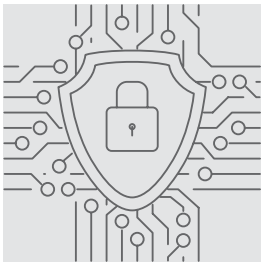
thinkBIG...

pulse of the SME sector

Cyber security for SMEs and startups:

Want to raise equity, IPO, list or get acquired? Better make sure your cyber security isn't cause for concern.



THE POWER OF BEING UNDERSTOOD
AUDIT | TAX | CONSULTING

Celebrating 100 Est.1922 in Australia

RSM

CONTENTS

EXECUTIVE SUMMARY

Solid cyber security is one of those things SME owners and startup founders realise is important but often struggle to get around to focusing on. Unfortunately, cybercriminals don't make any allowances for busy business owners who haven't had time to create a secure cyber posture. Increasingly, neither do regulators, customers or suppliers.

Supranational groups, such as the European Union (EU), and national governments, including Australia's, have been tightening up laws around the collection, storage and use of data since 2018. Businesses that suffer a successful cyber attack are now required to notify the relevant regulator and any potentially impacted stakeholders and may also have to pay heavy fines or penalties. In the wake of a serious data breach, they may find their options limited if they wish to IPO, list or get acquired at some future date.

While cyber security remains more of an art than a science, there are some basic precautions all business owners can take. Understanding the risks they face, taking action to mitigate those risks, and taking a proactive rather than reactive approach to cyber security is a good start.

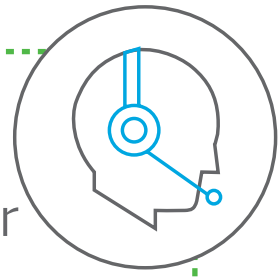
It's difficult to determine exactly how cyber secure Australia's SMEs and startups are. Nonetheless, there appears to be a widespread consensus that there is room for improvement, especially in industries that haven't historically had an ethical or legal obligation to protect their customers' data.

Cybercrime is an enormous industry, projected to inflict US$10.5 trillion (A$15 trillion) in damages globally by 2025. Australian regulators, lawyers, investment bankers and cyber security experts, not to mention SME owners and startup founders themselves, all seem to agree that while most Australian businesses have basic cyber defences in place, in many cases these defences should be substantially upgraded.

If they are not upgraded, those who own or oversee businesses can no longer expect much wriggle room from regulators or courts. There are currently moves afoot to hold directors personally liable for failing to appropriately manage cyber security risks. And in recent times, Australian businesses have had to pay out hundreds of thousands and sometimes millions of dollars for failing to properly use or safeguard their customers' data.

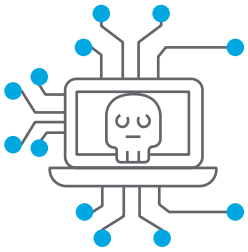
Fortunately, business owners only need to summon the will to improve their cyber security rather than find the time and energy to oversee the task themselves. That task can be outsourced to the experienced cyber security experts at RSM Australia.

For more information visit
rsm.com.au/thinkbig-report



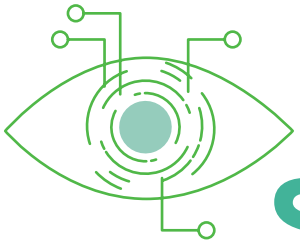
310%

The increase in calls to the Australian Cyber Security Centre (ACSC) hotline in the 2020–21 financial year *(from the previous financial year)*



67,500

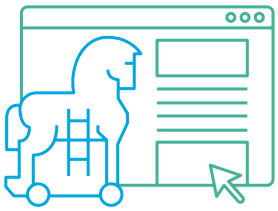
Number of cybercrimes reported to the ACSC in 2020–21



$5.1 billion

What Australian organisations spent on cyber security in the 2021 calendar year

$33 billion



Australian individuals and organisations' self-reported losses from cybercrime in the 2020–21 financial year

Estimated cost of cybercrime by 2025:

$15 trillion

Businesses of all types are inclined to treat cyber security as a second-order issue, but the temptation for SMEs and startups to put it on the backburner is near irresistible. After all, if you're not entirely sure your business will be able to make payroll at the end of the month, or be a going concern at the end of the quarter, why devote attention and resources to shoring up your cyber defences?

The most compelling reason for any organisation to strengthen its cyber security is because cybercrime is widespread and the potential financial and reputational consequences of suffering a data breach have become more severe in recent years.

But those with an equity stake in a business that they hope will IPO, list or be acquired have a far more powerful and immediate motivation to act. As will be detailed in the following pages, a startup that can't prove it has its cyber security house in order will increasingly struggle to attract interest from potential investors or acquirers. Especially as those investors and acquirers become more cognisant of the prevalence and consequences of data breaches. Furthermore, an SME with plans to go public may find it difficult to enter into business relationships with large companies if it can't prove to those companies it's cyber security posture is reassuringly secure.

A brief history of cyber regulation

Until relatively recently, there was a tacit but widespread consensus that cyberspace was the Wild West and that individuals and businesses engaged in online activity at their own risk.

Cyber threats, such as viruses, have been around since the dawn of the digital age. But the idea that organisations might have a legal responsibility to safely store and responsibly use the data they collected has been slow to take hold. For three decades after the Internet achieved mass penetration, self-regulation was the norm.

After the controversial dating site Ashley Madison was hacked in 2015, the personal information of 39 million users was compromised, resulting in several suicides. Yet the only consequence for the site's owner, aside from negative media attention, was a US$11.2 million payout to settle a class action.

The end of the Wild West era

The Big Bang of cyberspace regulation was the EU's introduction of the General Data Protection Regulation (GDPR) in May, 2018. Two months later, California (the world's fifth-largest economy) unveiled the California Consumer Privacy Act (CCPA). Since then, many national governments, including Australia's, have introduced (or tightened up) laws around the collection, storage and use of personal data.

An Australian business that suffers a successful cyber attack no longer has the option of sweeping it under the rug. At a minimum, it now must alert any customers and suppliers that may have been affected and alert the Office of the Australian Information Commissioner (OAIC).

At the very least, a business that is revealed to have ineffective cyber defences is likely to suffer reputational damage. Reputational damage that will usually have significant commercial implications. There is no data available on the post-data-breach performance of Australian companies, but NASDAQ-listed companies that suffered a breach underperformed the market by -15.6% for the following three years.

The challenges of a globalised digital economy

Businesses with an online presence not only have to abide by the local laws; they also need to be compliant with the laws in any other nations they operate in.

For instance, since the GDPR was introduced, American companies such as Amazon, Google, Facebook and Marriot have collectively paid well over €1 billion (A$1.5 billion) in GDPR fines. While it hasn't happened yet, an Australian business that has European customers could find itself facing fines of up to 2% of its total worldwide annual revenue if it's found not to be GDPR compliant.

Most companies that have been fined in recent years have deliberately chosen to push the envelope in their use of customers' data. However, there have also been substantial fines handed out for data breaches. After hackers stole the personal data of around 400,000 of its customers, British Airways was threatened with a £183 million (A$325 million) fine by the UK's Information Commissioner's Office (IOC). Even though its customers didn't appear to suffer any financial losses because of the breach, British Airways ultimately had to pay a £20m (A$35m) fine.

Timeline

1969 The Internet is established.

1971 Creeper, the first computer virus is released.

1991 Tim Berners-Lee invents the World Wide Web.

1995 Amazon and eBay.com launch. Bill Gates proclaims, "There will be two types of businesses in the next five years, those that are on the Internet, and those that are out of business."

2000 A Canadian teenager unleashes a DDoS attack on websites such as Amazon, eBay and Yahoo causing an estimated US$1.2 billion (A$1.7 billion) of commercial losses.

2007 Apple releases the first smartphone.

2016 The global digital economy is estimated to be worth US$3 trillion (A$4.2 trillion).

2017 WannaCry ransomware attack infects 200,000 computers in 150 countries resulting in economic losses of up to US$4 billion (A$5.7 billion).

2018 GDPR, CCPA and (Australia's) Notifiable Data Breaches Scheme are introduced.

2019 39 million customers of Canva have their personal details stolen. Canva's head of security states company executives now understand, "Security breaches are part of the business's existential risk now and need to be managed as such."

2021 Amazon receives a €746m (A$1.1 billion) GDPR fine for data protection violations.

Does my business's cyber security strategy pass muster?

The Australian Cyber Security Centre defines cyber resilience as, "The ability to adapt to disruptions caused by cyber security incidents while maintaining continuous business operations. This includes the ability to detect, manage and recover from cyber security incidents."

You may be wondering exactly what constitutes an appropriate investment in cyber security. After all, every business has finite resources, and SMEs and startups are particularly resource constrained. So where exactly does the dividing line between an adequate and an inadequate investment in cyber resilience lie?

Unfortunately, there is no list of cyber security boxes a startup can tick off and then be seen to have done all it reasonably could have to achieve cyber resilience. No matter how much time and effort a startup has put into creating redoubtable cyber defences, it will almost always be seen to have underinvested if those defences are breached.

Fortunately, there's usually a lot of low-hanging cyber-resilience fruit that businesses can pluck and many useful guides to plucking that fruit.

ASIC's advice

ASIC suggests this three-pronged approach to cyber security for business owners and directors:

1. UNDERSTAND YOUR DUTIES

If you own or oversee a business, it's your responsibility to educate yourself about common cyber threats and ways to protect your business from them. (As always, ignorance is no defence under the law.) ASIC suggests owners and directors ensure they can answer the following eight questions:

> *Are cyber risks an integral part of the organisation's risk-management framework?
>
> *How often is the cyber resilience program reviewed at board level?
>
> *What risk is posed by cyber threats to the organisation's business?
>
> *Does the board need further expertise to understand the risk?
>
> *How can cyber risk be monitored and what escalation triggers should be adopted?
>
> *What is the people strategy around cyber security?
>
> *What is in place to protect critical information assets?
>
> *What needs to occur in the event of a breach?

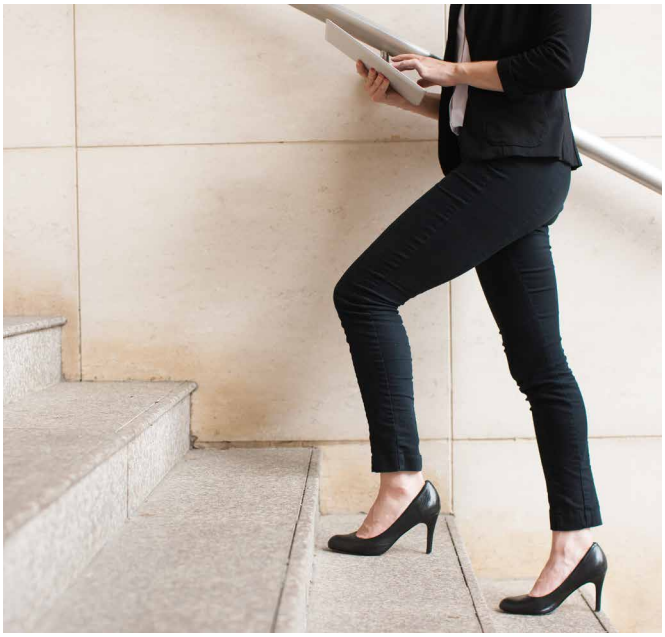
2. TAKE ACTION

In the likely event you can't answer all eight questions confidently, the next step is to make sure "robust cyber security resilience strategies are in place to protect against threats and scams". These strategies will vary between industries and businesses. But ASIC provides guides that detail what the most likely threats are (e.g. malware, ransomware, phishing) and the strategies that have proven most effective at stymieing malicious actors (e.g. strong passwords, multifactor authentication, identity and access controls, training staff about cyber security, using software that automatically updates and regular backing up of data).

3. REMAIN VIGILANT

Cybercriminals are nothing if not adaptable and inventive. That means putting robust cyber security in place is not a one-off, set-and-forget affair. Founders, directors and IT teams need to not only educate themselves about existing cyber threats, they also need to take reasonable steps to remain alert to emerging ones. (A range of local and foreign government agencies publish alerts about the current threat environment.)

There are a plethora of credible cyber security guides, but they all have essentially the same advice as ASIC's: identify and fix existing vulnerabilities then remain alert to emerging threats.



If you're not doing scans and penetration tests, then just know that someone else is. And they don't work for you.

George Grachis
Author and cyber security expert

IT risk or business risk?

With the possible exception of "We've always done it this way", "We can leave it to the IT guy to look after cyber security" is the most dangerous phrase that can be uttered in the boardroom of a 21st century business.

Unless they have an equity stake, it's unlikely to be the IT guy who suffers serious reputational and legal consequences if a business finds out the hard way its cyber security is deficient.

Australian directors are already expected to be heavily involved in formulating cyber security strategies. Soon, they could be held personally liable for failing to appropriately manage cyber security risks, as is already the case in Germany, the US, Canada, South Africa and the UAE.

It's not just directors who can see their lives turned upside down. Cyberattacks are an existential risk for small businesses in a way they rarely are for large companies and government agencies. The latter can eat the substantial losses arising from payouts to affected stakeholders, fines and lost business; startups and SMEs usually can't.

A near miss

Andrew Clifford who is a Partner at RSM and part of the Corporate Finance division which advises companies looking to list or IPO, knows that cyberattacks can rapidly escalate into near-death experiences for startups because he's seen it happen.

"I'm not at liberty to go into details, but a startup I recently worked with suffered a 'malicious insider' attack that cost it the best part of half a million dollars," Clifford says. "An employee with inside knowledge, including knowledge of the cyber security their employer had in place, siphoned off money that was meant to end up in customers' bank accounts. Fortunately, in that instance, it was an embarrassing body blow rather than a death blow to the startup, which did go on to successfully list. But many of the cashflow-constrained startups and SMEs I've worked with would immediately collapse if either a malicious insider or external cybercriminal made off with hundreds of thousands of dollars."

How cyber resilient are Australian startups?

Clifford says it's difficult to determine just how cyber security-conscious smaller Australian businesses are. "If you look at the prospectus of a startup, you'll often find there is a paragraph or two stating that the startup in question recognises the risks of cyber attacks and has taken all reasonable precautions to prevent them. But there's rarely anything in the prospectus that demonstrates cyber resilience is something that's taken particularly seriously."

Noting that cyber security is generally not something that gets much attention when startups are looking to IPO, list or get acquired, Clifford says either an optimistic or pessimistic view can be taken about this.

"The optimistic view is that startup founders get their cyber security sorted out shortly after launching, so they don't need to worry about it by the time they are looking to list or get acquired," he says. "I'm sure many startups, particularly those in industries such as fintech, do bake in robust cyber resilience early on."

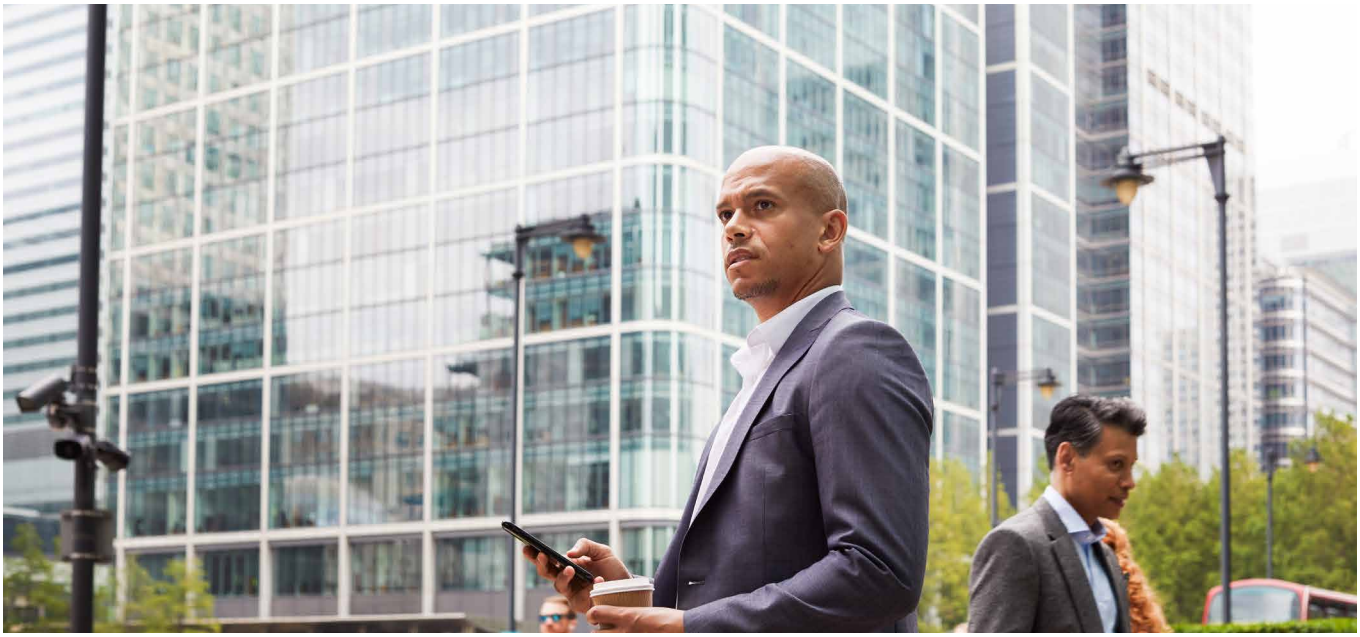
But Clifford isn't certain robust cyber security is the norm. "The pessimistic view is that SME owners and startup founders don't do much more than they have to," he says. "They may plan to invest more in cyber security down the track. But down the track usually means after the big capital injection that comes with an IPO, listing or acquisition."

The cyber security future is here but unevenly distributed

Clifford isn't sure how many startups fall into the no-frills cyber security category but notes they could soon have more to worry about than cybercriminals.

"We're already at the stage where those considering investing in a business operating in an industry such as financial services, healthcare, IT or software want to be reassured that it is cyber resilient," he says. "In the not-too-distant future, I imagine investors will want to see evidence of cyber resiliency for any type of startup they are running the ruler over."

Cyber security is generally not something that gets much attention when startups are looking to IPO, list or get acquired.



Australian organisations that suffered significant data breaches in 2021

ASIC

Eastern Health

Nine Entertainment Co

Northern Territory government

NSW Department of Health

Oxfam Australia

Sunwater

Swinburne University

Tasmanian Ambulance

TPG Telecom

Transport for NSW

UnitingCare Queensland

Western Australian Parliament

Source:

www.gizmodo.com.au/2021/12/2021-data-breaches-australia

Top 5 Australian industry sectors for data breaches, Jan–Jun 2021

Health service providers

Finance

Legal, accounting and management services

Federal government

Insurance

Source:

www.oaic.gov.au/privacy/notifiable-data-breaches/notifiable-data-breaches-statistics/notifiable-data-breaches-report-january-june-2021

The cyber resilience of Australia's late-stage startups

There is little data available about the cyber resilience of Australia's late-stage startups. In an attempt to generate some, RSM went through the annual reports of the 271 companies that listed on the ASX during the last three financial years (2018–2019, 2019–2020, 2020–2021).

Of course, no straightforward correlation exists between how often a company mentions cyber security in its annual report and that company's commitment to cyber resilience. Nonetheless, in the likely event some correlation does exist, the data makes for interesting reading.

Cyber security consciousness seems to be increasing

6.41% of companies that listed in the 2018–2019 financial year mentioned cyber security in their annual reports. This figure increased to 10.86% in the 2019–2020 financial year then jumped up to 17.68% in the 2020–2021 financial year. Overall, there was a 104.2% increase in mentions of cyber security over the three financial years surveyed.

Cyber security mentions tend to be formulaic

If less than one in five recently listed companies mentioned cyber resilience in its first annual report, that necessarily means that more than four in five didn't. It should also be noted that many of the companies that did mention cyber threats did so in a boilerplate fashion. This typically involved noting, usually in the 'Key Risks and Business Challenges' section of the annual report, that the company collects and stores sensitive data, which could potentially be stolen during a cyber attack, which could result in litigation, claims, fines, penalties and reputational damage.

Few businesses display a comprehensive commitment to cyber security

Of the 271 companies that listed over the last three financial years, just 17 – that is, 6% of them – dealt with cyber resilience in anything other than a pro forma manner in their first annual report. What's more, these businesses either tended to already be substantial businesses before listing (e.g. Magellan Global Fund, Nuix, TPG Telecom) or to be operating in industries with a longstanding ethical or legal requirement to protect sensitive personal data (e.g. finance, healthcare and telecommunications).

What constitutes best practice?

Some of the measures taken by the cyber security high achievers involved significant outlays of time and money, but many didn't. If you're a business owner looking to lift your cyber resilience game, you may want to consider one or more of the following initiatives:

*Making 'maintaining industry-leading cyber security' one of the CEO's KPIs

*Recruiting directors with technology backgrounds or encouraging existing directors to educate themselves about cyber security

*Establishing a cyber risk committee

*Making strong data protection one of your startup's ESG commitments

*Committing to a substantial investment in cyber security technology during the next financial year

*Committing to substantial investment in cyber security staff training during the next financial year

Darren Booth is the National Head of RSM's Cyber Security and Privacy Risk Services. Darren has many years of experience delivering an extensive range of technology risk management projects including technical security assessments, governance and strategy, data privacy, third-party risk, cloud security assessments and risk strategy.

Booth isn't surprised that the analysis of the annual reports of recently listed companies suggests cyber resilience isn't a priority for most Australian startups. He says that while well-capitalised startups usually have redoubtable cyber security in place from the get-go, less well-capitalised startups often mistakenly assume they are of little interest to cybercriminals.

"RSM works with Australian businesses of all sizes but predominantly smaller to mid-sized ones," Booth says. "If you're in charge of a well-capitalised startup, you're likely to be cyber security conscious from early on. That's because you're probably going to have experienced directors and investors on your case about cyber resilience before you even launch.

It's also because you'll almost always be planning to go public as soon as is feasible, with all the regulatory requirements, and public and media scrutiny, that it involves. Also, if your startup is a substantial business from early on, it's likely to soon enter into commercial relationships with well-established and well-run businesses. At least one of those well-managed businesses will likely be acutely aware that it could be subject to a 'backdoor' cyber attack that involves a malicious actor breaching the cyber defences of one of its subcontractors or suppliers.

That business will want to see evidence, ideally in the form of an ISO certification, that any startup it is considering partnering with is cyber resilient."

Smaller doesn't mean safer

In contrast, if someone scrapes together a few hundred thousand dollars from friends and family members who have little or no business experience and sees listing as either an improbable or far-off event, they aren't likely to experience the same external pressures to get their cyber security affairs in order.

Ashwin Pal is a Partner at RSM who specialises in privacy and security.

"Smaller players tend to be acutely aware of their lack of resources, so it's natural for them to assume that criminals wouldn't have any interest in what they perceive to be slim pickings," Pal says. "But I always say that no individual or organisation is immune from cyber crime.

If you are on the internet, you are vulnerable. A cyber criminal is just as happy to spend a day stealing $250,000 from four modestly sized startups with basic cyber defences as to spend a day stealing $1 million from a larger startup with more sophisticated cyber defences."

In the past, many Australian SMEs could get by with 'bare bones' cyber security, but Pal says that pressure is building on them to lift their game. "Nowadays, many small businesses engage with large ones and do this mainly or exclusively online. That means cybercriminals can penetrate the cyber defences of a poorly protected small player that sells to or buys from a large company, then use the small company's systems as a beachhead to worm their way into the larger company's IT infrastructure. Reasonably enough, large companies don't want to find themselves potentially millions of dollars out of pocket due to one of these 'backdoor' attacks. Accordingly, they are increasingly insisting all their suppliers and, in some cases, even their customers demonstrate they have the correct cyber security posture."

An investment banker's perspective

Gavan Carroll has had senior roles at Credit Suisse and a large accounting and consulting firm and is currently a Managing Director at Ord Minnett, where he heads up Capital Markets and technology coverage. He has worked with many emerging technology companies over the last two decades.

The encouraging news

Carroll believes that even if it hasn't happened to them or a company they know, Australian startup founders are well aware that local startups can and have been breached.

"In our experience, Australian startup founders are cyber security conscious," Carroll says. "The majority of those we've dealt with are familiar with GDPR and the Notifiable Data Breaches scheme. Most are also aware of Australian businesses that have paid a high price for either irresponsible data use or inadequate cyber security. The case of a local emerging technology business incurring significant penalties for allowing industry participants to access their users' personal information without their knowledge was an important reminder of the importance of appropriate data policies."

To borrow from Donald Rumsfeld, Carroll believes that Australian startups are generally doing well when it comes to the 'known knowns' of cyber threats. "Our observation is that Australian startups are generally aware of their obligations around collecting, storing and using data appropriately," he says.

The somewhat less encouraging news

While Carroll believes that Australian startups are mindful of the necessary precautions to guard against existing threats, he is more cautious about their level of preparation for new ones. "Are startup founders doing things such as constantly reviewing threat intelligence reports and regularly conducting penetration testing on their systems? If they are running a fintech startup, it's more probable they are. But if they are running a startup in an industry where cyber security might not receive the same prominence then it's perhaps less likely they would be taking such a proactive approach and expending the necessary time and effort to implement industry-leading cyber security measures."

What investors expect

Carroll believes that sophisticated investors already pay attention to cyber resilience and expect that companies have appropriately assessed and addressed their cyber risk. "A startup that suffers a significant breach could well see an impact on its future funding options," he says.

The benefits of outsourcing to a third party

Carroll observes an external specialist consultant is likely to focus on more than just the risks that are known but also the less recognised and evolving threats."

What can go wrong

Given the infrequency with which they hear about successful cyberattacks, it's perhaps not surprising that Australian SME owners and startup founders frequently lapse into a false sense of (cyber) security.

A blizzard of statistics about the prevalence and financial consequences of cybercrime is all very well, but if you rarely hear about Australian businesses paying a high price for inadequate cyber security, cyber resilience probably won't remain top of mind.

While Australian businesses may now be obliged to report successful cyberattacks to the OAIC, as well as any potentially impacted stakeholders, they have little incentive to publicise these events. And cyberattacks rarely make for exciting copy, so unless there's an unusual angle or a well-known organisation involved, the media usually isn't interested in covering them.

But while they may not generate much public or media interest, cyberattacks happen every day of the week, sometimes with life-altering consequences for those affected.

The investment firm that's $750,000 out of pocket

RI Advice is a small, Sydney-based firm that provides retirement investment advice. It was breached several times from 2014–2020. Its clients had their data — including their contact details, copies of their passports and driver's licenses and, in some cases, sensitive health information — compromised. One client also lost $50,000 as a result of the breach.

In mid-2018, by which time it was aware one of its file servers had been accessed by a malicious actor, RI Advice obtained a cyber-resilience plan. However, it then took three years to implement this plan to what was deemed to be "a good level". This allowed further breaches to occur.

RI Advice was taken to court by ASIC. On the 5/5/2022, the Federal Court of Australia found,

"RI Advice contravened... 912A(1)(a) and (h) of the Corporations Act from 15 May 2018 to 5 August 2021 as a result of its failure to have documentation and controls in respect of cyber security and cyber resilience in place that were adequate to manage risk".

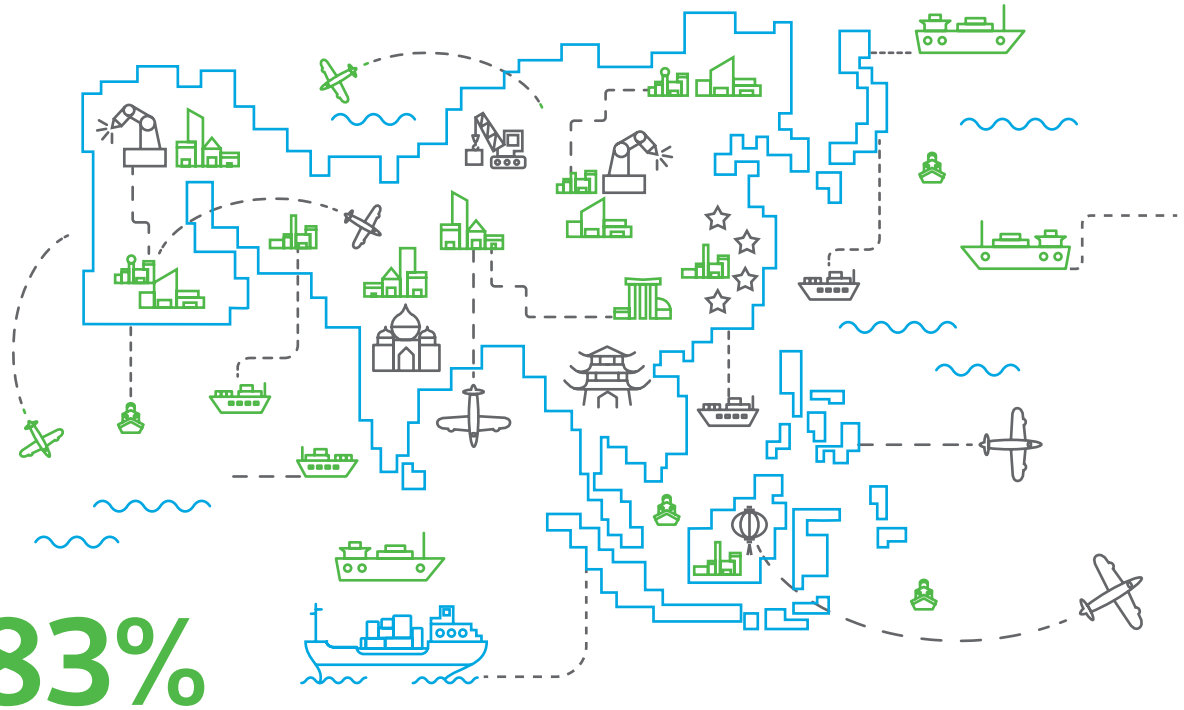
RI Advice was ordered to "pay a contribution to the plaintiff's [ASIC's] costs of the proceeding fixed in the amount of $750,000". It was also ordered to engage an outside cyber security expert "to identify what, if any, further documentation and controls in respect of cyber security and cyber resilience are necessary for RI Advice to implement to adequately manage risk" then rapidly and fully implement any "further measures" recommended by the cyber security expert.

A shot across the bows

An ASIC spokesperson remarked that RI Advice got off relatively lightly given breaches of 912A can potentially result in penalties of up to $525 million. (Among other things, Section 912A of the Corporations Act requires financial services licensees to have adequate risk management systems in place.)

Rachael Falk, CEO of the Cyber Security Research Centre, described it as a "landmark case" deserving "utmost attention from senior management, boards and directors as our nation navigates a new era of cyber security uplift". Falk also warned:

> "Ultimately, this judgement highlights that ASIC will be paying close attention to the cyber security practices of organisations that fall under its remit — and is prepared to take action. More broadly, it is a clear signal to all organisations right across the economy that the Corporations Act will be enforced as it relates to cyber security and it's only a matter of time before more cyber security-related actions are brought before the courts."



83%

of surveyed Asia Pacific organisations were breached by ransomware between 2017–2022

Only 32%

of those organisations publicly disclosed the ransomware attack

54%

of surveyed Asia Pacific organisations last updated their cyber security infrastructure in 2020 or before

Just 43% of surveyed IT decision-makers in Australia have "a high degree of confidence in their organisation's ability to prevent or mitigate cyber security threats"

$3.7 million

the average cost of a data breach in Australia in 2021 (Source)

311 days

the average time it takes an Australian company to detect and contain a data breach (Source)

A lawyer's perspective

Harry Kingsley is a Partner at K&L Gates and a senior corporate and commercial lawyer who has worked with many Australian businesses.

He believes Australian businesses, especially those at the small and micro cap end of the market, need to devote greater attention to building cyber resilient businesses. But he understands that it is a big ask.

"Entrepreneurs are by nature risk-takers," he says. "The type of person who walks away from a corporate position to launch a startup business is not likely to be the same type of person who wants to cover all business risks from day one. This could include full coverage insurance, cyber security, governance or protecting their intellectual property"

Even if they do happen to be the anxious type, Kingsley argues business owners will inevitably struggle to find the time to devote to cyber security.

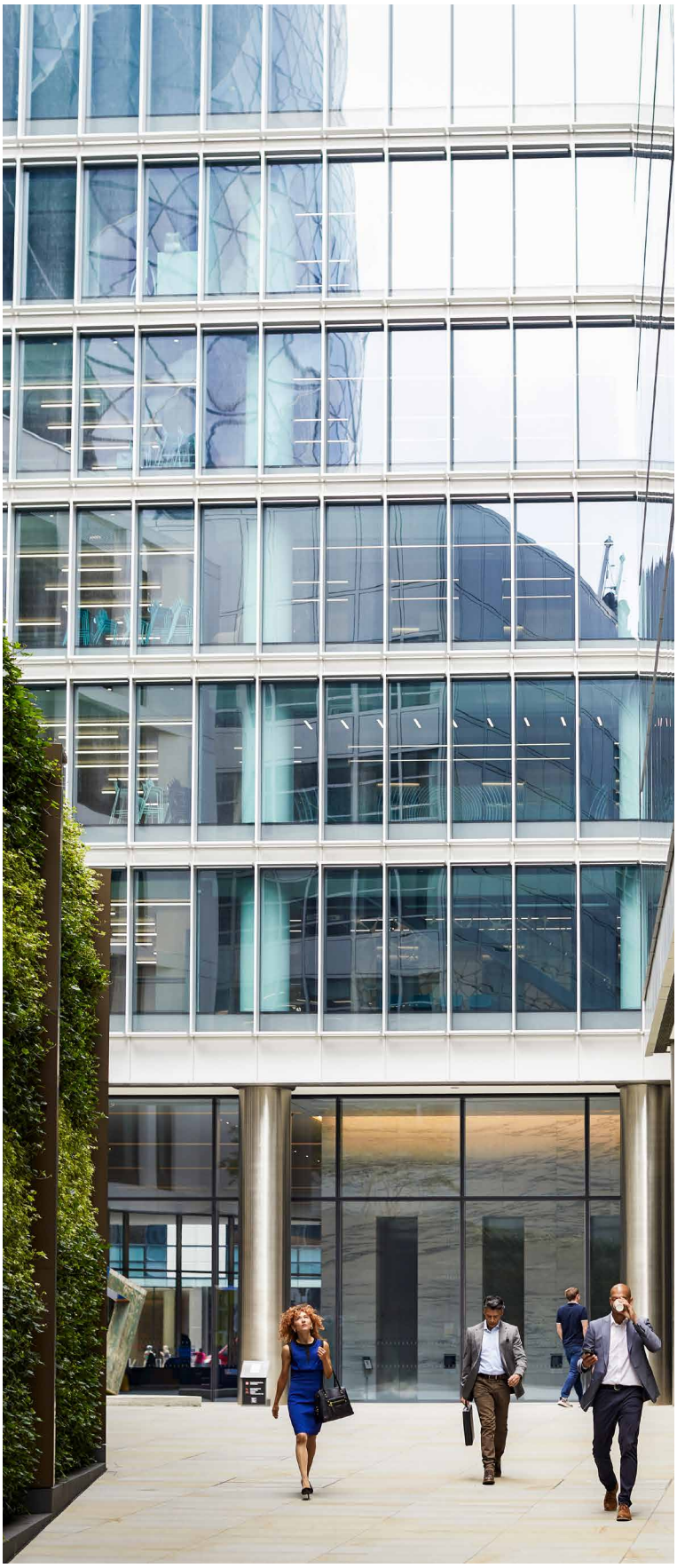
"Each professional seeks to provide best in breed advice on their particular specialisation. However, to a time poor founder, it is inevitable that they will triage their efforts on to their most pressing needs. Those needs are likely to be, hiring the right team, commercialising their technology, growing or initiating sales and raising capital."

A turning tide

Kingsley argues the submission of the final report of the Banking Royal Commission in 2019 and the widespread embrace of remote working in 2020-2021 perhaps did far more to raise cyber security awareness than the introduction of GDPR, CCPA and NDP scheme in 2018.

"In 2019, the people who serve on boards, or who aspire to do so, saw bank directors have their reputations shredded. Many of these individuals didn't just lose their one bank board position, they lost all their directorships. That wasn't to do with cyber security, but it was to do with governance. I suspect that post-Banking Royal Commission, Australian directors are far more focused on meticulously discharging their duties. Duties that include ensuring the organisations they oversee are cyber resilient."

Kingsley believes that even directors and business owners could not ignore the impact of COVID. "Suddenly, staff were BYO'd-ing, downloading sensitive personal or commercial data from their work laptop to the desktop in their home office. That prompted many businesses to reconsider their cyber security policies and infrastructure."



Commercial practicalities

Kingsley notes that, reasonably or otherwise, cyber security would be unlikely to be on top of most business founders' to-do lists. "Early on, they are going to be obsessed with raising capital," he says. "If they clear that hurdle, they are then going to be consumed with staffing up, managing cashflow, commercialising and shipping product. Then, if they are among the small fraction of business founders who have a realistic prospect of listing or getting acquired, they are going to be focused on value capture."

> Getting a good price may involve proving your business has strong cyber security firmly in place. But, historically, this has been the exception rather than the rule.

"If you're operating in an industry where a lot of personal data is collected, such as fintech, telecommunications or utilities, you're likely to have all the right cyber resilience policies and procedures in place from Day One," Kingsley says. "But often it won't be strictly necessary or commercially practical to have gold-plated cyber security. Lots of Australian businesses implement off-the-shelf cyber security solutions that provide protection against the standard ransomware and malware threats but baulk at the cost of bespoke solutions that address the specific threats that their business faces."


A little
understanding
goes a long way

What now?

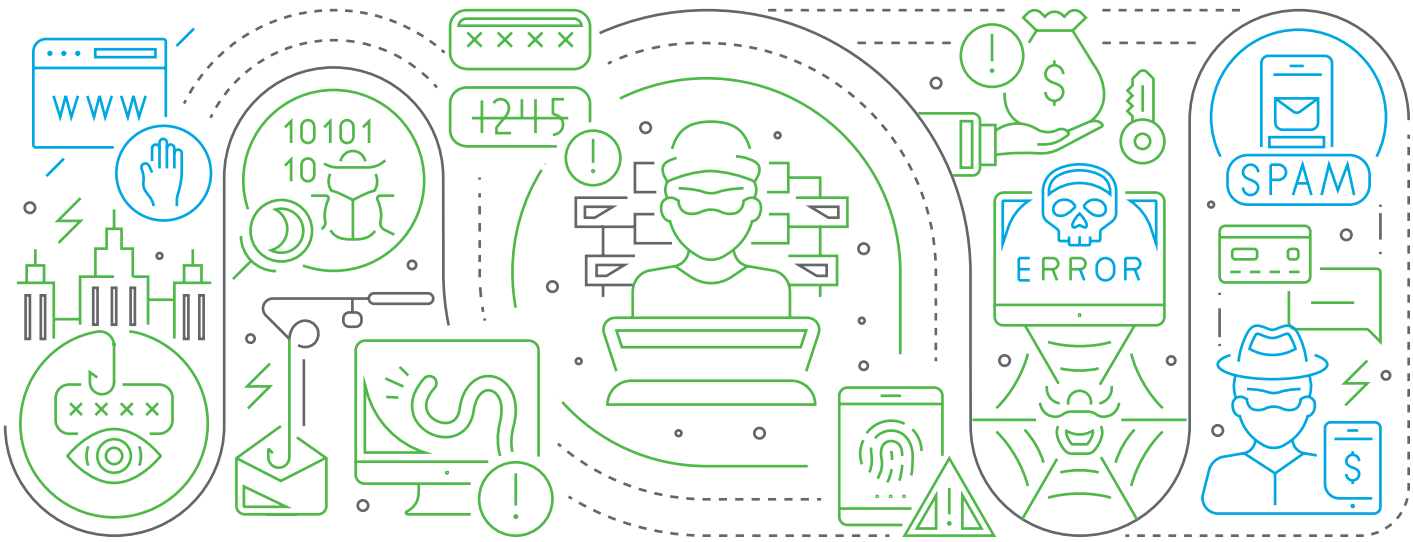
Let's assume that you're now much more aware of the risks cyber threats pose to your business than you were when you began reading this ebook. That's useful, but unless you take action it's not going to improve your situation. And the reality is that any good intentions you may currently have to improve your business cyber security are likely to ebb away as you're once again consumed with the day-to-day demands of running an SME. (And possibly the added demands of preparing that business for sale in the immediate or medium-term future.)

> Fortunately, there is a way to square this circle – outsourcing. If you and your staff don't have the bandwidth for it, you can delegate the task of getting your business' cyber security up to scratch to a third party such as RSM.

Cyber security experts you can rely on

RSM is a professional services firm that has a long history of working with Australian businesses and startups. Its Cyber Security & Resilience Services division employs some of Australia's most respected cyber security experts. Experts that are available to identify then address the most pressing cyber risks your business faces. RSM is also one of a small number of organisations in Australia that are CREST accredited for penetration testing with individuals performing the testing having CREST certifications.

After conducting a comprehensive assessment of the cyber security your SME presently has in place, RSM's cyber security experts can strengthen system controls and suggest best-practice policies and procedures for access control, monitoring protocols and system architecture.



ACKNOWLEDGEMENTS

Darren Booth – Partner, RSM
Ashwin Pal – Partner, RSM
Andrew Clifford – Partner, RSM
Harry Kingsley – Partner, K&L Gates
Gavan Carroll – Managing Director, Head of Capital Markets, Ord Minnett

THE POWER OF BEING UNDERSTOOD
AUDIT | TAX | CONSULTING

rsm.com.au

Celebrating 100 Est.1922 in Australia

RSM