2021 Gallagher Australia CYBER INSIGHTS Report

How to identify risks, reduce exposure and maximise resilience

ajg.com.au/cyber

Gallagher

Insurance | Risk Management | Consulting

Foreword

Today's enterprise risk management programs have moved cyber risk to the top of the list of concerns for organisations, and with good reason. Cyber threats dramatically escalated in 2020 and this negative trend has continued into the first quarter of 2021. Adding to this development, the COVID-19 pandemic contributed to security breaches as employees quickly moved to work from home, creating a greater attack surface for cyber criminals and hostile state sponsored adversaries.

Along with vulnerabilities in the home setting, hackers have exploited the unique set of circumstances with new variants of ransomware and social engineering campaigns. Regulators have taken note and sharpened their focus in state, federal and international jurisdictions. And while politically motivated strike forces mount attacks against institutions and government organisations, the most common threat is from ordinary hackers managing to stay one step ahead of both business and regulators which has been overwhelming for some organisations.

This report was driven by our time-honoured focus on understanding our clients' business concerns and exposures. To assess your ongoing insurance needs we canvassed our clients with a survey to gauge their confidence in their cyber security position, and **received more than 600 responses** from Australian organisations[1].

Here we address the areas of concern highlighted by our clients and outline the steps your business can take towards minimising your vulnerability to a cyber attack. The focus is on prevention and building a strong defence, as well as fostering the conditions that will allow your business to bounce back quickly.

We hope this report helps you stay on the front foot so you can face your future with confidence.

Contents

Robyn Adcock

Cyber/Technology Practice Leader

P: 02 9242 2000

E: cyber@ajg.com.au

[1] 'Cyber Survey 2020–21' carried out between 24 Nov 2020 and 28 Feb 2021 by Gallagher Australia. Data retrieved 28 Feb 2021

KEY RISK AREA: INTERNAL VULNERABILITIES

How confident are you that your business conducts regular, up to date cyber security awareness training with all members of the team? *(415 respondents)*

"Only 45% of businesses surveyed were confident their employees received regular cyber security training."[2]

The problem

While cyber risk is often portrayed as outside attacks perpetrate by malicious hackers, one of the biggest sources of cyber threats companies face is their own employees. Malware, including ransomware, is used by cyber criminals to damage or access your network and your data and is delivered via downloads or electronic messages. Malware enables everything from denial of service ransom demands to identity theft to withdrawing funds from business accounts.

Troublingly, in a survey of more than 1000 Australian businesses[3] nearly half of employees admitted they had put their organisations at risk by either

- opening an attachment or clicking a link in an email from an unfamiliar sender, or
- downloading apps, software, videos or games without their employers' permission, or
- sharing viral emails from unknown sources.

Prevent

Preventing malware from entering your system depends on the entire company being alert to the risk.

Arm your staff with the knowledge they need to identify a fraudulent email or communication through regular training. Phishing emails are widely employed to deceive users into clicking on a link or attachment and are relatively easy to recognise. Higher value targets may receive more sophisticated messages aimed at specific individuals within an organisation, including executives, and are more difficult to detect as fraudulent without guidance and practice.

Record or document training, ensure it is built into on boarding procedures and regularly communicated through internal channels on cyber safely.

Prepare

All employees should also be trained in the appropriate response if they believe they may have fallen victim to a trap laid by a cyber criminal. It is important that all threats be reported, and this requires a psychologically safe work environment where no blame is attached to the error.

In the event of an actual cyber attack - staff should be aware of, and follow, a pre-prepared incident response plan to limit both financial and reputational harm, with the understanding that different types of attacks may require different responses for optimal mitigation.

Protect

Review your cyber security posture in conjunction with your cyber resilience protocols and discuss your insurance program with your broker for potential gaps in cover. Make sure you have an adequate, up to date, stand alone cyber insurance policy and you are familiar with how it responds to either a cyber threat or cyber incident.

WANT TO LEARN MORE?

Article: Cyber security weak points in SMEs – what you need to know

Article: Beware of malware bypassing or tricking your business anti-virus software

[2] 6 Survey participant. Cyber Survey 2020–21 carried out between 24 Nov 2020 and 28 Feb 2021 by Gallagher Australia. Data retrieved 28 Feb 2021
[3] 'Cyber attacks worsening among Australian businesses, costing economy $1 billion a year', retrieved 2 Mar 2021 from ITBrief

KEY RISK AREA: REMOTE WORKFORCE

Are you confident your remote workforce use the same security protocols and procedures as they would in the office environment? *(370 respondents)*

"The biggest weakness that a network can have is its people." Ben Maidment[4]

Prevent

In a world where the workforce is flexible and transitions between working in the office to working from home, employees pose an especially high risk to maintaining consistent and secure cyber security measures.

To minimise this risk businesses should take the following steps:

1. If your mobile workforce is using remote desktop protocol, be sure it is properly configured and secured, and that software patches are up to date.
2. Antivirus software should be installed on all employee devices — laptops, phones, tablets, USB drives, etc.
3. Introduce multi-factor authentication to protect company information. Authentication should include something you know (username and password), something you have (phone and security code) or something you are (biometric data).
4. Strengthen email security to protect remote employees from phishing scams and business email compromise (BEC).
5. Credential stuffing is a form of identity theft where hackers use tools to inject breached usernames and passwords into numerous sites to infiltrate accounts. Address this threat by using bot detection, such as captcha, adopting a strong password policy and implementing multi-factor authentication.
6. Manage employee privacy footprint by limiting social media oversharing and deleting risky applications.
7. Extend education to employees' families connected to the same network, and encourage cyber solutions that secure entire households as opposed to individual users.
8. Reduce/eliminate/monitor personal devices used for work related tasks.
9. Prohibit use of public Wi-Fi for work related tasks.

Prepare

In the case of a cyber incident the following items should be the primary areas of focus in your pre-prepared incident response plan.

- engage key members of the incident response team
- familiarise employees with the identity of key incident response team members
- document the incident and actions taken in detail
- preserve evidence
- escalate matters internally
- assess obligations to report to regulator
- report to insurance carriers, and engage insurance panel vendors to assist.

Protect

While insurance can't completely close the gaps in cyber security in the home environment, it's an essential component of managing business risk and an effective back-up to the controls organisations can put in place to limit their exposures through staff working remotely.

Some insurance policies will cover actual or suspected cyber incidents. It is important to activate your incident response plan and/or business continuity plan and, at the same time, engage your cyber breach response coach as per your cyber insurance policy. Your response coach and insurance broker will help you with

- insurance policy obligations to report incidents and claims using preapproved panel vendors
- documentation of lost business and extra expenses incurred
- a review of other policies (i.e., crime, K&R, D&O, E&O, GL, property, etc).

WANT TO LEARN MORE?

Webinar: Managing Cyber Risk with a Remote Workforce

Article: The role of risk mitigation in fighting the working from home cyber crime wave

Article: Staying cyber safe while working from home

[4] 'A window into Cyber, Feb 2021,' retrieved 2 Mar 2021 from Brit Cyber Services

KEY RISK AREA: CYBER SECURITY STRATEGIES

Does your business employ the following baseline cyber security measures? *(411 responses)*

The problem

Australian businesses have embraced technology and it is rare to find a business that has not digitised at least one major area of operation. For all its advantages, technology comes with risk. Australians report cyber security incidents to cyber.gov.au every 10 minutes[5]. As the numbers of attacks have risen dramatically in the past year the Australian government has warned of the need for all businesses to be prepared, with the right defences and recovery resources in place.

Prevent

The Australian government recommends all organisations implement eight essential mitigation strategies as a baseline. Known as the '**Essential Eight**', once in place these strategies make it much more difficult for cyber criminals to access or damage your systems. Each strategy may be customised, taking into account your business's risk profile and greatest cyber security concerns[6].

THE ESSENTIAL EIGHT - MITIGATION STRATEGIES

PREVENT MALWARE DELIVERY AND EXECUTION

Application control
Disallow unapproved programs, users or installers to run on your network.

Patch applications
Use the latest versions and patch all computers with extreme vulnerabilities within 48 hours.

Configure Microsoft Office
Allow only vetted macros and block all macros from the internet

User application hardening
Restrict or disable applications. Disable unused Microsoft Office features.

LIMIT THE EXTENT OF CYBER SECURITY INCIDENTS

Restrict admin privileges
On operating systems and applications based on users. Regularly revisit.

Patch operating systems
Use the latest operating systems. Patch all computers (inc network devices) with extreme vulnerabilities within 48 hours.

Multi-factor authentication
For all users when they perform a privileged action or access an important (sensitive/high-availability) data repository.

RECOVER DATA AND SYSTEM AVAILABILITY

Daily backups
Data, software and configuration settings and stored disconnected from your network multiple times every year.

[5] 'ACSC Annual Cyber Threat Report, July 2019 to June 2020', retrieved 2 Mar 2021 from Australian Cyber Security Centre

[6] 'Eight eight explained', retrieved 2 Mar 2021 from Australian Cyber Security Centre

Prepare

Many businesses will find that they are already performing at least three of these recommendations – most commonly, patching in a timely manner, system and data backups and the restriction of administrative privileges. Implementing the remaining Australian Cyber Security Centre (ACSC) 'Essential Eight' cyber security framework ensures that your business has the basics right and the benefits of establishing these safeguards, especially in those areas that are critical for your business, should be viewed as far outweighing the potential cost.

If your business has embedded the 'Essential Eight' strategies then the goal should be to increase your maturity level so that each of your implemented mitigation strategies is fully aligned with the intent of that strategy. Good cyber security and continually improving your businesses cyber resilience is a journey that never ends.

Protect

Cyber insurance supports both cybersecurity and cyber resilience. Data storage, encryption, vulnerability scanning and penetration testing, external audits, security of mobile phones and frequency of patching are among the operational practices that will come under scrutiny by an insurance broker conducting risk analysis for cyber insurance.

WANT TO LEARN MORE?

Blog: Do you have a strategy for handling a cyber attack?
Guide: Small business cyber security guide (ACSC)
Cyber.gov.au: Strategies to mitigate cyber security incidents
Cyber.gov.au: Essential Eight

KEY RISK AREA: VENDOR RISK

If one of your third party suppliers is breached, how confident are you that they have sufficient insurance to cover cyber breach costs? *(390 respondents)*

"I hadn't thought about third party suppliers before."[7]

The problem

When focusing on an organisation, cyber criminals will often look for vulnerabilities in their vendors' security systems as a way into their target's network. Supplier networks can be more vulnerable than those of the desired target, as larger organisations often have more resources dedicated to cyber security.

Prevent

Preventing vendor risk starts with creating a vendor management program. Your program has to take into account both regulatory compliance and mitigation of legal/business/reputation risk. Here are some considerations for your vendor management program

- require your vendor to conduct periodic cyber risk assessments, vulnerability scans and penetration tests of their networks
- require employee and contractors background checks and training
- address roles and responsibilities in breach response
- clarify insurance and indemnification language
- have a contingency plan to use alternate vendors
- document gaps and remediation efforts
- rank your vendors from best to worst - and consider alternatives.

Prepare

On learning about a breach of your vendor's network involving your sensitive data, there are several strategies that can help contain the damage

- review existing contractual requirements with vendors, key business partners and clients for potential risk transfer, including hold-harmless language
- be mindful of contract terms and regulatory requirements that may impose obligations you have to external parties in responding to your vendor's data breach
- follow your incident response plan for guidance on addressing how the investigation and communication of the incident will be handled in conjunction with the affected vendor.

Protect

If your data or network is compromised by your vendor, the risk can be transferred through your vendor's insurance policy. However, some key areas may be excluded by your vendor's policy. Your vendor should have adequate and up to date insurance covering losses resulting from

- technology products and services
- network security and information security liability
- communications and media liability
- professional liability
- expense reimbursement
- contingent business interruption
- retroactive cover.

Potential exclusions: your vendor's policy may exclude losses resulting from

- breach of contract and negligence
- delay in delivering products or services
- wear and tear
- software copyright infringement
- bodily injury/property damage.

Bear in mind your vendors are likely to have one insurance program and one limit for all their customers. If there is a loss for services provided by another customer their policy may be eroded, leaving them, and consequentially you, uninsured. Your Gallagher broker can assist with strategies to mitigate this risk.

WANT TO LEARN MORE?

Webinar: What Happens When My Vendor Gets Hacked?

[7] Survey participant. Cyber Survey 2020–21 carried out between 24 Nov 2020 and 28 Feb 2021 by Gallagher Australia. Data retrieved 28 Feb 2021

PREVENTION: TOOLS, TESTING AND BEST PRACTICES

How confident are you in your business's ability to detect a network intrusion? *(410 respondents)*

How confident are you that your organisation has a data breach response plan or cyber incident response plan that meets business and regulatory requirements? *(370 respondents)*

"Having been maliciously hacked on one occasion - lessons learned."[8]

Prevention strategies

While new cybersecurity tools and strategies are constantly being introduced to address emerging cyber risks, here are five core measures to ensure your organisation is one step ahead of cybercriminals.

1. **Employee training:** employees at every level of the organisation may be targeted by hackers. Regular training should be mandatory for all employees, focusing on ways to recognise cyber threats such as phishing, and should include process controls and escalation procedures.
2. **Create an incident response plan:** incident response plans establish an organisation's standard of care and best practices in compliance with regulation, contracts and insurance underwriting. Your plan should be backed by a group of internal and external experts briefed and trained on what to do in the case of a cyber incident.
   - **Internal response team:** includes senior management, HR/ customer service, legal, IT, compliance, finance, operations, PR and marketing
   - **External response team:** includes a breach coach, IT forensics firms, crisis communications, notification and call centres, credit monitoring firms, extortion negotiators, and data asset restoration experts
3. **Hire a hacker:** test your IT defences by hiring an expert in hacking techniques to identify vulnerabilities in your network.
   - **Penetration tests:** conducted by certified ethical hackers with specific parameters to test for vulnerabilities in technology, people, processes or facilities
   - **Bug bounties:** a deal offered by organisations by which anyone can receive compensation for reporting vulnerabilities, allowing IT security to discover and resolve bugs to prevent incidents/ widespread abuse before the general public is aware of them
4. **Conducting a risk assessment:** hire an external party to regularly scan your external facing ports for known vulnerabilities on a regular basis. This assessment can expand beyond technology controls to identify additional areas of improvement, such as risks stemming from current processes, lack of employee training, compliance requirements and physical access to premises.
5. **Conduct tabletop exercises:** test the incident response plan through a simulated cyber attack. This collaborative and interactive approach helps to evaluate an organisation's cyber crisis preparedness and identify areas of needed improvement. Ultimately tabletop exercises should provide the tools and proficiency needed to effectively respond from both a strategic and technical perspective.

All five of these strategies can be used alongside a cyber insurance program. Many policies include services such as employee training, incident response planning tools, cyber risk assessments and other valuable exercises. Performing these actions can significantly improve a business's cyber risk management posture.

8 Survey participant. Cyber Survey 2020–21 carried out between 24 Nov 2020 and 28 Feb 2021 by Gallagher Australia. Data retrieved 28 Feb 2021

PROTECTION: CONFIDENCE IN CYBER APPROACH

How confident are you that your organisation is protected against cyber threats? *(626 respondents)*

How confident are you that your business has sufficient insurance to cover the associated costs of a cyber incident? *(618 respondents)*

"We have a laptop and PC with back-up to OneDrive. We use Office 365 and security via Windows Defender and updates are downloaded regularly. Only three people have access and passwords. I work in the IT Industry and am very alert to phishing, spam and scam emails. We know none of us are really safe in the modern environment."[9]

The problem

As the numbers of cyber attacks have risen with our growing reliance on technology, the Australian government has warned of the need to be prepared, with the right defences and recovery resources. Business leaders know that computer systems are inherently vulnerable, yet many organisations are challenged by limited time, budgets, an absence of appropriately skilled IT support and/or knowledge of the evolving complexity regarding cyber security solutions, leaving them uncertain about how much is to be done to manage their cyber risk[8].

The main motivation for any business owner or leader to manage cyber risk is the consideration that a cyber incident is perhaps inevitable in our current digital landscape, regardless of the level of confidence you may have in your cyber security posture. We see many clients enhance their cyber security, cyber risk management and cyber protection as a result of having been the victim of cyber incident and suffering anything from reputational damage to financial devastation caused by data loss or breach.

[9] 'Big cyber security questions for small business', retrieved 28 Feb 2021 from Cynch Security

CYBER INSURANCE: PROTECTION FOR CYBER EVENTS

Protect

Put simply, cyber insurance covers your business's liability in the event of a data breach affecting you or your customer, employee and or contractors information.

Cyber insurance typically covers

- legal fees
- cost of recovering data
- cost of restoring the identities of affected clients
- cost of notifying customers of the breach/data loss.

Cyber insurance can also cover

- **cyber, privacy and network security liability** – failure to protect private or confidential information from others and failure to prevent a cyber incident from impacting others systems
- **payment card loss** – contractual liabilities owed to payment card industry firms as a result of a cyber incident
- **regulatory procedures** – defence of regulatory actions and cover for fines and penalties
- **media liability** – copyright and trademark infringement with scope of defined media content
- **cyber incident response** – forensics, notification costs, credit monitoring, public relations
- **business interruption** – loss of profits and expenses from interruptions to business systems, losses from interruptions of other's systems
- **digital data recovery** – costs to restore of replace lost or damaged data or software
- **telephone toll fraud** – cost incurred as phone bill charges due to fraudulent calling
- **network extortion** – payments to pre digital destruction or impairment
- **computer fraud** – third party accessing your business's computers to take money
- **funds transfer fraud** – third party tricking a bank into transferring funds from your business account
- **social engineering fraud** – third party tricking an employee into transferring money.

Cover designed to meet your cyber risk profile

What does your business need? Your business's cyber liability is rarely simple. Understanding the known and unknown risks within its scope is complex and requires expertise to understand how an insurance program can be implemented to protect your organisation. After we assess your current cyber coverage, we develop a customised program that takes into account your unique needs.

To address the sophisticated and evolving nature of cyber liability insurance, we have developed a global practice that takes a consultative and action based approach. We offer

- proprietary cyber insurance limits modelling, third-party benchmarking, cost of a breach calculator, quantitative cyber analysis
- insurance coverage gap analysis, broker table top exercises, insurance policy on boarding[10]
- incident response planning (spells out steps to be taken in event of a breach – including access to a breach coach)
- insurance policy design and implementation
- contract analysis for your insurance documentation.

Cyber claims advocacy

Gallagher provides a comprehensive program that aids you with recouping from loss and having a seamless claims process. We have experience with the cyber liability claim lifecycle, from the breach to recovery. We will assist you with breach preparedness during the strategic risk management program phase, help you develop a breach response plan and assess and select vendor partners.

A breach response necessarily involves a panel of experts. A good quality cyber insurance policy will include preapproved providers with deep experience, determined by the insurer. There may be scope to employ providers that have an existing relationship with the insured while experiencing a cyber incident. This should be discussed and decided upon prior to the inception of policy.

We recommend the following service providers for an optimal breach response

- forensic investigator
- payment card industry investigators (PFIs)
- breach notification service provider
- credit monitoring/ID monitoring service provider
- PR firm
- legal representation.

[10] Gallagher will coordinate this service for an additional cost

Conclusion

Cyber exposures are constantly and quickly evolving, and the cyber risk management journey is continual, with no end in sight. We have no way to predict exactly what the future of the cyber threat landscape will be but we do know that technology will continue to advance and that society will continue to embrace it. Hackers will remain focused on ways to exploit it, solicitors will continue to litigate and regulators will continue to create compliance laws aimed at preventing the reoccurrence of hacks and wrongful data collection. So goes the vicious cycle of cyber risk, and organisations are paying a steep price as they continue to lose ground to cyber criminals.

Efforts to manage cyber risk can be further complicated by unforeseen events, as we have witnessed over the past year, which can push organisations across industries into unfamiliar and, in many instances, riskier operating environments. However, when proactive efforts are made in the three key areas of prevention, preparation and protection, we firmly believe that managers of cyber risk can and will turn the tide.

For more information about how Gallagher's dedicated cyber team can help you reduce your cyber exposure, please get in touch.

Contact our cyber team:

02 9242 2000 | **cyber@ajg.com.au**

Robyn Adcock

Cyber/Technology Practice Leader

Alberto Piccenna

Client Manager, Professional and Financial Risks

The Gallagher cyber practice: Cyber | Gallagher Australia