



Telstra Business Intelligence | 

Securing your business and protecting your customer data.

# Insights and advice to help your business thrive in a changing world.

Welcome to the latest report of Telstra Business Intelligence 2021. In this series, we look at how Australia's small and medium businesses (SMBs) can take advantage of the opportunities technology creates – and how they can protect themselves from any associated risks.

The Telstra Business Intelligence Study saw us survey 1,000 consumers and 1,000 SMBs (businesses with fewer than 100 employees) to understand what customers expect and what small businesses deliver online. As things changed throughout 2020, we conducted further research and drew on other sources to help us understand how we could best support SMBs adjust to the new landscape.

Already in this series, we've shared reports on Digital Marketing and the broader Customer Experience journey – designed to help customers find and choose you, and help you meet their expectations online. We learnt that consumers are using digital platforms more and more to engage with businesses. In turn, businesses are using digital tools to respond to customer needs and manage business operations more efficiently. The shift to digital – accelerated by COVID-19 – has brought plenty of opportunities for SMBs, but it's also increased the risk of a cyber incident, the impacts of which can be severe.

The good news is that managing risks online isn't a dark art. With the right tools, advice and partners, it's more like an insurance policy that protects your bottom line, your reputation and your customer's privacy. Being proactive can even help you build trust with customers who want to know their data is being kept safe.

There's never been a better time to re-assess your business's approach to cyber security. We hope this report helps you on your way.

**Anne Da Cunha, Small Business Executive, and  
Matthew O'Brien, Cyber Security Executive, Telstra.**

# Contents.

<b>Foreword.</b>	<b>2</b>
<b>Introduction to Managing Risks Online:</b> Securing your business and earning your customers' trust online.	<b>4</b>
<b>3.1 Re-evaluating online threats.</b> Recognising the risks associated with doing business online.	<b>8</b>
<b>3.2 Assessing your valuables.</b> Taking stock of the business assets you need to secure.	<b>18</b>
<b>3.3 Security fundamentals.</b> Basic security strategies to protect your business and customers.	<b>24</b>
<b>3.4 Managing an incident.</b> Containing and mitigating the damage of a security breach.	<b>32</b>
<b>Cyber Security resources.</b>	<b>40</b>
<b>Appendix.</b>	<b>41</b>
1. Methodology.	<b>41</b>
2. Definitions.	<b>42</b>
3. Acknowledgements.	<b>42</b>



### 3.0 MANAGING RISKS ONLINE

Introduction

**Protecting  
your business,  
customers and  
bottom line in an  
evolving digital  
landscape.**

# Online security can help you build customer trust, protect your bottom line and maintain business continuity.

In the wake of COVID-19, consumers are spending and sharing more online and businesses are turning to new digital solutions to keep up. Along with a mass shift to working from home – bringing with it a greater number of networks and devices being used to conduct business – these factors have created an environment for criminals to exploit any gaps in security using known and new tactics.

---

## Security is seen as a secondary concern, while online crime is on the rise.

When we first surveyed SMBs for the Telstra Business Intelligence Study, their top concerns were around finding customers, improving revenue, controlling costs, improving cash flow and meeting customer service expectations.

Cyber security – the protective measures used to defend technology devices, networks and data from digital theft or damage – was a lesser concern for a significant proportion of SMBs. Our research suggested many businesses underestimate or don't fully understand the need for business-grade cyber security that can protect them from an online incident – whether it's a targeted or opportunistic attack, accidental data breach or other security issue. These happen frequently and can negatively impact the things SMBs care about most.

The Australian Cyber Security Centre (ACSC) (the Australian Government's cyber security agency) released a report on Cyber Security and Australian Small Businesses in 2020, which found that 62% of Australian SMBs they surveyed had experienced a cyber security incident, and that a cyber crime is reported in Australia every 10 minutes.

Recovering from a significant cyber incident can impact business continuity to such an extreme that, if the attack doesn't directly shut down your business, the time and money required to recover from the attack could. In that way, cyber security is not a nice-to-have – it's a cornerstone of running a successful business.

**86%**

of people surveyed\* agree they expect businesses will keep any personal data they provide secure.



Around

**1/4**

of SMBs surveyed\* had no formal measures in place to protect the information they collect from customers.

**There are benefits to being proactive.**

Cyber security is not just relevant to large organisations; any business that uses the internet or collects customer information needs to know how to keep its online assets secure. And while doing so is essential for safeguarding your business, it can also give it a competitive edge.

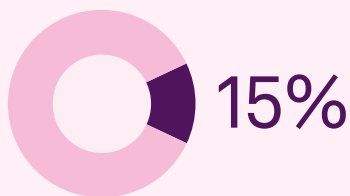


**“A cyber breach for a small business – which could involve the loss of critical information, client data or trade secrets – can have a devastating impact. The business may lose their competitive position, along with customer satisfaction and loyalty.”**

*Matthew O'Brien,  
Cyber Security Executive,  
Telstra*

**Consumers we surveyed\* told us the top 3 things they consider when deciding if they can trust a small business are:**

- ▶ 1. No hidden fees or charges
- ▶ 2. Delivers products/services consistently every time
- ▶ 3. Transactions and data are secure



But only 15% of SMBs surveyed\* placed security of transactions and data in the top 3 things they think are important to consumers in this context.

Knowing their information is secure can help customers trust your business and make them more likely to spend with you.

In fact, 82% of consumers in our survey\* told us that when they know of multiple businesses offering a similar product or service at a similar price, they choose the one they trust most, and online security is a key part of this.

Is your business losing potential customers through an outdated – or non-existent – approach to online security?



**“When making online purchases, cyber security is on my mind. The products I buy are normally from companies I know and trust.”**

*Joseph, 32, Kirribilli,  
NSW, consumer*

# Reap the benefits, avoid the threats.

A considered approach to how you manage online risks can help you take advantage of the opportunities – and avoid the hazards – that come with digitising your business.

## In this report, we will:

---



Equip you with an understanding of online threats and information about the kinds of valuable assets that need protecting in a digital environment.

---



Run through the fundamentals of security vulnerabilities to help you confidently engage with partners and service providers to best protect your business and customers.

---



Cover the steps you need to take in the event of a cyber incident, so you know how to respond if something does go wrong.

---

**As you adopt new technologies or working processes, are you also taking time to understand how to manage online threats to your customers, employees and business?**

# Download attachment?



3.1 MANAGING RISKS ONLINE  
Re-evaluating online threats

---

Recognising the risks associated with doing business online.



# After a year like no other, is it time to reconsider how your business is placed to avoid or respond to an online incident?

The changing digital landscape presents plenty of opportunities for businesses, but it also brings with it a heightened risk of online crime or an accidental data breach.

This section will outline changes in consumer behaviours and the SMB landscape, how criminals target businesses online, the impacts an incident can have, why small businesses are at risk, and why it may be time to re-evaluate your existing security measures.

---

## As habits change, customer concern grows.

Our working and buying habits changed in 2020, with more SMBs making the transition to doing business online (reflecting customer buying habits) and work being done remotely on more devices on different networks.

This growing dependency on new technologies and interconnected devices increases both the likelihood and potential severity of online incidents for both businesses and consumers.

Around a third of consumers we reached out to in June 2020<sup>^</sup> said they have become more concerned about cyber security and online safety due to COVID-19. And they're right to be wary.

According to IDCARE, Australia and New Zealand's national identity and cyber support service, over 10,500 individual cases of cyber incidents were reported between June and August of 2020. "During COVID-19 we have seen a 40% increase in volume of both individuals and organisations, big and small, impacted by cyber security issues and identity misuse," says Moises Sanabria, IDCARE's Head of Identity Security Operations Centre and Business Development Manager.

**62%**

of Australian SMBs have been victims of cyber crime.<sup>+</sup>



Almost

**60%**

of small businesses surveyed<sup>\*</sup> felt they could be doing more to protect their business from cyber attacks.

# The common types of online crime.

You don't need to become a cyber security expert to understand the main types of online crime, but to protect your customers and business, it is vital to understand how criminals attempt to breach SMBs.

As outlined by the Australian Cyber Security Centre (ACSC)'s Small Business Cyber Security Guide, the main online crimes that target Australian businesses and their customers are:


 <b>Identity theft</b>	 <b>Online fraud and shopping scams</b>	 <b>Bulk extortion</b>	 <b>Wire-fraud and business email compromise</b>
--	---	--	--



**“Data breach or compromise is the greatest business risk in today’s digital era.”**

*Keyur Desai,  
Principal Security Architect,  
APAC, Microland*

While all manner of fraud and scams can impact an SMB's reputation and bottom line, businesses should familiarise themselves with the following types of attacks:

  
**Scam emails or phishing**

### Scam emails or phishing

Fraudulent emails (often disguised as legitimate ones) designed to obtain sensitive data – including usernames, passwords, credit card details and customer information – that can be used for identity theft.

  
**Ransomware**


### Ransomware

A kind of malicious software (malware) designed to compromise your device and data. After infiltrating your device, criminals hold the information it contains to ransom by charging a fee to allow you access again.

Fraudulent crimes often begin in innocuous, commonplace ways, with malicious emails mimicking parking fines, missed deliveries, and other kinds of rudimentary messages you'll interact with without a second thought. Scams like these are very successful in installing malware or collecting logins and personal information, which can lead to a number of attacks including business email compromise.

# 93%

of consumers surveyed\* agree the security of their personal data is a priority for them.

# 86%

of consumers surveyed\* would avoid dealing with a business if they thought their personal data wouldn't be kept secure.\*

**The impacts of an online incident can be severe.**

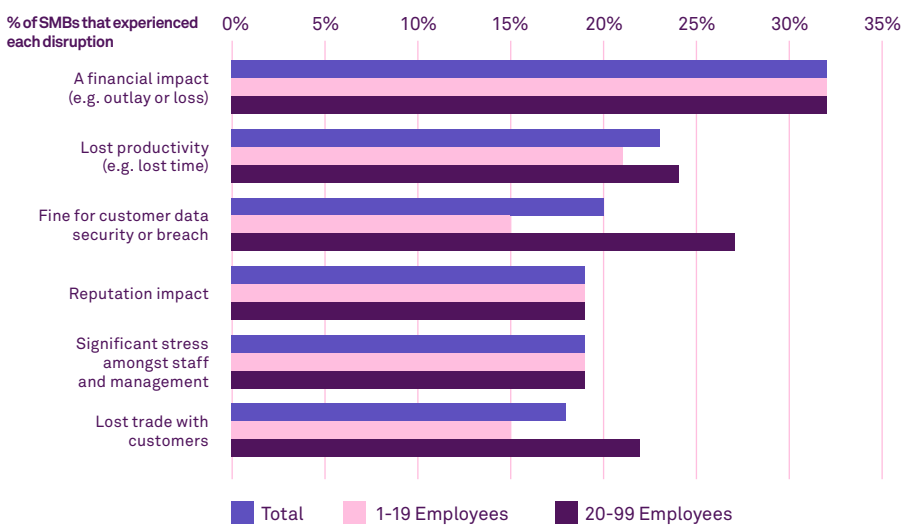
While many people and businesses will experience a cyber incident, not all of them will recover in the same ways – or at all. Of all the SMBs in our survey\* that experienced a cyber attack, 77% of them faced a major disruption to their business. Of those, over half said it took a matter of days to weeks to regain control. Notably, around 1 in 3 businesses we surveyed\* experienced a financial outlay or loss after being attacked online. This hit to a business’s bottom line can be due to lost trade, the cost of repairs and potential fines for breaching privacy laws – and money is only the tip of the iceberg when it comes to the potential negative impacts of a cyber attack.



**“Small businesses often live and die by their reputations. A cyber breach may result in customers losing trust in the business, and ultimately going elsewhere.”**

*Matthew O'Brien,  
Cyber Security Executive,  
Telstra*

**Negative implications experienced by SMBs due to a cyber attack.**



Source: Telstra Business Intelligence Insights Study December 2019. Question: Did the cyber attack that you experienced disrupt your business in any of these ways?

The financial impact can be significant, but recovering from a cyber attack also can affect productivity and business continuity, especially if business or personal data is compromised or held to ransom.

Significantly, almost 1 in 5 businesses we surveyed\* that experienced an attack suffered reputational damage. “Small businesses often live and die by their reputations,” says Telstra’s Matthew O’Brien. “A cyber breach may result in customers losing trust in the business, potentially resulting in loss of customers.” For example, if your customers’ personal data is breached, they might not buy from you again. Or, as outlined in our first report on Digital Marketing, it’s all too easy for unhappy customers to post negative reviews online as a warning to other potential buyers. And while the impacts of a cyber crime can be significant for consumers – including the possibility of identity theft and fraud – it can lead to prolonged negative impacts on businesses, their customers and their employees. “The largest concerns for any business are: will this event cause my customers harm, will they leave and will my business fail from this one event?” IDCARE’s Moises Sanabria told us.

Source: ^Telstra Cyber Security: Quantitative Research June 2020.  
\*Telstra Business Intelligence Insights Study December 2019.

# Why your business might be a target.

## Think your business is too small to be a target? Think again.

In fact, SMBs are often the target of criminals *because* of their size and the less robust security solutions they employ. “Often small businesses can be at risk due to having disparate solutions that aren’t integrated,” Samantha Zammit, Microsoft’s SMB Modern Workplace Lead, told us.

These disparate solutions might include the built-in measures that come with software, or a single shared password for your office network connection. “These fragmented solutions leave seams or cracks that can enable security breaches.” The numbers support this theory: 43% of all online crimes committed in 2019 targeted SMBs#.

“As small businesses are the backbone of a growing economy, they inevitably become the preferred target compared to large organisations which are more mature when it comes to implementation of security measures and controls,” says Keyur Desai, Principal Security Architect, APAC at Microland, a leading IT infrastructure services company with over 30 years of experience.

And small businesses don’t have to be individually targeted to become collateral damage in an attack. Consider the supply chain: your business could fall foul because a supplier you trust with your customer information could be breached.

Or if you are part of a supply chain for a larger business, any free or stop-gap security solutions could make you a weak link, and unlock a path into the organisation. In recognition of this risk, many businesses are establishing security standards that their suppliers must meet.

## Security can give you a competitive advantage.

Taking steps to safeguard sensitive customer data can increase customer satisfaction and trust, and help you to avoid reputational damage.

Customers assess the safety of your business the moment they arrive on your website, with 81% of consumers we surveyed\* saying they think a site being trustworthy (that is, one with an SSL certificate) is important when they are engaging with SMBs online. The tech they use helps in their decision-making: operating systems can alert consumers that they’re connected to unsecured networks, and browsers often tell them when a site is not secure. To develop trust with potential new customers and keep them coming back, your business needs to demonstrate its ability to keep customers’ information and transactions secure.

As we covered in our last report on digital Customer Experience, 70% of respondents in a recent Venture Insights survey<sup>7</sup> said they now consciously support local businesses. As customers look to keep their dollars close to home, demonstrating your security measures can go a long way in giving your business a competitive edge.



**“A business can show customers it’s secure online by having an SSL certificate on its website. In ‘https’ the ‘s’ stands for ‘secure’, which means the website is validated by a certificate saying it’s secure.”**

*Brooke Pengelly,  
Sales Leader of Small Business,  
Trend Micro*



**“I definitely would not use a website if it looked like it was unsecure. I would go purchase elsewhere.”**

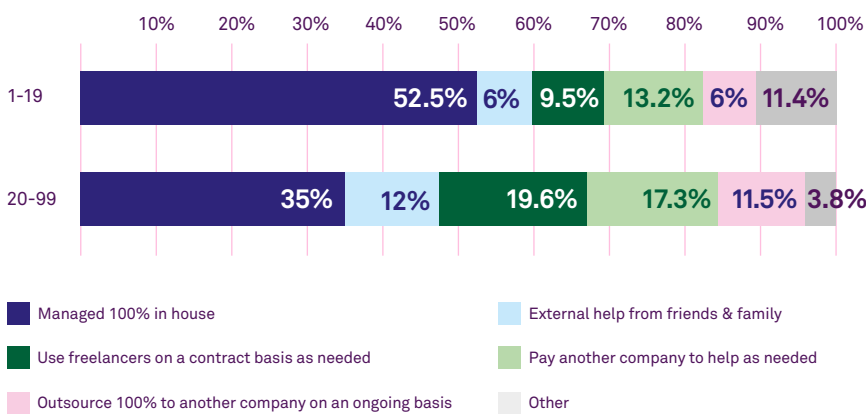
*Blair, 54, Caboolture,  
QLD, consumer*

Source: #Verizon 2019 Data Breach Investigations Report. \*Telstra Business Intelligence Insights Study December 2019. <sup>7</sup>Venture Insights Australian Consumer Behavioural Survey: Part 3 - Opportunities for growth in local online shopping.

# Are you doing enough to protect your business and customers?

The way you handle cyber security can also make you a target, and our research showed there was a wide variance among SMBs in this area.

## Approach to managing cyber security by business size.



Source: Telstra Business Intelligence Insights Study December 2019. Question: Small businesses often rely on external help or outsourcing. Please indicate your approach to cyber security.

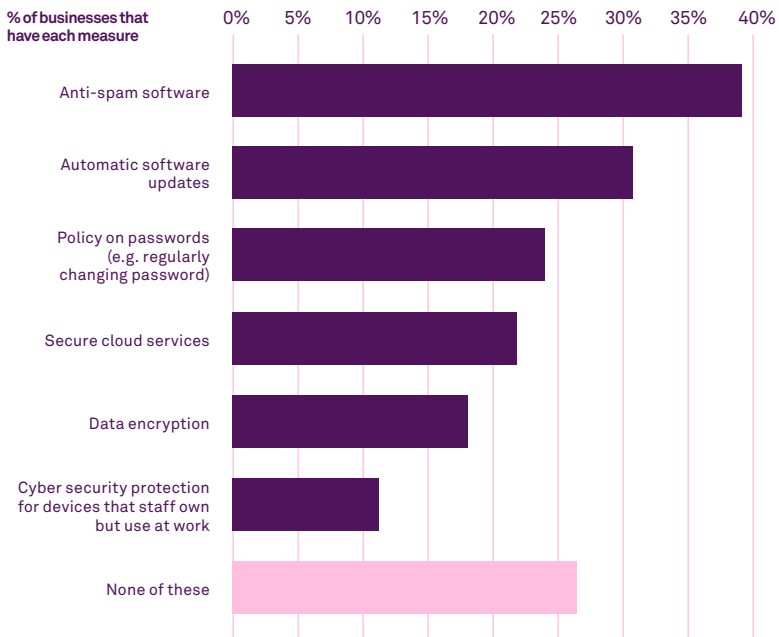
Many smaller businesses we surveyed\* – those with fewer than 20 employees – were commonly handling security themselves. Conversely, over half of all SMBs with 20 or more employees we surveyed\* use external support for cyber security, including engaging a freelancer or company when needed, outsourcing to another company on an ongoing basis, or getting help from friends and family.

Our research^ showed that many of the small businesses handling security in-house do so with basic, free, consumer-grade solutions that are limited in the protection they can offer. Those businesses that do outsource get help from a wide range of places\*, but those sources might not be fully set up to provide the current and best security expertise.

Source: \*Telstra Business Intelligence Insights Study December 2019.

We also found that many of the SMBs we surveyed\* in late 2019 didn't have the adequate protective measures in place that have been shown to help prevent a cyber security incident, with over a quarter having no measures in place to protect their customer information.

**Security measures SMBs have in place to protect customer information.**



Source: Telstra Business Intelligence Insights Study December 2019. Question: Which of the following, if any, does your business have in place to protect the information you collect from customers?

Some of the more favoured security measures of the SMBs we surveyed\* included anti-spam software, automatic software updates and password policies. Our research suggests that smaller businesses (those with under 20 employees) are not as proactive as bigger ones when it comes to implementing cyber security measures to protect their customers' information.

Those businesses with few or no security measures in place could be putting their customers, their business continuity and their bottom lines at risk. Of the SMBs we surveyed\*, 44% said they could be doing more to protect their business from cyber attacks.

This number rose to 56% when we just looked at SMBs with 20-99 employees, which suggests that bigger businesses better understand the risks and impacts of an online incident. Regardless of business size, many SMBs could be doing more to protect their business and their customers.

Source: \*Telstra Business Intelligence Insights Study December 2019.

# Online security begins with thinking differently.



**“Taking a proactive approach to cyber security means you are less likely to be breached.”**

*Matthew O'Brien,  
Cyber Security Executive,  
Telstra*

If you knew, in a week, your business would be targeted by criminals, would you prefer to clean up the fallout of the attack after it happens, or get proactive now and attempt to stop it from occurring in the first place? “The steps for prevention are better than needing to find the cure,” Telstra’s Cyber Security Executive Matthew O’Brien advises. “Taking a proactive approach to cyber security means you are less likely to be breached.”

Consider who is in charge of your online security. Do they have the expertise required to be ‘always on’ in this fast-moving space? Can they help to prevent an attack, or are they a ‘break-fix’ solution, one that might be able to help you patch together a remedy, but doesn’t decrease your risk? If it’s the latter, can your business afford the time, money and stress of managing an attack after it happens?

Larger SMBs often defer to experts to handle their approach to security, but relying on external expertise is not always enough. With security handled elsewhere, those inside the business may not dedicate the necessary time to building an understanding of the online threat landscape.

The first step is to think about security not as something you can buy and implement once, but as an ongoing, active change in behaviour to protect your business. Keyur from Microland agrees: “Enforcement of a good cyber security hygiene across your organisation is a continuous process and not a one-stop solution.”

Every business has a unique level of risk when it comes to online threats. But no matter your risk profile, it’s vital to take a proactive and preventative approach, rather than trying to repair the damage later. Because the effects of online crime are not just felt in your pocket, but also in your ability to meet your customers’ expectations around trust and security.




**“Enforcement of a good cyber security hygiene across your organisation is a continuous process and not a one-stop solution.”**

*Keyur Desai, Principal Security Architect,  
APAC, Microland*

## It happened to us: Decorative balloon company.

A balloon company relaying online orders to events and décor suppliers across the country.

 Founded: late '90s

 Number of employees: 5

We have featured this business anonymously to protect its privacy.



In 2007, George\* hired an overseas company to set up a website for his balloon supply company to maintain stock levels, handle payments and reporting, and service his partners around the country.

When orders stopped one day, George discovered his server had been hacked. He restored the homepage he'd saved to a hard drive, updated the login and password, and hoped for the best.

Three days later, the attackers changed it back. As this back-and-forth went on, George escalated the problem with the company that had built and still hosted his website, "but they washed their hands of it". George had recruited different IT help to assist with ad hoc changes over the years – the result was a website "stitched together with sticky tape", and with no back-up.

About a week in, there was a new homepage message saying the hackers were holding the company's database to ransom. George paid \$5,000 to hire an expert who moved the website to a cloud host and discovered, thankfully, the database was still there, hidden within local files on the server.

As this happened, George took orders by phone, which cost his business a couple of thousand dollars' worth of staff hours. Two weeks of forced downtime cost George, he estimates, over \$20,000 in sales and commissions.

Doubling the financial hit was the "stress and grey hair" that came from recovering from the incident. "It would've been a million times better if somebody came around with a brick and smashed a window," he says.

Knowing what he knows now, the message he'd give his past self is to be more proactive and set greater expectations for the suppliers he works with. With all the losses tallied up, the cost of developing a cyber security plan pales in comparison.

**"It would've been a million times better if somebody came around with a brick and smashed a window."**

*George\*, owner,  
decorative balloon company*

\*Not his real name.



## Your re-evaluating online threats checklist.

### Inform yourself.

- Stay across the latest on cyber security threats and encourage others who work within or with your business to do the same.
- Educate yourself on how you can better protect your business by making a habit to read a cyber security news story each day.
- Great places to start are the small business updates on [cyber.gov.au](https://www.cyber.gov.au), and the technology sections on news websites, like the [ABC](https://www.abc.net.au).
- Consider how your cyber security needs may have changed in light of COVID-19.

### Put yourself in your customers' shoes.

- Understand what your customers expect from you in a digital environment, and the associated security you might need to implement to meet these expectations, e.g. SSL certificates, reCAPTCHA codes. Begin by checking your websites on different devices and operating systems; do any warnings appear?
- Consider how you can use cyber security to show your customers you're trustworthy. You might have assurance your website is safe – can you add any info to it so your customers have the same peace of mind? Outline your privacy, security and data policies.

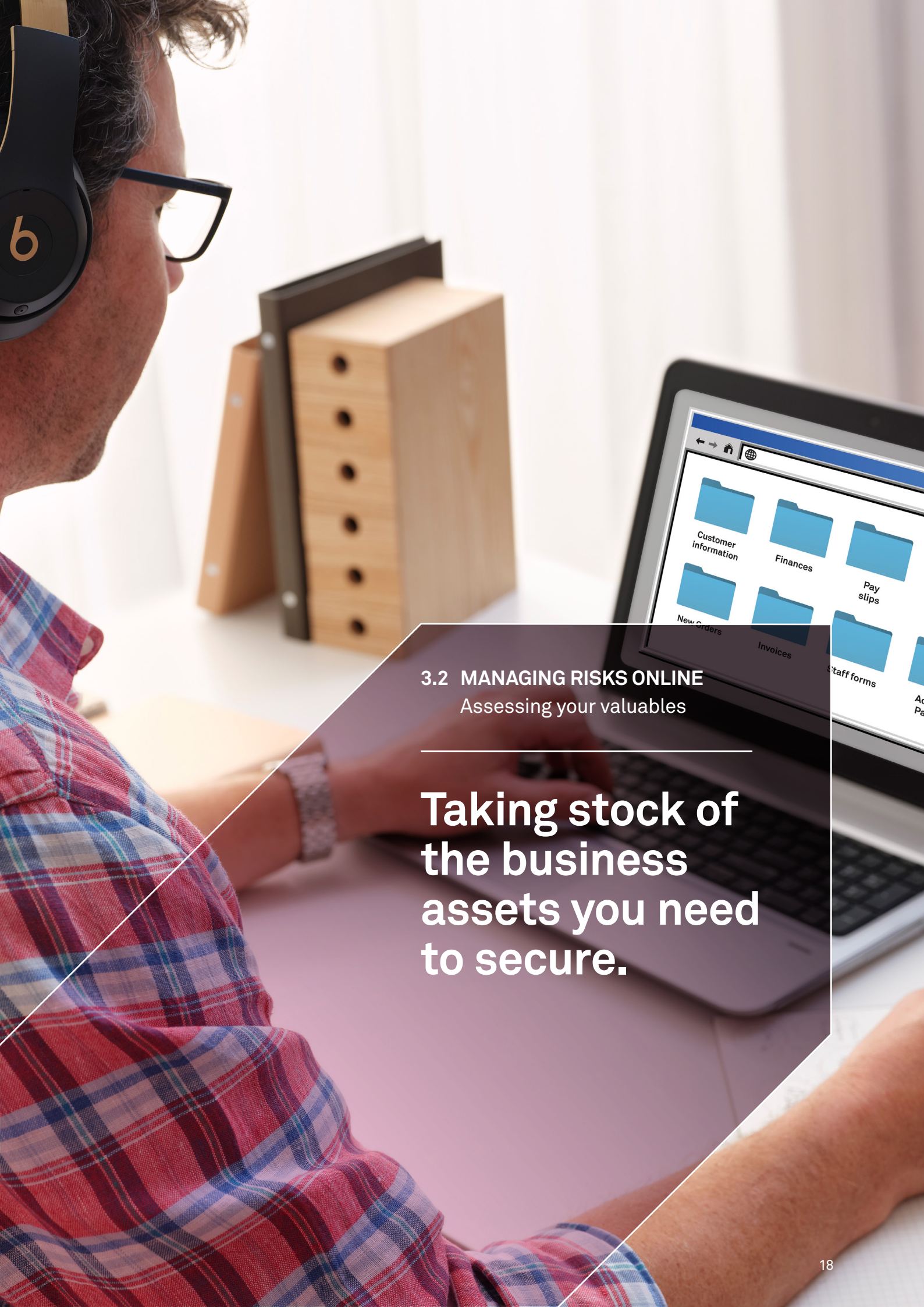
### Set or follow procedures for every link in the supply chain.

- Are you part of a supply chain (or are other businesses part of yours)? Ensure you understand or communicate the security expectations at every link of the chain.

## Is your business keeping up when it comes to online security?

Once you understand these risks, there are strategies you can use to confidently manage them and expertise you can outsource.

Get started with expert advice from [Telstra Business Cyber Security Services](#).



### 3.2 MANAGING RISKS ONLINE

Assessing your valuables

---

**Taking stock of  
the business  
assets you need  
to secure.**

# Do you know what criminals are looking for?

The day-to-day actions you take to keep your valuables safe are second-nature. You know where your wallet and credit cards, phone and keys are at all times, because they're essential to your life and losing track of them can be a costly headache.

When it comes to securing your business, 'valuables' refers to data, information and intellectual property. These things need the same kind of ongoing daily protection because if they are stolen, lost or compromised, it could have a significant negative impact on your business, customers or employees.

This section looks at the types of valuables that can be targeted or breached, the ways this can happen, and the importance of creating a plan to ensure you can maintain operations in the event of an incident.

## What cyber criminals want.

Cyber criminals are looking for money, and they try to get it either directly – by infiltrating financial systems to siphon off money from bank accounts – or by extracting critical business data and either holding it to ransom or selling it on the dark web.

Criminals clearly see a value in the data SMBs retain – even if not all businesses do. We found that, while many SMBs are aware of potential financial impacts of online crime, they don't necessarily have a thorough enough understanding of the potential threats to view themselves as targets; 64% of SMBs we surveyed\* told us they think cyber attacks would have a limited impact on their customers as they don't keep sensitive customer information. But many SMBs may be inadvertently, rather than consciously, collecting and storing data online.

SMBs need to consider the safety, security and privacy considerations of their customers, including what personal data they collect and store. Australian eSafety Commissioner Julie Inman Grant has a reminder that the internet can create opportunities for people to exploit, harm and abuse others. "Every online business or platform collects sensitive customer data," she says. "In most cases it is in the form of seemingly benign registration and sign-up information, including customer names, email addresses, telephone numbers and dates of birth. But this information can be misused to target, harass and abuse others."

# 24%

of SMBs surveyed\* had no formal measures in place to protect the information they collect from customers.



**"I've been to sites before when I possibly am looking to purchase, and if they don't have credit card security information or if there aren't secure payment methods, I won't purchase. I'll look to purchase elsewhere."**

*Anna, 33, Mosman, NSW, consumer*

# What is considered valuable?



**“Every online business collects sensitive customer data. This information can be exploited for illegal and inappropriate use unless proactive measures are taken to ensure its protection. Securing the safety, security and privacy of customers and their data should be a priority for all businesses.”**

*Julie Inman Grant,  
eSafety Commissioner*

Types of online valuables include:



## Customer data

All of the sensitive or personal information your business holds about the people and organisations it serves. This varies between businesses, but can include names, DOBs, purchase history, credit card information and email addresses.



## Employee data

Personal information or sensitive data, including tax file numbers, salaries or home addresses.



## Intellectual property

Data that may be considered commercially sensitive and important to keep confidential in the interest of your competitive advantage or viability of business operations e.g. product designs, strategies/plans and customer information.



## Critical business data and application

Other types of business data may be valuable due to the operational impacts they would have if lost or made inaccessible e.g. business data that could cause business continuity issues if ransomed or lost/destroyed, your website which could be copied/hijacked by criminals.

As well as putting your business, customers and employees at risk, security incidents can potentially have legal ramifications. For businesses in some industries and with annual turnover of over \$3 million, the information your business holds about customers and partners is governed by [the Privacy Act](#), which also specifies that it needs to be managed and stored securely.

Outside of these regulatory considerations, consumers place high value on the security of their personal data and it's a key factor in deciding if they can trust a small business.

# Time to audit your information.

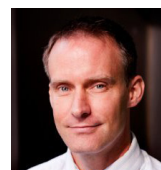
“The first step an organisation should take is to understand the data they have, the content of that data and where it is stored,” advises Gary Gardiner, the Head of Security Engineering, APAC at Check Point. “This will allow the company to look at the controls, policies and procedures it has in place to ensure the security of the data and the resources that access the data.”

When you're putting security barriers in place, imagine your business is a person going for a walk in the rain: one solution, like a pair of gumboots, is handy for staying dry.

But layering a few protective methods – including multi-factor authentication, a password manager and a secure VPN – will combine to keep you as safe as possible, like virtual umbrellas and raincoats. Implementing basic, foundational defences like these can prevent a whole class of attacks.

In creating your protection plan or policy – the formal measures your business takes to keep your data safe – be sure to assess the security of all types of digital data your business is handling or creating, and prepare the proactive measures your business will implement from now on.

The measures – which can be built into every part of the IT management processes – are known as ‘security-by-design’. Beyond protecting against crime, SMBs need to plan for business continuity and data to be protected, regardless of any external malicious attack.



**“The first step an organisation should take is to understand the data they have, the content of that data and where it is stored.”**

*Gary Gardiner,  
Head of Security Engineering,  
APAC, Check Point*




**“Small businesses should consider security-by-design, privacy-by-design and user safety considerations which are balanced when securing the ongoing confidentiality, integrity and availability of personal data and information.”**

*Julie Inman Grant, eSafety Commissioner,  
Office of the eSafety Commissioner.*

## How they do it: myAutonomy.

An NDIS plan management provider helping people with disabilities and their carers live independently.

 Founded: 2020

 Number of employees: 4



John Drill and his team at myAutonomy support people who are covered by the National Disability Insurance Scheme (NDIS) with managing administration and budgeting needs for their unique requirements.

The business consults remotely and must ensure client data (like home addresses, disability information and financial details) is managed and stored securely.

As a service provider working with the NDIS, myAutonomy must adhere to strict guidelines around privacy and sensitive information, and John had to demonstrate that his business is secure and complies with government requirements.

The business uses firewall protection and security software to identify potential threats, along with internal controls over financial information and the secure filing of incoming details. Using cloud-based software paired with additional security measures, the business ensures its applications are protected and its data is backed-up securely. “We have two-factor authentication when we’re dealing directly with the NDIS and also for access to our finance software.”

Because they handle millions of dollars of clients’ money, John and his team are vigilant of phishing scams and trained in spotting suspicious activity. “People are willingly trusting us and hoping we have the controls in place to protect them.” He also contracts an online security expert to assist with things like automated software updates and patching, and help if an incident does occur.

With team education, up-to-date security software and expert help, the business is best placed to prevent online threats and act suitably if there is an attack.

**“People are willingly trusting us and hoping we have the controls in place to protect them.”**

*John Drill,  
founder, myAutonomy*

## Your checklist for assessing your valuables.

### Get the full picture on what data you have...

- Audit your digital footprint to make sure you understand what data you are creating or collecting.
- Check when was the last time you backed up your website or files.
- Run regular tests to ensure you can recover your website or files, and check that your back-up frequency is adequate.

### ... And where the data is located.

- Review where and how your data is being stored. If someone found their way into your devices, network or software, could you keep this data safe?
- Consider the data you are creating or collecting in the context of [the Privacy Act](#). Is your business governed by these regulations, and are you equipped to satisfy them?

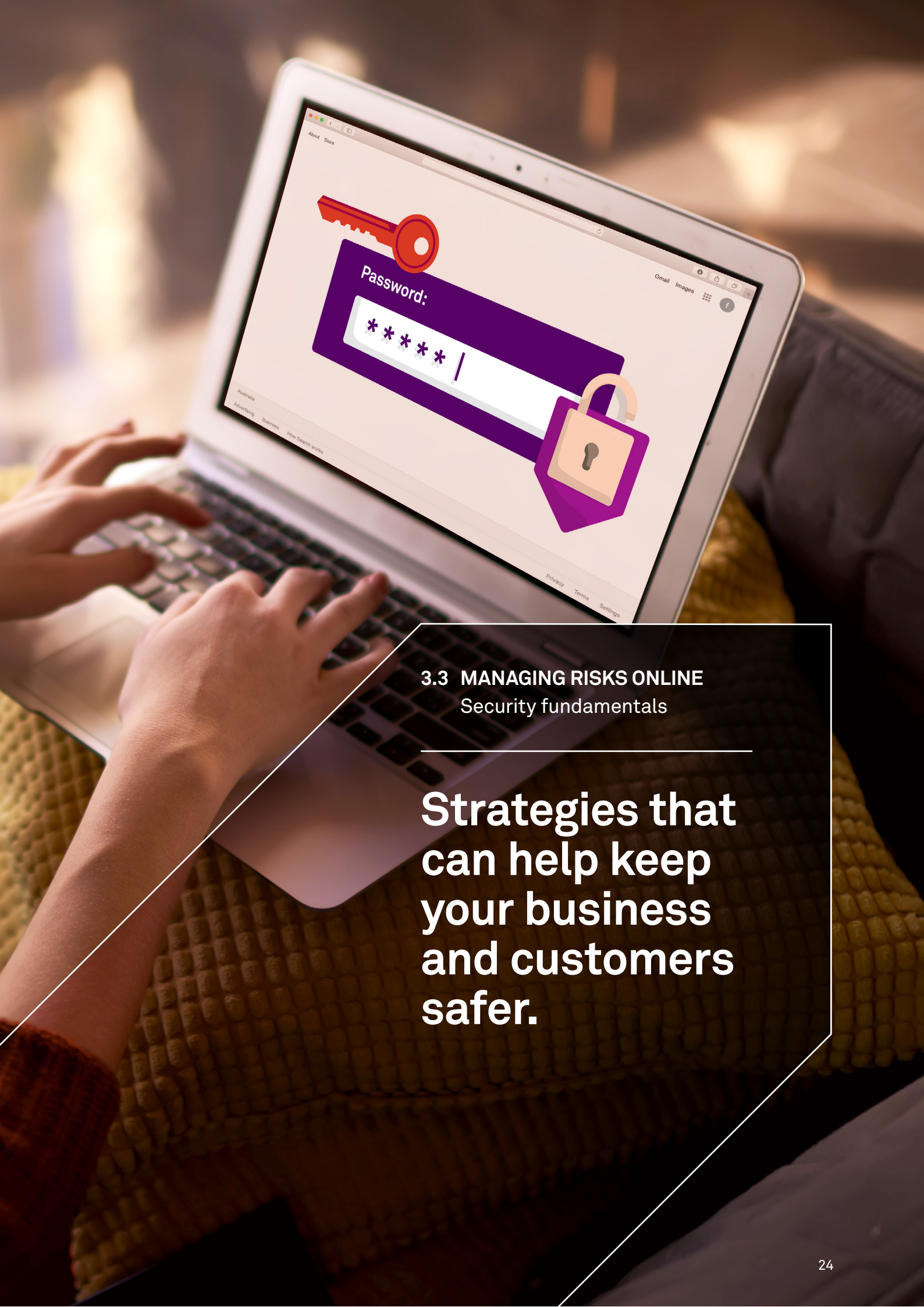
### Establish procedures for protecting data.

- Only collect the customer data you need, as this could reduce the impact of any breaches.
- Create a clear protection plan or policy for management of customer, employee and business critical data.

## Need to protect your business's valuables?

Telstra Business Cyber Security Services offers 24/7 support, regular cyber security updates, protection across a range of compatible devices and four cyber security assessments per year.

Learn more about how we can help [safeguard your business from threats](#).



### 3.3 MANAGING RISKS ONLINE

Security fundamentals

**Strategies that  
can help keep  
your business  
and customers  
safer.**



# Your security practices are your first line of defence against a cyber breach.

While no measures can guarantee absolute security, SMBs can implement some security fundamentals and adopt a protective mindset to minimise risks for their business, customers and employees.

This section will look at the vulnerabilities that might exist in your business so you can understand your risk profile and start to build a plan to help protect what matters.

## Creating your risk profile.

Now that you've taken stock of the valuable data and information your business retains, it's time to assess how vulnerable your business is to attack, and where those vulnerabilities lie.

"A cyber security vulnerability is a weakness which can be exploited by an attacker to gain access to a computer system," says Matthew O'Brien, Cyber Security Executive at Telstra. "Common weaknesses cyber criminals look out for can be technical (things like unpatched systems or software that hasn't been updated in a while) or ones caused by human error and lack of awareness."

When it comes to securing your business, keep your protective measures as holistic as possible. Risks emerge as a result of fragmented approaches (multiple separate solutions from different providers) to protection. Having a single system or partner is not just easier to manage, but critical to ensure you're doing all you can to prevent an incident – rather than dealing with the fallout of one.

## To develop your cyber security approach, start by breaking down the following things that comprise your working environment:

### WHO

Who is doing the work – humans who provide first line of defence through their actions.

### WHERE

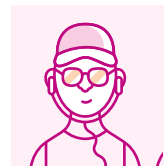
Where they are working – environments and networks where the work happens.

### HOW

How they are working – tools and programs used to create, share and store information.

# 72%

of employees surveyed\* would like more support and training when new technology is introduced at work to enable them to use it productively.



"I think it's really important that websites and online retailers have key mechanisms along the purchase journey to help with cyber security."

Things like needing to log in and authenticate who you are, reCAPTCHA, two-factor authentication for cards and things like that."

*Dominic, 29, Ivanhoe, VIC, consumer*

Source: \*Telstra Business Intelligence Insights Study December 2019.

# Who



## Vulnerability: Business owners and managers.

As guardians of the security of the business, business owners and managers are responsible for keeping up with the changing climate of online security. Keeping an SMB safe is not a 'set and forget' project. It's more like a car you drive every day, checking its dash frequently and getting it tuned up every now and then. As new challenges and risks emerge, it's vital for SMBs to have a consistent security mindset.

### What to do:

Educate yourself on government and expert recommendations, and seek out advice when you need it. Make a point to read reports, articles and studies regularly to ensure your awareness of the space is up-to-date. Support employees through dedicated training when new technology is introduced at work. Encourage employees to embrace new processes through transparency: you're all working toward the same goal.



**“When it comes to employees, your cyber security controls are only as good as your weakest link, with most breaches involving some kind of human error.”**

*Matthew O'Brien,  
Cyber Security Executive,  
Telstra*



## Vulnerability: Employees, contractors and suppliers.

The more people connected to a business, the greater the risk. One of the most common types of attacks on SMBs begins when a person clicks on a malicious email link. This and other types of human error can illuminate security weaknesses that criminals are waiting to exploit.

### What to do:

Create policies and have clear processes that both educate your employees on the relevant risks and instil in them habits that will bolster your business's security. When it comes to the way employees manage the tools and software your business uses, ensure everyone has up-to-date training. Be vigilant around access and identity – do you know who can access what, and do you have the authentication tools to know who they are?



**“All industries should seek to put user safety and rights at the centre of the design, development and deployment of online products and services, in order to safeguard their customers, and ensure that safety measures are baked in at the front end – and not bolted on as an afterthought.”**

*Julie Inman Grant,  
eSafety Commissioner*



## Vulnerability: Customers.

Any time a customer engages with a business online, they are creating digital data. A record of their information and behaviour is an attractive prize to criminals. Businesses need to consider how they protect customers – and, by extension, their business – from the outset.

### What to do:

Embed security into your product and experience design. The [Australian Government's Safety by Design initiative](#) can help you to embed safety into the culture and operations of your business at each stage of the product development lifecycle.

# Where



## Vulnerability: In the workplace.

A business's online assets are at significant risk if a criminal hacks its office network, so secure Wi-Fi or internet network is one of the most important barriers against attack.

### What to do:

Upgrade to a business-grade solution to help keep your workplace network more secure, and implement identity management (individual sign-in details) to restrict outside access. Are any of the devices that connect to your network mobile? Mobility and device protection should be applied to laptops, tablets or mobile devices that move between spaces and networks.



## Vulnerability: At home.

If any owner, manager or employee of a business works at home, the opportunity for a breach expands to include the networks they are signed in to and other devices attached to those networks, known as the Internet of Things (IoT). This includes voice assistants and Wi-Fi-enabled appliances. Working from home was already common among sole traders and suppliers before 2020, and COVID-19 lockdown accelerated this for employees of all kinds of businesses.

### What to do:

Implement working from home and device management policies to keep your business and devices secure, whether they belong to you or your employee.



## Vulnerability: On the go.

When employees work remotely, they may connect their mobile devices to unsecured networks at airports, cafes, hotels and other locations where business valuables can be intercepted and hacked.

### What to do:

If your business involves work outside of the office or home, implement policies and education on secure networks.



**“A growing number of devices coming from unsecure networks to your secure business network means more opportunities for cyber criminals to use them to infiltrate your company’s network and data.”**

*Keyur Desai,  
Principal Security Architect,  
APAC, Microland*



**“As data increasingly moves out into the cloud and more people work remotely, the scope of protection broadens in a way that requires businesses to think about how they defend, detect and respond across multiple potential points of security breach.”**

*Samantha Zammit,  
SMB Modern Workplace Lead,  
Microsoft*

# How



## **Vulnerability: Email and messaging.**

The ways a business communicates and shares information can be intercepted or exploited.

### **What to do:**

Make sure you're using a secure, business-grade email solution and that your employees can recognise malicious messages, especially as scam emails become more sophisticated. If sending sensitive documents or data files, consider encryption or password protection for extra security.

For large financial transfers, double check details verbally before transacting.

---



## **Vulnerability: Storage.**

Depending on how it's stored and backed up, business information – including sensitive data, company assets, documents and files – can leave a business more vulnerable to ransomware, inappropriate access and malicious attacks.

### **What to do:**

If your current storage solution needs an update, consider switching to something more secure. Cloud storage is an option that can allow you to both work on and store important documents online, making ransomware less effective.

If you're using an on-site server, ensure you're backing it up regularly. You can also consider encryption for sensitive documents and data files as an extra layer of protection.

---



**“Not all data needs to be treated equally, but it is important to ensure your critical data is protected.”**

*Matthew O'Brien,  
Cyber Security Executive,  
Telstra*

# How



## **Vulnerability: Tools and applications.**

The third-party software and tools used to create, access and transfer digital data need to be considered as part of an overall approach to security.

Applications, email clients, software, online tools and social media can all provide criminals (and even employees) with many avenues from which to launch an attack.

### **What to do:**

Consider your security ecosystem holistically rather than relying on what comes with a tool or program.

Only use trusted programs, consider who gets to administer them on behalf of your business (access controls), keep them updated (preferably through auto-update) and patched to remove known security flaws, and consider implementing identity controls like password policies, a password manager and multi-factor authentication.



## **Vulnerability: Devices.**

Whether they are supplied by the business or belong to employees, devices are vulnerable to breaches. The more there are, the greater the opportunity for criminals to find a way in through them.

### **What to do:**


Use protection software that gives you the ability to remotely wipe devices, and develop a tailored plan to secure the devices you and your employees use. This could include implementing a personal use policy and minimum requirements for passwords with regular mandatory changes.


“With so much money in cyber crime, attacks and breaches are increasing, so invest the time and effort to protect yourself. My advice is: Understand how to secure your business or work with someone who does. Test your back-ups and review incident response plans to ensure you can rely on them when needed, minimising damage from breaches.”

Suzi Dyke, Senior Security Specialist, Telstra

## How they do it: Water Tight Canberra.

Water Tight Canberra is a local plumbing, drainage and gasfitting business.

 Founded: 2010

 Number of employees: 14



Tom Martin, the owner of Water Tight Canberra, realised that if he was going to rely on digital tools – like electronic job quotes – and store customer emails and company financial data, he needed to make online security a priority. “As we continued to implement new technology, we knew we needed to stay protected with straightforward and effective online security measures.”

The business conducted its own research and consulted an expert to evaluate its online security. “We dedicated time to learn about online security. It’s actually simple to put in steps like two-step authentication, anti-virus software and HTTPS encryption. It takes a minute, but it keeps things much more secure,” says Tom. Things like security training for new employees, securely storing customer data, having a mobile device management strategy and using a password management system are some of the essentials they’ve adopted.

Online security must be a priority for everyone in the business – from the administration team to each of its plumbers in the field – for it to be effective. By using cloud-based programs to store documents and data securely, the business operates with up-to-date applications. And at regular meetings, staff check and update their own software and phone applications. “This ensures the not-so-tech-savvy plumbers can get support from the younger generation, if they need it.”

These measures – along with an incident response plan – give Tom peace of mind that if an attack were to occur the effects would be minimal. “All of our data is recoverable.”

“You’ve got to remember that using tech in the first place is saving you a hundred times in terms of efficiency. The slight inconvenience of making sure you’re doing it securely is tiny in comparison to what it could be saving you.”

**“It’s actually simple to put in steps like two-step authentication, anti-virus software and HTTPS encryption.”**

*Tom Martin,  
owner,  
Water Tight Canberra*

## Your security fundamentals checklist.

### Develop your risk profile.

- Consider how work is done online – through what devices, connected to what networks and by whom (consider suppliers, customers, employees).
- Use this information to formulate your risk profile and look for gaps or vulnerabilities where you may be under-protected and possibly at risk.
- Consider the value of your data, both to yourself and others, and the potential impacts of business downtime.

### Find the people who can keep you secure.

- Review any new solutions you may need to put in place to patch up those gaps and minimise risks. This might be device protection, network security or access protocols.
- This is a great point to enlist a cyber security expert or partner to conduct an audit and explore the right solutions for your business.

### Share new approaches with your team.

- Do employees and others in the business understand how to keep devices safe if they need to work from home or other networks? This information can form a business device policy.
- Consider how you are going to approach cyber security in an ongoing manner, as part of routine business operations and continuity planning. Try scheduling in regular blocks of time for all staff to perform routine updates and change passwords. This can help to send the message that consistent security maintenance is part of day-to-day work.

## Need a hand assessing your business's vulnerabilities?

Telstra Business Cyber Security Services can work with you on a personalised, multi-layered protection plan across your internet, email and devices.

[Discover how we can help.](#)



3.4 MANAGING RISKS ONLINE  
Handling an incident

---

**Containing and  
mitigating the  
damage of a  
security breach.**



# If your business was breached tomorrow, would you know what to do?

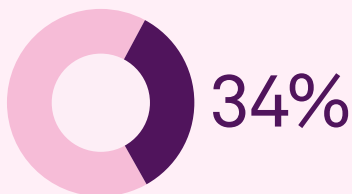
Regardless of the extent of your business’s online presence, the risks and vulnerabilities we’ve outlined in this report apply to all businesses that are connected to the internet.

Many SMBs in our survey said they are unsure of what to do if their business is breached online. If you’re among them, this section will cover the steps to take if your business is compromised, what your legal obligations are when it comes to disclosing a breach to authorities and customers, and some best-practice guidelines for mitigating the damage.

# 34%

of SMBs wouldn’t know what measures they need to take if their business experienced a cyber attack\*.

## SMB vs consumer confidence in responding to an attack.



34% of SMBs surveyed\* wouldn't know what measures they need to take if their business experienced a cyber attack.



59% of consumers surveyed\* don't feel confident they know the steps to take if their personal data was exposed via a breach.



**“It’s likely that at some point an SMB will experience a cyber attack. The number one critical item all businesses should have is a response and communication plan to help manage a breach.”**

*Matthew O'Brien,  
Cyber Security Executive,  
Telstra*

\*Telstra Business Intelligence Insights Study December 2019.








# What to do if you've been targeted.



**“I’m always concerned about my data being sold on. Also, if a company gets hacked and your data is stolen, that’s a concern.”**

*Blair, 54, Caboolture, QLD, consumer*

If you believe your company has been the target of a successful attack, the steps you should be prepared to take are:

-  **Step 1: Confirm**
- 
-  **Step 2: Report**
- 
-  **Step 3: Repair**
- 
-  **Step 4: Communicate**

By establishing and following an action plan, everyone in your business can be on the same page to begin taking these steps concurrently, to help you recover faster.

---

## How to confirm a data breach



### Step 1: Confirm.

“The first thing to do in the event of a cyber security attack is to get confirmation of the attack and determine what, if any, information has been exposed or potentially stolen, and attempt to contain the breach,” advises Matthew O’Brien, Telstra’s Cyber Security Executive.

If, after assessing, you confirm that a breach has occurred, you need to be across the local legal requirements around disclosing a data breach to customers, industry bodies and the government.

---

## How to report a data breach



#### Step 2: Report.

According to the ACSC's Cybercrime in Australia July to September 2019 report, there are some steps you might take to respond to common types of cyber crime:

- 1. Report the crime to [ReportCyber](#).** ReportCyber directs your incident to a local police specialist.
- 2. Contact your bank if your financial information has been compromised.** Have you shared banking details with or sent money to someone you don't know? Tell your bank immediately.
- 3. Contact IDCARE if your identity has been stolen.** For the best hope of recovering your identity quickly, get in touch with IDCARE's Identity and Cyber Security Counsellors or download their [Cyber First Aid Kit](#).
- 4. Report it to the [Office of the eSafety Commissioner](#).** Keep a record of and report any offensive, illegal or abusive content you find online.
- 5. Report scams to [Scamwatch](#).** This is the step to take when you receive a suspicious email or text.

There may be financial consequences if consumer information is compromised; 20% of SMBs we surveyed\* who experienced an online security attack received a fine for breach of customer data.

While the mandatory breach notification only applies to small businesses with a turnover of more than \$3 million, notifying the bodies listed above (where relevant) and customers is generally recommended. "We believe notification is in the best interest of the business and their customers," Matthew says. "It's also worth noting that if a company has a cyber insurance policy that covers them financially in the event of a breach, failure to notify may void the policy."



### Step 3: Repair.

Internally, you'll want to begin to try and fix the damage caused by an attack straight away. To do this, you or a person you employ will need to identify and close the breach entry point. Calling on an experienced partner to advise you throughout the process can help to make a draining and costly experience a little smoother.

Moises Sanabria, Head of Identity Security Operations Centre and Business Development Manager at IDCARE, Australia and New Zealand's national identity and cyber support service, suggests engaging a partner who can help you to understand the risks associated with the data lost and form up an action plan including who to notify.

**“Some top tips are: Apply the latest updates. Use strong passwords. Use multi-factor authentication when available. Good habits are equally essential in staying safe and secure.”**

*Cynthia Wong,  
Cyber Security Product  
Owner Principal, Telstra*



### Step 4: Communicate.

Even if you don't have any legal obligations to disclose what happened, many businesses wanting to do right by their customers might make the choice to inform them of the breach. This gives customers the opportunity to do things like change their passwords or check any suspicious activity that might have occurred as a result of their data being exposed. Do you know how to communicate with your customers in the event of an online incident?

“The number one critical item all businesses should have is a response and communication plan,” Matthew says. Knowing how to provide an effective response – which should include who you need to notify and can call for help with identification and remediation – is essential. “My belief is that, as good corporate citizens, it is incumbent on all businesses to notify their customers if they believe their personal information has been breached.”

Moises agrees, recommending SMBs make themselves available to customers to reinforce a sense of care and trust. He also encourages SMBs to keep a record of their actions as they deal with the breach, and make the process transparent. “Communications that show a specific record of when you took what actions and who was notified will give clients confidence. Poor communication will create concern, distrust, anger and more customer engagements to manage.”

**“It's likely that at some point an SMB will experience a cyber attack. Investment in establishing a clear response, recovery and communication plan, as well as providing fundamental cyber security hygiene, is critical to reducing the impact.”**

*Matthew O'Brien, Cyber Security Executive, Telstra*

# Prepare now, recover faster later.

It's worth reinforcing one key point as your business begins securing itself against the threat of a security incident: prevention goes a long way.

You'll be much better prepared to handle the fallout of an attack if you're proactive – not reactive – in how you think about online security.

You might think you can handle a breach when it happens, but Samantha Zammit, Microsoft's SMB Modern Workplace Lead, reminds us that the effects happen fast: "Ransomware attacks can spread across an organisation in less than an hour from initial infiltration. Reaction to threats needs to be in minutes, not hours or days, to limit risk of potential damage."



**"Ransomware attacks can spread across an organisation in less than an hour from initial infiltration. Reaction to threats needs to be in minutes, not hours or days to limit risk of potential damage."**


*Samatha Zammit,  
SMB Modern Workplace Lead, Microsoft*


The time and money required to recover from an incident can't be overstated, nor can the wide-ranging impacts that can affect your business continuity, financial stability, reputation and levels of customer trust. These things often can't be mitigated, no matter how much you spend on your recovery efforts.

This is why it's important to build your knowledge to simplify what's becoming an increasingly complicated space. With that awareness, you can engage confidently with the right partners and suppliers to come up with a holistic, proactive security plan that evolves as your business needs do.

## It happened to us: Cleaning & maintenance service provider.

A cleaning and maintenance business,  
predominantly servicing the construction industry.

 Founded: 2019

 Number of employees: 18

We have featured this business anonymously to protect its privacy.



When Henry's\* business was just getting off the ground and into an efficient operating rhythm, it suffered an online attack. The business is a side project to his full-time job in data science, so Henry was managing most of the basic website build and maintenance himself, and the server was hacked after he had been working in the backend of the website and left it unsecured by mistake. "Someone cracked one of the passwords on either our app or website."

Customers couldn't view his services or make a booking online, so Henry had to manually manage bookings and delegate tasks to his team by phone. He describes this period as exhausting and stressful, a feeling only amplified by the knowledge that the criminal could access his customers' data. Not only was his business's bottom line and reputation at stake, so was the safety and privacy of his customers.

The business advertises on multiple channels and the ads were not paused during this period, meaning some of its marketing budget was wasted. The business faced reputational damage as bookings were disrupted and the website displayed an error page, likely deterring any new visitors. The total forced downtime from the event was two days, until Henry hired an expert to fix the situation.

His advice to other businesses is to hire an expert from the get-go. "If we had the right online security measures in place, we may not have had a breach," says Henry. "You can't know everything, so having an expert that knows your business can prevent avoidable mistakes. A consistent approach towards cyber security is key."

**"If we had the right  
online security  
measures in place,  
we may not have had  
a breach."**

*Henry\*, owner,  
cleaning and maintenance  
service provider*

\*Not his real name.

## Your checklist for handling an incident.

### Start planning who to tell and what to say.

- Create a clear incident plan in case anything goes wrong. This should cover your plans for response, recovery and communication.
- Do you have templates or plans in place for communicating with customers? Consider loyalty offers to earn back their trust or secure future business.

### Check your network of partners and experts.

- Familiarise yourself with who to tell and what to do if a breach occurs. Are the partners and suppliers you've enlisted for support prepared to respond as soon as something goes wrong?

### Make sure you're covered.

- Consider cyber security insurance if you don't have it.
- If you already have it, check the scope of your insurance. Does it cover you in the event of a loss from cyber attack? Some plans will not cover you if you're seen to have not done everything you can to help protect against an attack. All the more reason to enlist experienced partners today.

## Ready to prepare your recovery plan?

If your business is attacked, Telstra can help you manage the situation and put measures in place to prevent it happening again.

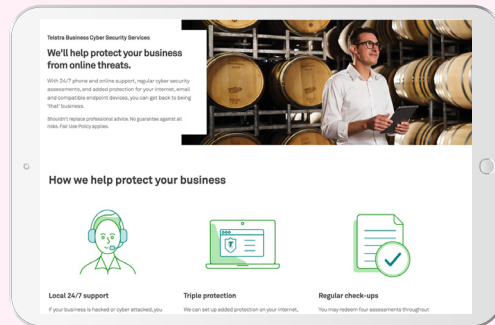
Discover how [Telstra Business Cyber Security Services](#) can help.

# Cyber Security resources.

## Need help securing your business's online assets?

Ensure your website, communications and storage solutions are as secure as possible in the event of an incident.

[Telstra's Business Cyber Security Services team can help.](#)





## Appendix.

### Who is this report series for?

Telstra Business Intelligence is for all businesses with under 100 employees – from qualified tradies and entrepreneurial sole traders to businesses with multiple staff. It's even for larger SMBs that operate from multiple premises, manage remote employees or have teams of people out on the road.

While businesses differ, their customers have more in common – particularly when it comes to how technology is changing their behaviours and expectations.

This report series is especially for businesses that may be holding back on investing in technology due to limited resources or because they're not aware of what their customers want. It's also for those businesses that want to make the most of the opportunities that technology presents to increase productivity or grow their business.

---

### Methodology.

Telstra Business Intelligence draws on both quantitative and qualitative research.

- **The core quantitative research** – Telstra Business Intelligence Study – was commissioned by Telstra and undertaken by independent research agency Picnic Customer Intelligence via online surveys in November 2019 with a sample of 1,000 consumers (aged 18 years and over) and 1,000 businesses with <100 employees. Quotas were used to ensure the sample was representative of the market. Fieldwork was conducted from 27 November 2019 to 11 December 2019.
- **Additional quantitative research**, commissioned by Telstra, was conducted by Picnic Customer Intelligence and Potentiate between 18 and 29 June 2020 (following national COVID-19 lockdowns) with n=383 Small Business owners decision-makers and n=1707 consumer household decision-makers.
- **Qualitative research** took place with a range of small business owners, industry experts and consumers from January 2020 to November 2020.
- **We've also drawn on other research studies** published in 2020 to illustrate specific areas where consumer and SMB attitudes and behaviours have been impacted by events during the year. This includes research from Venture Insights, the Australian Cyber Security Centre, and Verizon.

## Definitions.

In the context of our research and this report:

- A 'small business' is defined as having 1-19 employees. A 'medium business' is defined as having 20-99 employees. 'SMB' groups together small and medium businesses per the above definitions.
- Technology encompasses everything from the internet and telephone, to hardware devices (including mobiles and desktops) and software. In the context of the Telstra Business Intelligence report series, we place emphasis on technology that is used to connected people – be it businesses, customers or employees.
- Consumer or customer is used to describe both existing and potential customers as well as consumers in general.

---

## Acknowledgements.

We would like to acknowledge the tremendous contribution made to Telstra Business Intelligence by a number of organisations and individuals.

### Subject matter experts:

- Gary Gardiner, Head of Security Engineering, APAC at Check Point
- Julie Inman Grant, eSafety Commissioner
- Keyur Desai, Principal Security Architect, APAC at Microland
- Samantha Zammit, SMB Modern Workplace Lead at Microsoft
- Matthew O'Brien, Cyber Security Executive at Telstra
- Cynthia Wong, Cyber Security Product Owner Principal at Telstra
- Suzi Dyke, Senior Security Specialist at Telstra
- Anita Batistic, Partner Manager, Professional Services at Telstra
- Darren Pauli, Senior Project Specialist/Threat Research at Telstra
- Brooke Pengelly, Sales Leader of Small Business at Trend Micro
- Moises Sanabria, Head of Identity Security Operations Centre and Business Development Manager at IDCARE
- The team at Cisco Systems

### Business owners:

- Tom Martin, owner, Water Tight Canberra
- John Drill, founder, myAutonomy
- The anonymous business owners who shared their experiences around cyber security with us
- Telstra's Customer Research & Insights team – SMB Insights lead, Nikki Murrell
- Matt Howley and Raymond Lo from Picnic Customer Intelligence, a research consultancy dedicated to helping businesses make the smartest, 'most right' decisions. Picnic was the research partner engaged in helping design and develop the core studies that supported this report.
- Melissa Riley and Helen Barnes from Potentiate, our research partner, for fieldwork services for quantitative research in June 2020 to support this report
- Michelle Dekkers, Katherine Kennedy and Hayley Spring, Telstra Marketing and Product Leads

All of the wonderful consumers and small and medium business owners who contributed their time so generously to be interviewed or participate in our surveys.

Thank you for reading the third report in the Telstra Business Intelligence series. We hope it's been valuable. Head to our [hub page](#) for more insights, expert advice and best-in-class case studies from this series.

