals or being released into the public domain. Customers and consumers of services, have an expectation of every organisation to keep information about them safe. The size, type or function of an organisation matter very little when it comes to the customers' expectations about cyber security.

Loss of intellectual property

While the reputational impact associated with a cyber security incident can be severe, the loss of intellectual property can be crippling. Some researchers estimate that intellectual property constitutes around three quarters of a company's value, yet some organisations overlook the business risk that the theft or loss of access to trade secrets and proprietary information can have. These impacts can be costly, including a direct loss of profit or decrease in share price or valuation. Cyber security incidents impacting intellectual property can also cause a loss of market advantage and missed business opportunities or irreparable damage to reputation.
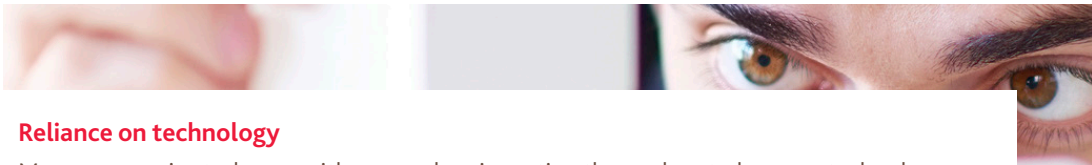
Reliance on technology

Many companies today are either eagerly reinventing themselves to become technology companies in their own right, or are born from capitalising on the latest information technology advancement. Cyber security incidents can impact on an organisation's core infrastructure, disrupt its ability to function or simply take it completely offline. When a cyber security incident directly impacts the organisation's ability to operate due to a complete loss of access to systems or the destruction of digital assets, some businesses simply cease to exist.

Not just an issue for the 'big end of town'

The majority of cyber security related incidents being reported in the media today involve large organisations. They suffer financial losses related to fines, impacts to their share price, a lack of confidence from consumers, or are forced to admit their previous failings. All of this will require significant focus and steps to address cyber security better in the future. It is critical for all our economic futures that businesses understand cyber security incidents do not just befall large companies and government departments. The impacts of incidents can be felt most heavily by smaller business. There are numerous victims of cyber security incidents whose story does not make it as far as the news. When a cyber security incident occurs in a small or medium size business it could have a major impact on the business causing it to close down.

The range of threats changes constantly. A big concern is phishing attacks for contacts details and system access. We have had phone calls attempting to get data that would aid a cyber attack. Private company in the Electricity, gas, water and waste water services industry.

What is the one thing that concerns you most about cyber security in your organisation today?

Education of staff about information security. Staff can be naive about security implications and see security precautions as an inconvenience. Having them understand the importance of proper security processes and procedures is a challenge – Not-for-profit in the Healthcare sector.

People and staff are the weakest link. A lot of money can be spent on IT technologies, but they can all be bypassed by the end user being compromised. Security Awareness is the most important task that an organisation can perform to reduce the risk of a cyber attack. Technologies are only one piece of the puzzle – State government department.

Resources who focus on security and compliance/policy requirements are not up to date with current threat landscape. We spend significant efforts addressing low value security activities because they are required to tick a compliance tick-box while time and effort could be better spent focusing on true security – Private company in the Financial services sector.

As a small home based business in a small rural town it is difficult to know who to ask to visit the home office and provide IT support. While there is no shortage of people advertising their skills etc, they seem to be unregulated and you have to believe what they tell you. You take a stab in the dark and hope they can fix/help you and fingers crossed it's good advice – Privately owned property developer.

We are a small medium enterprise but most of today's technology is more aimed at Large corporates along with its costing. While we are aware of the potential risks, we cannot fully cover that risk to the advice provided due to resourcing and costings. We have to mitigate this as much as possible by taking out Cyber Insurance, which once again do not provide full risk cover – Not for profit organisation in Education & training sector.

Zero Days on a myriad of vendor hardware. Even assuming patching is completed regularly and diligently and regardless of network/device security, these exploits can compromise security. Traffic monitoring is limited and may not catch properly hidden exfiltration – Public listed company in the Information, Media and Telecommunications sector.

Underestimation or limited understanding of cyber security risks by senior executives. Willingness to make decisions without fully understanding the associated business and technical impacts. Immature business analysis, design/architecture, project/program management, and risk management capabilities – Government department.

Lack of internal understanding of the risk awareness exists but not understanding. Given our size we are heavily dependent on our outsourced IT function. This is new as of mid 2016 so we are yet to fully 'road test' the vendors capabilities – Public listed company in the professional services and technical services industry.

VIEW OF CYBER SECURITY MATURITY ACROSS INDUSTRY

Adoption status of cyber security controls (across all respondents)

This survey captured information about respondents' adoption of security technologies, the maturity of their processes, and the cyber security knowledge and capability of business leaders, IT engineers and employees in general.

The results show that although many organisations have already adopted traditional technologies to address the delivery and propagation of viruses and malware, many organisations are yet to truly adopt a risk based approach for cyber security.

Legend:
- ALREADY OR CURRENTLY BEING ADOPTED
- PLAN TO ADOPT WITHIN NEXT 12 TO 24 MONTHS
- NOT CURRENTLY PLANNED OR DO NOT KNOW

SECURITY CONTROLS	Already or currently being adopted	Plan to adopt within next 12 to 24 months	Not currently planned or do not know
CYBER SECURITY INCIDENT RESPONSE TEAM/CAPABILITY	41.4%	22.0%	36.6%
CYBER SECURITY INCIDENT RESPONSE PLAN	48.1%	23.5%	28.4%
SECURITY OPERATIONS CENTRE	20.9%	20.1%	59.0%
THREAT AND VULNERABILITY SCANNING	65.7%	11.9%	22.4%
APPLICATION WHITELISTING	34.0%	20.5%	45.5%
SECURITY INFORMATION AND EVENT MANAGEMENT SYSTEM	40.3%	20.5%	39.2%
MOBILE DEVICE MANAGEMENT SYSTEM (MDM)	41.8%	25.0%	33.2%
WEBSITE AND INTERNET FILTERING (PROXY SERVER)	74.6%	6.4%	19.0%
EMAIL FILTERING SYSTEM TO BLOCK SUSPICIOUS EMAILS	91.0%	3.7%	5.3%
INTRUSION PREVENTION SYSTEM (IPS)	61.9%	14.6%	23.5%
INTRUSION DETECTION SYSTEM (IDS)	58.6%	15.3%	26.1%
DATA LOSS PREVENTION SYSTEM (DLP)	51.5%	22.8%	25.7%
ANTI-VIRUS/MALWARE PROTECTIONS	92.6%	3.7%	3.7%
PATCH MANAGEMENT PROCESSES	66.8%	10.4%	22.8%
PRIVILEGED ACCOUNT MANAGEMENT	66.4%	14.2%	19.4%
IDENTITY AND ACCESS MANAGEMENT SYSTEM	61.6%	20.1%	18.3%
PROCESS TO IDENTIFY CRITICAL SYSTEMS AND DATA	57.8%	26.2%	16.0%
CYBER SECURITY RISK REPORTING TO THE BOARD/EXECUTIVES	49.6%	24.3%	26.1%
THIRD PARTY/VENDOR RISK ASSESSMENTS	39.9%	27.6%	32.5%
REGULAR CYBER SECURITY RISK ASSESSMENTS	51.9%	28.4%	19.7%
CYBER SECURITY AWARENESS PROGRAM	47.4%	34.0%	18.6%
CHIEF INFORMATION SECURITY OFFICER (CISO)	18.7%	10.8%	70.5%
CLOUD SECURITY STANDARDS	44.4%	33.2%	22.4%
IT/CYBER SECURITY STANDARDS/BASELINES FOR THIRD PARTIES	42.9%	31.0%	26.1%
IT/CYBER SECURITY POLICY	62.3%	22.4%	15.3%

PERCENTAGE

What is the best piece of advice you would give a colleague or friend regarding cyber security?

Unless you know the value of the information you are protecting, you won't be able to work out what to spend on protecting it – Not for profit organisation in Healthcare sector.

Do risk assessments and provide these upwards - let the business reject them – don't give execs surprises – Public listed company in Information, Media and Telecommunications industry.

Make employees more aware of issues and have a six monthly (at least) cyber security audit internally – Government owned entity in the Electricity, gas, water and wastewater sector.

Everyone needs to take it seriously end users have to protect business data like it was their own. If you would not give out your PIN number for you credit card out randomly, then treat you work credentials with the same respect – State government department.

Ensure you have good backups that include ALL critical data and your restore process has been tested. It is pretty much a matter of time before you will be hit with Ransomware at some point so recovering from backup will need to occur – Private company in the Information, Media and Telecoms sector.

Bunker down - be diligent in managing access to your systems and minimise the access points to the system. Resist the temptation to open the system to more usability (which can mean compromising access controls) – Private company in Rental and real estate services sector.

Compliance initiatives are as much a cultural change, as it is a process change. Active security awareness of personnel is more effective than any Anti virus or host-based intrusion detection system as intrusion vectors target the lowest hanging fruit, in terms of exploit complexity. Building a culture of improving compliance and being technically adept, by building a rapport with all staff is important in maximizing visibility – Public listed company in Information, Media and Telecommunications sector.

1. Identify and understand the cyber security threats, risks and vulnerabilities that your system/organisation is exposed to
2. Develop and implement treatment strategies (including technical, operational and process-based controls) to mitigate, resolve or accept these items
3. Continuously monitor and improve your system/organisation to ensure emerging threats, risks and vulnerabilities are also managed effectively – Federal government department.
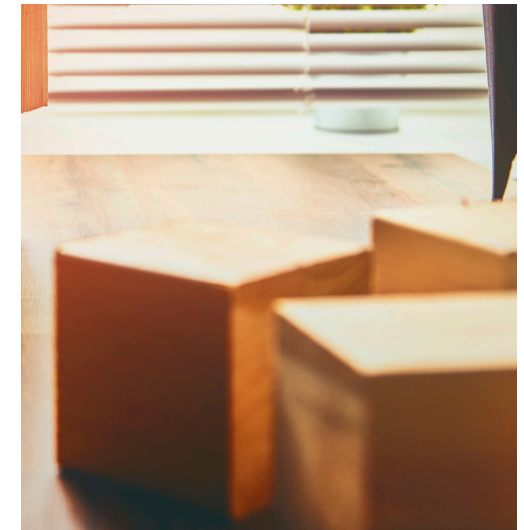
Patch, have good backups, have an incident response plan, assess your IT risks and tackle in order of business impact – Public listed company in Arts and recreational sector.

Be alert, not alarmed, and always notify the security team of suspicious activities. Their involvement contributes to a human firewall that protects the organisation just as much as technology controls – Private company in Professional, scientific and technical services industry.

Technology

93%

Anti-virus – 93% of respondents have already adopted or are currently adopting anti-virus controls.

It is not surprising to see such a high maturity in the use of anti-virus technologies. This basic security control protects organisations from most known threats and is seen as an essential application in most desktop and server deployments.

When respondent data was broken down into industries and sectors, it was surprising to see the lowest adoption of anti-virus was in the health care sector, with only 88% of respondents reported to have adopted anti-virus.

91%

Email filtering – 91% of respondents have already adopted or are currently adopting email filtering controls.

Email filtering is utilised by most industry sectors. 100% of government services, transport, and mining industry respondents indicated they have fully implemented this control and rated it as effective.

Although the survey results show a very high implementation rate for email systems to block suspicious and malicious content, a significant portion of the reported incidents are still caused by malicious phishing emails. Businesses must ensure they are adequately complementing their investments in anti-virus and email filtering with user awareness and continuous monitoring of how attacks are changing to remain well protected.

Process

21%

Security operations centre – Only 21% of respondents reported having a security operation centre in place, and 59% indicated they do not intend to implement one in the near future.

Security information and event management tools provide visibility of cyber incidents that are occurring on a business's network. When monitored by in-house security specialists or a security operations centre, security incidents can be detected and responded to in a much more timely manner, helping improve the overall response approach.

52%

Risk assessments – 52% of respondents have processes in place to conduct regular cyber security risk assessments, yet only 40% of the responders have a process in place to conduct third party/vendor risk assessments.

Organisations are rapidly adopting new technologies and partnering with third parties to conduct critical business processes. However, many organisations do not have repeatable processes in place to consider and assess the risks associated with these decisions. Such risks can severely impact on the organisation's ability to conduct its business if the third party or new technology solutions fail to deliver the desired outcomes.

■ HIGH MATURITY　　**■ MODERATE MATURITY**　　**■ LOW MATURITY**

67%

Patching – 67% of respondents have a patch management process in place.

System and application vulnerabilities are one of the main reasons why cyber attacks are successful. System owners and administrators have a big role to play when it comes to protecting their assets by ensuring vulnerabilities are addressed and vendor supplied patches for operating systems and applications are patched frequently.

The Information, Media and Telecommunications sector reported the highest adoption of patching processes, demonstrating that this sector is more aware of the risks associated with running vulnerable software.

67%

Privileged/administrative access management - 67% of respondents have implemented controls to manage privileged/administrative access rights.

As users become more independent and IT savvy, their reliance on system administrators drops. An increased number of business users now demand administrative access to allow them to customise their devices and install their own applications. This increases the risk exposure for the organisation as criminals will have full access to systems and data of compromised accounts.

People # 70%

Chief Information Security Officer – More than 70% of respondents indicated that they never intend to fund a dedicated role to manage cyber security outcomes for their organisation.

For smaller businesses, a role dedicated to managing cyber security risk is probably not viable, but that doesn't eliminate the need for someone in the business to take responsibility for it and drive security outcomes.

It is important for Senior Management to get more involved in managing cyber risks within their business. They must be committed to learning more about cyber risks and manage them adequately to ensure their business is protected and can continue to operate with relevance.
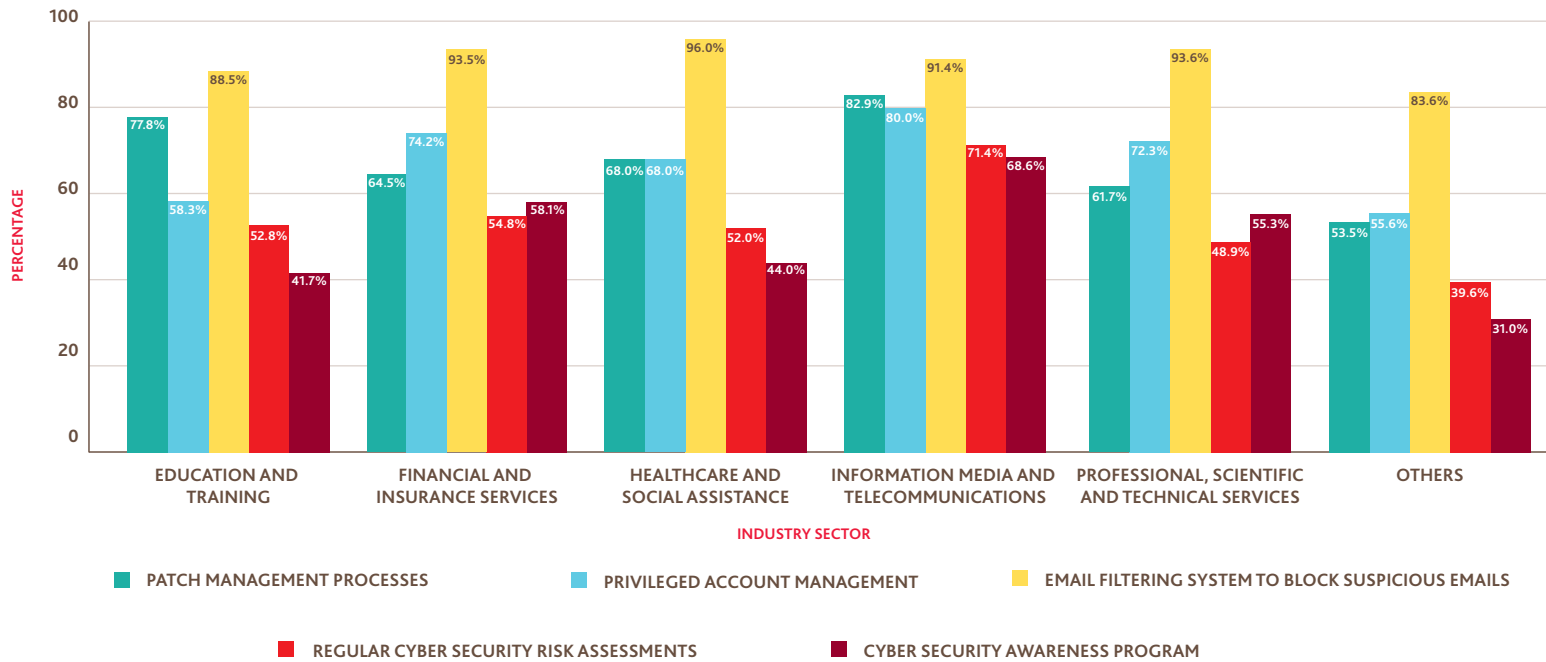
50%

Board and senior management education – Only 50% of the respondents indicated they had established regular cyber security risk reporting to their Boards and executives.

Cyber security risks can threaten the reputation and financial stability of an organisation, regardless of its size. It is essential for Boards and executives to be educated about the impact and likelihood of a security incident, and what the organisation's capabilities are to defend against it.
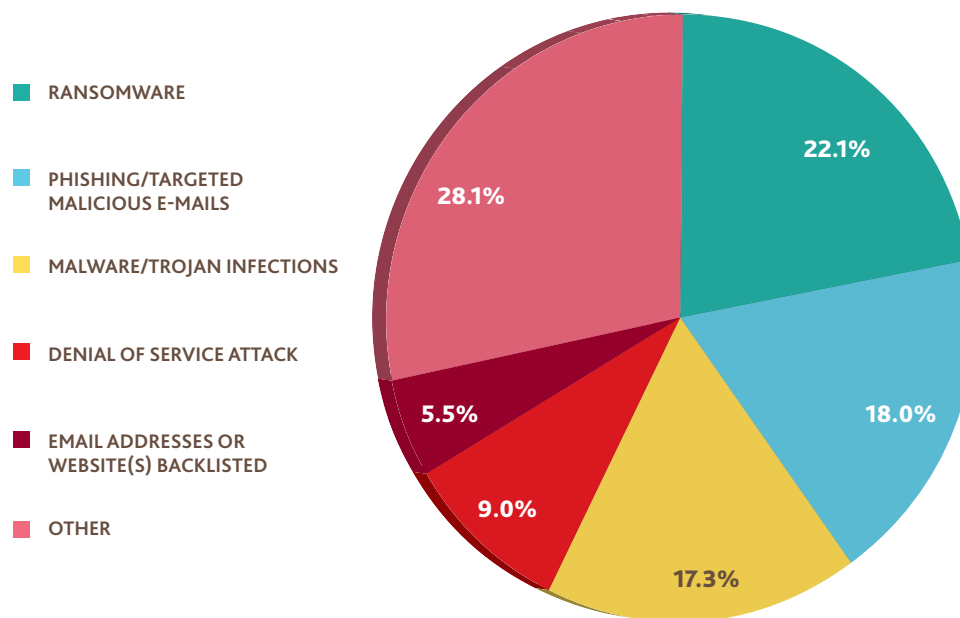
Cyber security controls already or currently being adopted (per industry sector)

PATCH MANAGEMENT PROCESSES

PRIVILEGED ACCOUNT MANAGEMENT

EMAIL FILTERING SYSTEM TO BLOCK SUSPICIOUS EMAILS

REGULAR CYBER SECURITY RISK ASSESSMENTS

CYBER SECURITY AWARENESS PROGRAM

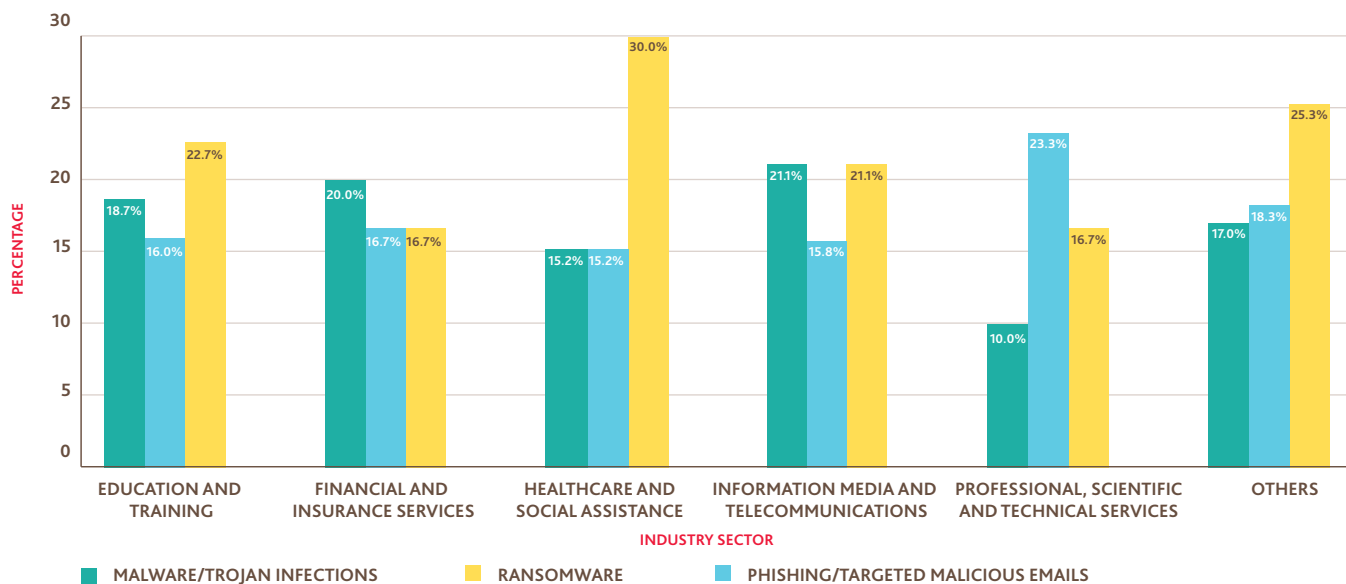# HOW ARE BUSINESSES BEING IMPACTED BY CYBER SECURITY INCIDENTS

CYBER SECURITY INCIDENT	PERCENTAGE OF RESPONDENTS WHO EXPERIENCED AN INCIDENT (ACROSS ALL RESPONDENTS)
Data breach and third party provider/supplier	5.2%
Data loss/theft of confidential information	5.2%
Denial of service attack	9.0%
Brute force attack	2.8%
Email addresses or website(s) blacklisted	5.5%
Malware/trojan infections	17.3%
Phishing/targeted malicious emails	18.0%
Ransomware	22.1%
Theft of laptops or mobile devices	3.8%
Unauthorised access to information by external user	3.5%
Unauthorised access to information by internal user	3.8%
Unauthorised modification of information	1.4%
Website defacement	2.4%

Cyber security incidents experienced last financial year (across all respondents)

- RANSOMWARE
- PHISHING/TARGETED MALICIOUS E-MAILS
- MALWARE/TROJAN INFECTIONS
- DENIAL OF SERVICE ATTACK
- EMAIL ADDRESSES OR WEBSITE(S) BACKLISTED
- OTHER

22.1%
18.0%
17.3%
9.0%
5.5%
28.1%

Top three cyber security incidents experienced last financial year (by industry sector)

Bar chart — PERCENTAGE (y-axis, 0 to 30) by INDUSTRY SECTOR (x-axis).

Industry sector	Malware/Trojan infections	Ransomware	Phishing/Targeted malicious emails
Education and training	18.7%	22.7%	16.0%
Financial and insurance services	20.0%	16.7%	16.7%
Healthcare and social assistance	15.2%	30.0%	15.2%
Information media and telecommunications	21.1%	21.1%	15.8%
Professional, scientific and technical services	10.0%	16.7%	23.3%
Others	17.0%	25.3%	18.3%

Legend: ■ MALWARE/TROJAN INFECTIONS ■ RANSOMWARE ■ PHISHING/TARGETED MALICIOUS EMAILS

Survey respondents shared information about the incidents they experienced over the past financial year, and the results show that most organisations had been impacted with ransomware, malware (malicious code) and phishing incidents.

Combined, these three incident types accounted for 57% of all incidents reported. The correlation between ransomware, malware and phishing is not overly surprising given how malicious individuals often leverage these together in their criminal efforts.

Ransomware – Cyber criminals are increasingly taking over systems, blocking business and users from accessing essential business data, and holding them to ransom. Results indicate that businesses of varying sizes have all been impacted by ransomware, despite the security controls they have available to protect them against these types of cyber attacks.

A significant number of respondents admitted to paying the ransom in order to resume their businesses, as the cost of implementing the necessary controls and capabilities are often seen as too high. These types of attacks will continue to increase until such time as organisations stop paying ransoms and they implement security controls to protect them against these attacks.
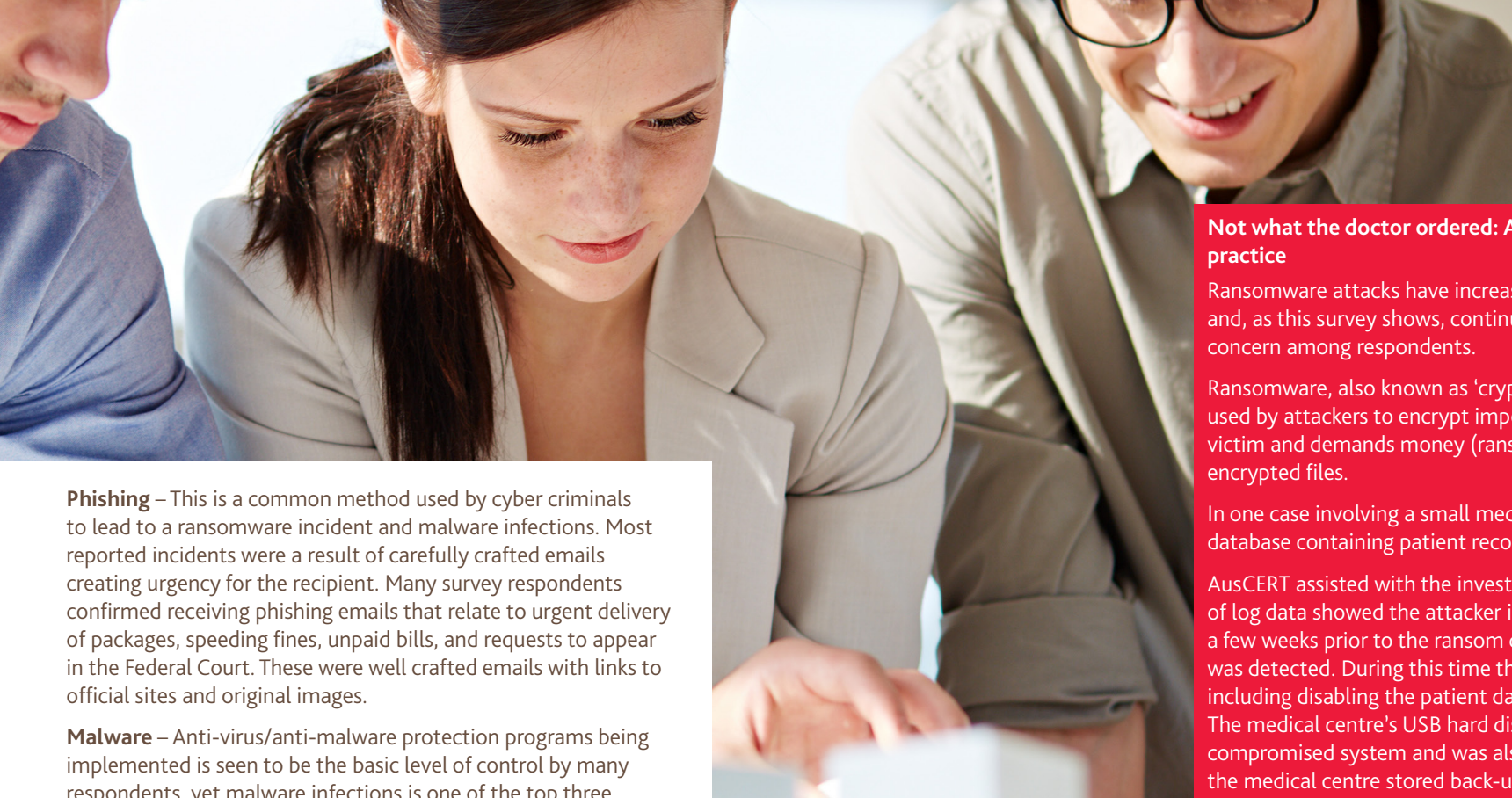
Phishing – This is a common method used by cyber criminals to lead to a ransomware incident and malware infections. Most reported incidents were a result of carefully crafted emails creating urgency for the recipient. Many survey respondents confirmed receiving phishing emails that relate to urgent delivery of packages, speeding fines, unpaid bills, and requests to appear in the Federal Court. These were well crafted emails with links to official sites and original images.

Malware – Anti-virus/anti-malware protection programs being implemented is seen to be the basic level of control by many respondents, yet malware infections is one of the top three reported incident types.

Ransomware incidents were particularly prevalent in the healthcare sector. Health records are sensitive in nature and access to such data is critical. Ransomware incidents would significantly impact the operational capabilities of hospitals and medical clinics and damage their reputation.

Basic anti-virus solutions are limited in their ability to detect sophisticated malware that attempts to evade detection. It is also important to ensure anti-virus programs are implemented across the entire network and kept up to date. 100% coverage can be difficult to achieve in organisations that allow personal devices to connect to the corporate network without appropriate controls. Organisations should consider implementing other controls such as attachment sandboxing, web filtering, and application whitelisting to reduce the number of successful infections.

Not what the doctor ordered: A ransomware incident at a medical practice

Ransomware attacks have increased significantly over the past few years and, as this survey shows, continue to be one of the highest areas of concern among respondents.

Ransomware, also known as 'crypto locker', is a form of malicious code used by attackers to encrypt important files. The attacker contacts the victim and demands money (ransom) in exchange for recovering the encrypted files.

In one case involving a small medical practice, the attacker encrypted a database containing patient records and demanded $4,000 to decrypt it.

AusCERT assisted with the investigation and recovery. An examination of log data showed the attacker infiltrated the medical centre's systems a few weeks prior to the ransom demand and before the intrusion was detected. During this time the attacker made numerous changes, including disabling the patient database in the tape backup scheduler. The medical centre's USB hard disk backup device was plugged into the compromised system and was also encrypted by the attacker. Although the medical centre stored back-ups off site, after a few weeks of tape rotations, recent back-ups were no longer available.
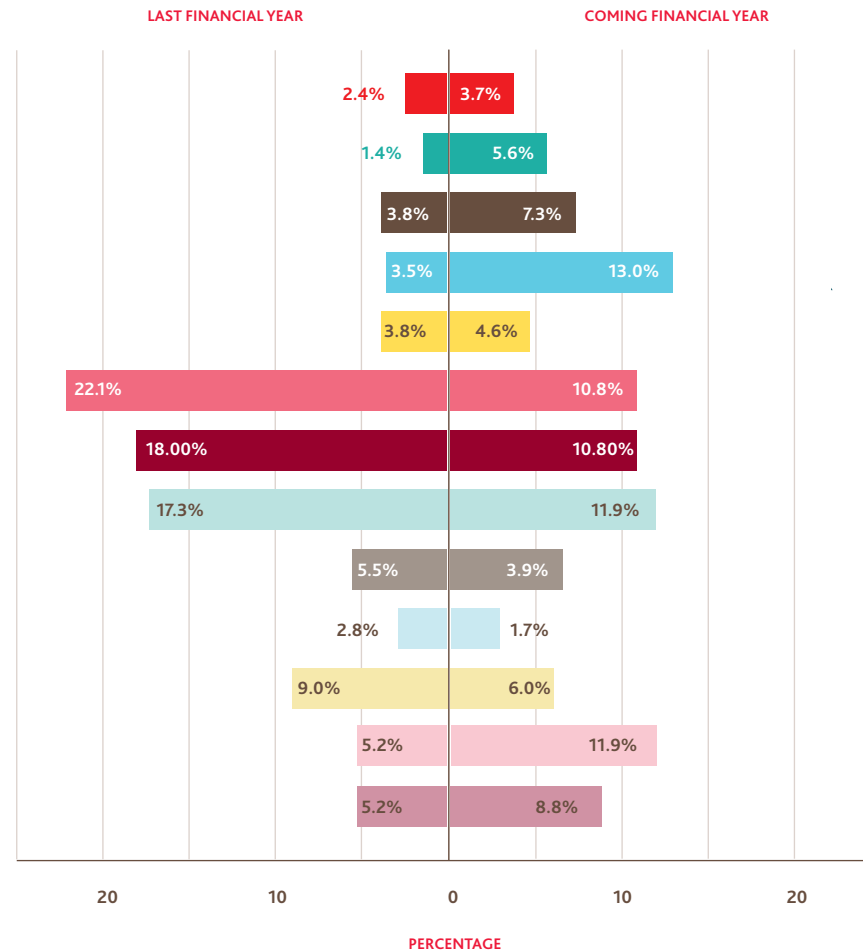
AusCERT advised the medical centre to erase and rebuild the server and recover older data from back-up tapes. While the medical centre had a number of good security practices in place, they were not enough to prevent or detect the attack and recovery was only partially successful.

It is possible that the attack could have been much worse and affected the medical practice's patients too. With full access to patient records containing personal identifying information, the attacker could have used this information for identity theft related fraud.

A comprehensive review of all its risks and security practices helped the medical centre identify ways to better prevent, detect and respond to cyber attacks in future.

WHAT HAS HAPPENED AND WHAT TO EXPECT

LAST FINANCIAL YEAR   **COMING FINANCIAL YEAR**

Legend:
- WEBSITE DEFACEMENT
- UNAUTHORISED MODIFICATION OF INFORMATION
- UNAUTHORISED ACCESS TO INFORMATION BY INTERNAL USER
- UNAUTHORISED ACCESS TO INFORMATION BY EXTERNAL USER
- THEFT OF LAPTOPS OR MOBILE DEVICES
- RANSOMWARE
- PHISHING/TARGETED MALICIOUS E-MAILS
- MALWARE/TROJAN INFECTIONS
- EMAIL ADDRESSES OR WEBSITE(S) BLACKLISTED
- BRUTE FORCE ATTACK
- DENIAL OF SERVICE ATTACK
- DATA LOSS/THEFT OF CONFIDENTIAL INFORMATION
- DATA BREACH AND THIRD PARTY PROVIDER/SUPPLIER

Category	Last Financial Year	Coming Financial Year
WEBSITE DEFACEMENT	2.4%	3.7%
UNAUTHORISED MODIFICATION OF INFORMATION	1.4%	5.6%
UNAUTHORISED ACCESS TO INFORMATION BY INTERNAL USER	3.8%	7.3%
UNAUTHORISED ACCESS TO INFORMATION BY EXTERNAL USER	3.5%	13.0%
THEFT OF LAPTOPS OR MOBILE DEVICES	3.8%	4.6%
RANSOMWARE	22.1%	10.8%
PHISHING/TARGETED MALICIOUS E-MAILS	18.00%	10.80%
MALWARE/TROJAN INFECTIONS	17.3%	11.9%
EMAIL ADDRESSES OR WEBSITE(S) BLACKLISTED	5.5%	3.9%
BRUTE FORCE ATTACK	2.8%	1.7%
DENIAL OF SERVICE ATTACK	9.0%	6.0%
DATA LOSS/THEFT OF CONFIDENTIAL INFORMATION	5.2%	11.9%
DATA BREACH AND THIRD PARTY PROVIDER/SUPPLIER	5.2%	8.8%

PERCENTAGE

Looking forward, respondents continue to express concerns over incidents and issues they experienced during the previous financial year.

However, there is a significant spike in concerns for respondents on incidents related to unauthorised access to/loss of data (whether by internal or external sources), compared to the availability of services they offer due to a denial of service attack. Since denial of service protection tools are gaining more maturity in the market, there is likely confidence that businesses can protect themselves as they implement these tools. However, businesses are struggling to manage third parties and implement processes to manage access privileges as they adopt new technologies and ways of working. As the use of cloud solutions increases, and the network perimeter becomes more transparent, organisations need to prepare themselves by having the right tools and processes in place to manage security risks directly under their control.

They can start with the simple step of identifying what the key external data sources and applications are that they have outsourced to third parties and ensure these have effective security controls in place. This will provide them with insights into the cyber risks in their supply chain and what strategies they need to implement to make them more cyber resilient.

Gone phishing: Hooking a CIO

Some cyber attacks involve tricking people to disclose their username or password, opening a malicious file or other action designed to help an attacker get access to systems or data. AusCERT handles thousands of phishing attacks each year.

In one case, the Personal Assistant (PA) of a CIO received an email from a company they had previously dealt with, requesting that the CIO read, sign and return the attached document to finalise the deal. The document asked for the CIO's username and password, which the PA knew, so they entered these details.

The email request was convincing because an email account from the sender company had been hacked allowing the attacker to read the previous email trail between the companies and impersonate the company.

When the PA entered the CIO's username and password, the details were sent to the attacker, enabling them to log in to the CIO's Office 365 email account. The attacker then sent a phishing email from the CIO's email account to their contacts requesting they click a link and follow the instructions given. The link redirected victims to an Office 365 phishing kit asking for the username and password of the victim's organisation account.

More than 1,000 of the CIO's contacts received the phishing email. Many recipients (particularly her employees) took the email seriously, believing it was from the CIO, and clicked on the link. Some recipients thought the request was odd and replied by email asking whether this was a legitimate request. As the attacker still had control of the CIO's mailbox, they replied it was. The attacker also deleted the CIO's contacts and all emails including sent and deleted items. The attacker created an automatic rule sending all future emails directly to the trash.

AusCERT provided onsite assistance to help the company contain and recover from the incident, shut down the phishing site, and provided mitigation advice to the CIO's contacts (internal and external) who may also have been targeted. The case highlights the importance of user awareness training about not sharing passwords and having in place appropriate back-ups.

CYBER INSURANCE AS A RISK MANAGEMENT STRATEGY

Responses for all respondents

- ■ YES - WE HAVE THIS COVER AS AN EXTENSION TO ANOTHER INSURANCE POLICY
- ■ YES - WE HAVE A STANDALONE CYBER POLICY
- ■ YES - BUT DO NOT KNOW HOW THE POLICY WAS ARRANGED
- ■ NOT YET - WE ARE CONSIDERING IT
- ■ NO - WE WERE NOT AWARE OF THIS TYPE OF INSURANCE
- ■ NO - WE SELF-INSURE
- ■ NO - WE DON'T FEEL WE NEED IT
- ■ NO - WE BELIEVE THIS RISK IS COVERED UNDER OTHER INSURANCE POLICIES WE HAVE

Pie chart values: 13.7%, 9.4%, 4.7%, 24.6%, 18.4%, 9.4%, 12.3%, 7.5%
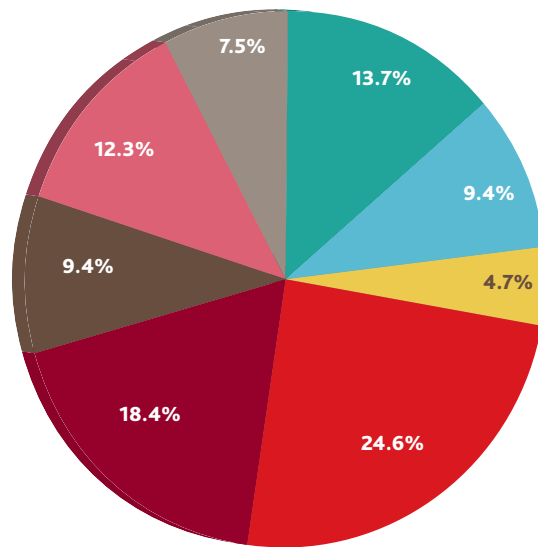
Cyber insurance as a risk management tool is in the early stages of adoption, with only 27.8% of respondents indicating they have insurance in place, 24.5% considering it and 9.4% having made the decision to self-insure.

Of the 27.8% of respondents who have cyber insurance in place, 56% are performing regular cyber security risk assessments while only 31% are performing third party/vendor risk assessments.

As highlighted earlier, only 52% of organisations are performing regular security risk assessments. This suggests that nearly half of all respondents don't have an accurate view of their cyber risks. This raises the question as to whether those organisations who have taken out cyber insurance, have policies in place that will respond to insurance claims.

Ensuring cyber insurance fits your business

1. Identify your cyber risks and gaps – both within your environment and with third parties/vendors.
2. Determine the value of your data and how inherent it is to your operations – it might not sit on your balance sheet, but it could be the largest asset you have.
3. Quantify the impact of a breach and model its operational impact – do you know what it would cost your business to recover, including forensic investigation, loss of revenue, business interruption costs? Would your business be able to continue operating?
4. Assess your protection options – could you put a cyber remediation program in place? Will cyber insurance assist?
5. Insure – if you decide this is part of your business's approach, assess a range of policies and select one that provides the cover you need by looking at your specific cyber risks and use cyber attack or data breach scenarios to confirm the policy will respond to claims for each of those scenarios.
6. Regularly reassess your cyber risk posture – you must do this to confirm your cyber defences and insurance policies are providing you the required mitigation and cover.

How Australia's Cyber Security Strategy addresses cyber security for small to medium size businesses

Key strategic points to consider:

- **Tone at the top:** Industry and business leaders need to get more involved in cyber security and provide clear guidance and direction on the minimum security standards for the organisation

- **Clear insights into cyber threats:** Businesses should conduct security risk assessments more regularly to allow them to better understand the threats and risks for their industry and organisations

- **Improve user awareness and education:** Organisations must provide ongoing tailored user awareness training and education on cyber security as users and their devices are frequently targeted, and users are often the first line of defence against cyber attacks

- **Improve response capability:** Organisations need to put in place an effective cyber security incident response plan and supporting capability to respond to, and recover from cyber security incidents.

ABOUT US

About BDO in Australia and BDO in New Zealand

BDO is one of the world's leading accountancy and advisory organisations. We have clients of all types and sizes, in every sector. Our global reach allows us to remain abreast of industry developments and the emergence of new and evolving cyber security threats. BDO's Cyber Resilience Framework is based on industry best practice, allowing our clients to take a strategic view of their entire cyber security risk management lifecycle. This ensures they can better understand the evolving cyber risk landscape and build their cyber resilience over the long term.

Like every other area of our business, the delivery of our cyber security services is built on relationships. We focus on what's important to our clients and adopt a partnership-style approach. We're responsible and reliable, we keep our promises, and maintain open and frank communication. Using this insight, we look for innovative ways to help clients maximise their growth opportunities, improve processes and avoid pitfalls. The result is that we meet – and exceed – expectations.

BDO in Australia has almost 1,350 partners and staff across Australia, making us one of the countries largest associations of independently owned accounting practices, with offices in New South Wales, Northern Territory, Queensland, South Australia, Tasmania, Victoria and Western Australia.

BDO in New Zealand has more than 850 partners and staff in 15 offices across the North and South Islands, and BDO the fastest growing business services firm in New Zealand.

1,192 STAFF
10 OFFICES
155 PARTNERS
AS AT NOVEMBER 2016 NATIONAL TOTAL 1,347

750+ STAFF
15 OFFICES
91 PARTNERS

About AusCERT

AusCERT (the Australian Cyber Emergency Response Team) is a membership based, independent, self-funded, not-for-profit security team, which is part of The University of Queensland. AusCERT has a national focus across industry and government and a national and global reach. Established in 1993, AusCERT is one of the oldest cyber emergency response teams in the world. AusCERT services help organisations prevent, detect, respond and improve their resilience to cyber attacks. For more details about AusCERT services, please visit AusCERT's web site: www.auscert.org.au.

Contact us

LEON FOUCHE
NATIONAL LEADER, CYBER SECURITY, BDO
Tel: +61 7 3237 5688
leon.fouche@bdo.com.au

THOMAS KING
GENERAL MANAGER, AusCERT
Tel: +61 7 3346 6900
thomas.king@uq.edu.au

BOOK YOUR COMPLIMENTARY CYBER CONSULTATION

NEW SOUTH WALES

NORTHERN TERRITORY

QUEENSLAND

SOUTH AUSTRALIA

TASMANIA

VICTORIA

WESTERN AUSTRALIA

1300 138 991
www.bdo.com.au

Distinctively different – it's how we see you
AUDIT • TAX • ADVISORY