CYBER SECURITY: WHAT EVERY SMALL BUSINESS OWNER NEEDS TO KNOW

smartcompany

BROUGHT TO YOU BY BizCover

Introduction

Your information is a target, whether you believe it or not.

Too many small businesses believe a lie, that because they're so small hackers will prioritise larger businesses. Unfortunately, that's far from the truth.

Instead, here's the reality: if you hold any information about your customers in a server, you're just as big a target as the big end of town. The size of your turnover matters less than the information you hold.

The global controversy surrounding Facebook and Cambridge Analytica can blind us to where most attacks are taking place: on a small scale. Businesses with only one or a handful of employees, and small scale in turnover.

Yet, smaller businesses are less likely to instil a culture of safety in their organisations, ignoring things like training on how employees can report phishing emails, or even basics like robust password security.

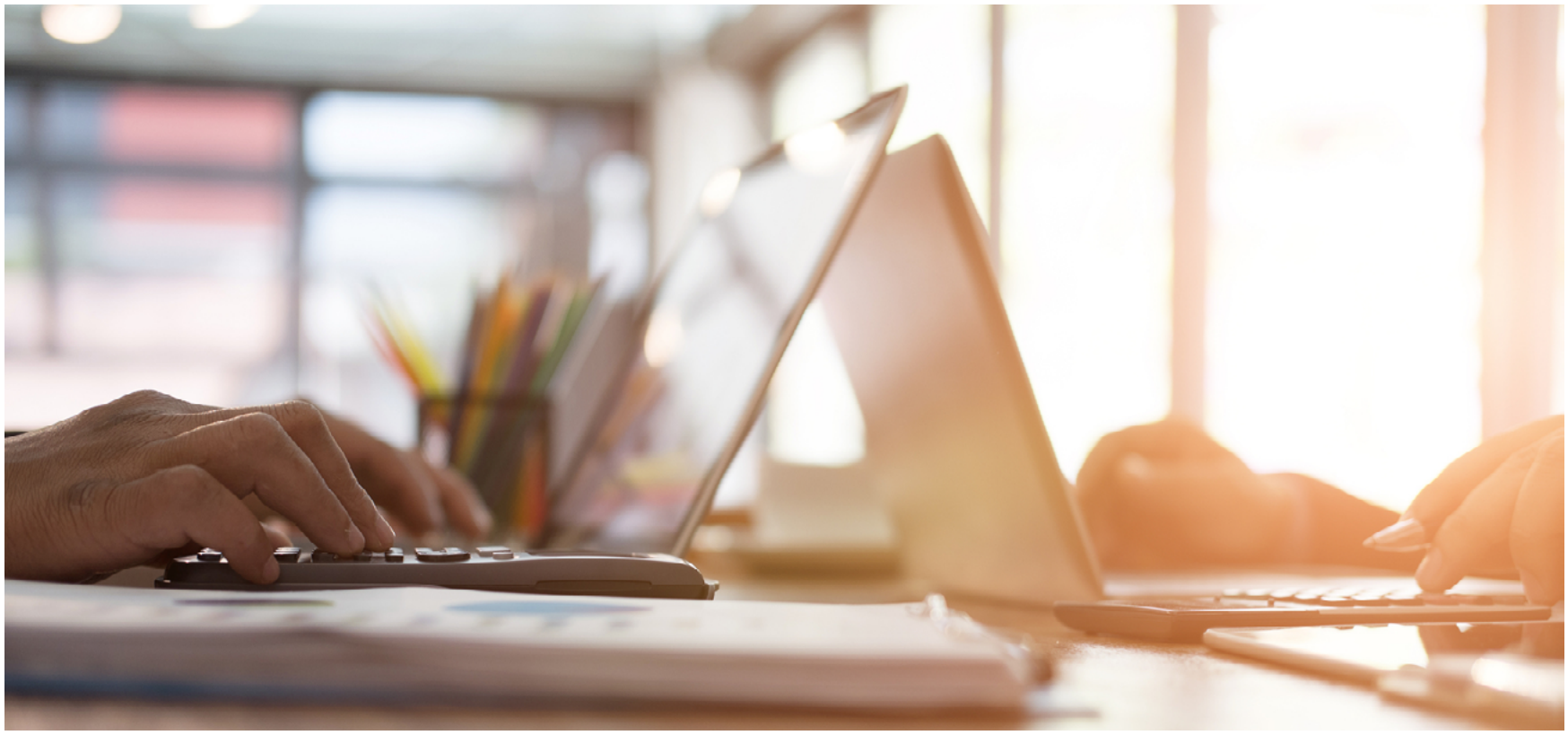
So what can you do?

That's what this ebook is for. We've compiled and curated advice from the nation's leading experts, analysts and even victims of cyber crime to give you a detailed plan on how to protect yourselves, including:

- how to identify common cyber attacks;
- how to protect the personal identifiable information in your business;
- strategies to create a culture of protection inside your business;
- methods to mitigate the financial loss of any cyber crimes; and
- what the impact of major cyber crimes – like the Facebook-Cambridge Analytica scandal – has for your business, and more.

You can't change the fact your business may be attacked. But you can protect yourself. This ebook will show you how.

Zoe Dattner, Publisher, SmartCompany



The common cyber crime threat

It is important to understand just how prolific cyber crimes are at the lower level of business.

According to the ACCC, business scams – including hacking attempts – were up by 30% during 2017. Not only that, but 6% of small businesses targeted by attacks said they paid out an average of $10,000 to those who held their computers ransom.

Overall, cyber crime costs Australian businesses more than $1 billion every year. But not every attack is equal. Look at the average cost of each type of attack, according to research compiled by the Federal Government:

- Denial of service: $180,458
- Web-based attacks: $79,380
- Malicious insider: $177,834
- Malicious code: $105,223
- Phishing and social engineering: $23,209
- Malware: $458
- Stolen devices: $13,044.

The worst statistic? Six out of 10 attacks targeted a small business. And while there are many types of attacks, experts point to three specific variations SMEs should be concerned about:

Dictionary of different cyber attacks

Malware
Malicious software installed on a computer that can track activities, including keystrokes.

Ransomware
Software that "locks" a computer and information from being accessed. Hackers use this to exploit money from users, with the promise of "unlocking" the computer once the ransom has been paid.

Phishing
Malicious emails sent to users under the guise of a legitimate email, with the purpose of stealing personal information.

Denial of service
Also known as a DDOS attack, these flood sites with artificial traffic to take them offline.

1. Ransomware;
2. Phishing; and
3. Malware.

The growing seriousness of these attacks is highlighted by their sophistication: experts say they're now becoming more difficult for even seasoned experts to identify.

Email scams are becoming more sophisticated

David Markus, chief executive and co-founder of IT services group, Combo, says the types of phishing attacks that usually target SMEs are becoming so sophisticated that identifying them is a significant challenge.

"These look like emails from friends and can genuinely be from them too. We're seeing malware bombs from things your friends send you, that look like genuine emails," he says.

"And in many cases, it literally comes from them because they've been hacked. They're not just the spoof of an email address."

One survey of cyber security professionals found 76% said their organisations fell victim to phishing attacks. Experts agree these emails are becoming much harder to differentiate, using sophisticated logos, high-quality graphics and authentic-sounding language to "blend in" among everyday communications.

Mandatory reporting laws

The Australian Government passed extensive mandatory disclosure laws relating to privacy breaches in February 2018.

Here's the low-down: if you earn less than $3 million a year, you're exempt, unless you handle personal information (for example, finance brokers, accountants and health providers). But anyone else needs to report a privacy breach to the Office of the Privacy Commissioner where the breach is likely to result in serious harm to affected individuals.

So, if you're above that threshold and haven't created some governance around your reporting mechanisms, then now is the time.

Personal information is defined by the Office of the Australian Information Commissioner (OAIC) as "information or an opinion that identifies or could reasonably identify an individual, whether true or not, and whether recorded in a material form or not". This includes things such as name, address, telephone number, tax file number etc.

One growing threat involves hackers breaking into an email address, then sending out emails to various contacts inviting them to download a file, usually accompanied by an inconspicuous message.

Because the hacker has access to the email address, any replies can be intercepted – and hackers often reply pretending to be the person whose account they've hijacked.

Once the file is downloaded – or a password is entered – the hackers now have access to another email, or can install ransomware.

"We see emails that might look as though they're from an executive, and they say things like, 'can you please pay this invoice?' to make it look like a normal part of everyday business," says Murray Goldschmidt, chief operating officer at Sense of Security.

David Markus says this has created a difficult situation where users can't necessarily trust a communication over email regarding a suspicious message.

"It's getting to the point now where you literally need to call your friend on the phone and confirm that something they sent has actually come from them," says Markus.

Ultimately, phishing is just a tool. What usually happens next can be much worse...

Ransomware targeting small business for Bitcoin

Jacques Jacobs is a partner at Norton Rose Fullbright, an international law firm, and works consistently with businesses which have been affected by cyber crime. Most of his clients, he says, are small-scale operations with only a handful of employees.

"This week I had one which was a suburban auto parts seller," he says. "They've got two shops, both computers are connected and it looks like someone has hacked in. There's a lock and they're now being asked for money."

"These attacks are often high frequency, because the ransoms they demand are not that high – I had one recently that was $7,000."

"They're not huge amounts, but cause significant disruption for a small business owner."

There has been a rise in these types of ransomware attacks. The WannaCry virus is perhaps one of the most well-known, after spreading through the internet in the first half of 2017. The attack struck governments along with organisations, including the British National Health Service. The virus locked computers, with a message to pay the perpetrators to unlock it.

Altogether, WannaCry hit 200,000 computers across 150 countries, but it's only one type of ransomware. As Charmaine Moldrich, CEO of the Outdoor Media Association (OMA), knows all too well, ransomware can hit smaller organisations at any time.

Last year, the OMA was struck with an attack and ultimately paid more than $25,000 to both unlock the attack, and to upgrade its IT infrastructure. But as Moldrich says, it wasn't an easy decision in the slightest.

"It's a pragmatic decision. There were ethical and moral issues that I recognised, and I didn't necessarily want to pay, but in the end, I'm running a business and you have to make decisions based around the best outcome of the business itself."

It is generally not recommend that a business pay ransoms as there is no guarantee the information will be released by the perpetrator or cease more ransom demands in future. Always speak to your insurer in relation to any ransom demands.

Easy targets

Murray Goldschmidt from Sense of Security says businesses need to realise that these attacks will continue perpetually, not because they are necessarily effective on a wide-scale, but because they are monetarily cheap to produce.

Ultimately, that means businesses need to get used to the idea of these types of attacks.

"You send someone an email, the download goes nowhere and it encrypts their computer...the cost is nothing. But the yield is high for the attacker," he says.

"We see this as being persistent."

What were the WannaCry and Petya attacks?

The WannaCry virus was a ransomware attack that struck more than 200,000 computers around the world, including government departments in Britain and the United States.

Another virus, Petya, infected Australian companies including Cadbury. Although not reported officially, it's believed that several Australian small businesses were infected as well.

Shocking cyber crime statistics

- Almost two out of three SME owners feel well-informed about cyber crime, and 80% feel they can respond to a security breach.
- Howvere, less than 30% of SMEs report suffering a cyber crime event.
- 75% say they are influenced by their own experience, rather than by an expert.
- Cyber crime costs Australians $300 million every year.

Source: *Cyber Scare: A look at small to medium-sized business and the emergence of cybercrime in Austalia*.

Arming yourself against potential loss

Imagine this: you're on a well-earned holiday from your business after years of hard work. After a few days of relaxing and taking in some sights, you get a call from your general manager – who you specifically told not to call unless there was an emergency.

"We've been hit by a cyber attack. Everything is gone," they tell you.

Sounds like a nightmare scenario. But according to Jacque Jacobs, this happens. In fact, it happened to a client of his just recently.

"This is a mum and dad operation, they were on holiday and got a call from their IT contractor. They had to ask them, 'what do we do?'"

"Thankfully they had (cyber) insurance, we were able to work with them straight away and sort it out. But they don't necessarily have the luxury of time."

For so many small businesses, relying on digital devices and networks to get the job done is a day of life. But as the Federal Government's own research has shown, even small downtimes or disruptions through DDOS or ransomware attacks can have huge ramifications.

Imagine if your entire system was disrupted, and you hadn't stored your backups for the past few months? What about the past year?

Charmaine Moldrich experienced that very dilemma when ransomware blocked her organisation's systems. Not only did the business not have the usual backups their IT contractor had promised – another reason to make IT a top priority – but given the number of people in the organisation, it meant the ransomware could erase up to a year's worth of work.

"All of these issues were human issues. We simply weren't talking about it in our WIPs, in our senior management meetings."

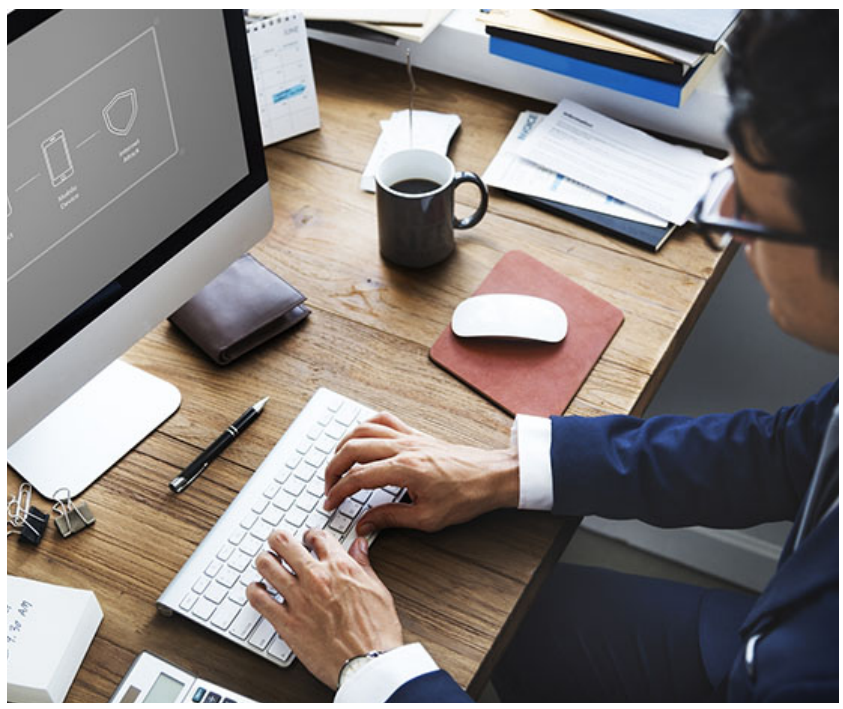
"It was never talked about unless something was broken as we didn't have a dedicated IT person on our team."

It is important to realise that cyber crime can hit any type of business. Even though these organisations mentioned may be professional, office-based businesses, just look at how many attacks businesses have suffered in a variety of industries:

- Retailers are regularly targeted, particularly within their point-of-sale infrastructure. Malware can infect systems to scrape credit card data. In 2013, the malware StarDust infected systems across the United States to compromise more than 20,000 cards.
- More than 75% of US healthcare providers have been hit by cyber attacks, according to *Scientific American*. Healthcare records are unusually expensive on the black market due to the personal data they contain, which can be combined with other records to create a more detailed profile.
- Manufacturing businesses are becoming a larger target, partly due to the fact many smaller businesses in this sector have not implemented a lot of cyber security on their own. This industry contains quite a lot of intellectual property and data related to government contracts. Attacks rose 24% in the second quarter of 2017.

It is clear cyber crime affects all businesses in all industries. Given the perpetual state of attack...what can SMEs actually do?

As it turns out, quite a lot.



Will your *small business* ***be the next?***

Don’t let the cost of a cyber breach destroy your business.

Protect it with ***Cyber Liability Insurance*** *today.*

Broad protection for small businesses

- ✓ Loss of 3rd party data and breach of privacy
- ✓ Business interruption loss
- ✓ Credit monitoring costs
- ✓ Cyber extortion costs
- ✓ Forensic costs
- ✓ Legal representation expenses
- ✓ Notification costs
- ✓ Fines and investigations
- ✓ Public relation costs

DID YOU KNOW?

Small businesses are the target of **43% of all cyber crimes in Australia**

Ready to compare? Get **FREE** online quotes

bizcover.com.au **1300 849 072**

BizCover

Six different steps SMEs can take to protect themselves from cyber attacks

1. Understand the data you actually have

Collecting information is a normal part of doing business. But as *Harvard Business Review* points out, too many businesses don't understand what data they actually have, and don't have a data-driven culture.

Customer data is one thing, but do you have product telemetry? (Product telemetry is information about what people are actually doing within your product.) What about intellectual property from business clients? Do you have credit card data?

Cisco chief privacy officer Michelle Dennedy once said that "understanding the information your company collects is the first step in respecting your customers' privacy". Once you know what you're dealing with you can make better steps to protect it.

2. Understand your backup protocols and put them in place

One of the biggest fears a business can have is when historical work is deleted. Not only do you have to start from scratch, but you may lose out on financial records. There could be money you need to chase up but have no record of.

Facing more than a year's worth of data being deleted, Charmaine Moldrich put a backup system into place as soon as the initial cyber attack was dealt with.

"Since then we've made backups a priority, we now have a log of them being done automatically, the updates are done in the middle of the night so they don't depend on humans."

"We also put IT on the agenda for all our meetings," she says.

But just having backups isn't enough, David Markus says. SMEs need multiple backups, with at least one held on a different server or not on the same network. (Merely having a backup won't help if that same backup is held on the computer blocked by ransomware.)

"You should really already have your backup plan in place right now," he says.

Jacque Jacobs sounds a warning: "We've had examples where the backup is on a connected USB or hard drive, and that also got infected. The options to recover were limited."

3. Understand what you need to do to protect your systems

As these experts point out, all too often business owners take an arm's length view of what's happening with their IT system.

But as Charmaine Moldrich says, that is exactly the problem that led to their disaster in the first place. No one knew what was happening until there was a problem.

"Somehow it had fallen between the cracks," she says.

"We had identified the issues, but there was nothing being followed up. We weren't talking about this at WIPs, and we didn't have a dedicated IT person at our meetings," she says. "We ended up changing our IT provider, because there were communications issues."

SME owners should be clear about this: backups need to happen regularly, there needs to be clear communication between yourself and whoever manages your IT (even if that is you), and IT security needs to be a point of discussion in regular meetings and updates.

4. Do you have a culture of protection within your workplace? Are people likely to recognise attacks?

Given phishing attacks are becoming more sophisticated, it makes complete sense that most people don't know how to identify them.

It only takes one unsuspecting employee to infect an entire network. That's why creating a culture of security within your organisation is so crucial – to train people so they are sceptical, they know how to report suspicious material, and they understand the ramifications of their actions.

Here are just a few things our panel of experts recommend you should do within your business:

1. Train staff so they understand how to recognise phishing emails. For example, always check the email address from which the message was delivered, check for small details on logos or graphics for mistakes.
2. If you do receive a phishing email, do not respond or click on any of the links or attachments in the email. If unsure, forward the email to your IT service provider to confirm or delete the email. You can also block the sender so as not to receive any further emails from the sender.
3. Never be afraid to tell someone about a phishing email, even if you have unexpectedly fallen victim to it. There should not be a culture of blame if these things occur, as this will stop other employees from speaking out.
4. Regularly change passwords – have your IT department force this on your employees – and use two-factor authentication if possible. Also consider rules such as not leaving workspaces unattended.
5. Make sure your employees understand the financial ramifications of any ransomware attack. Align your security goals to the goals of the business to create context.

5. Take out cyber liability insurance

Taking out cyber liability insurance will provide financial protection if your business was to suffer a cyberattack, by covering the expenses and legal costs associated with the data breaches, hacking or from theft of client information.

The insurance will cover the costs of the business interruption suffered by your business as well as forensic investigation, data recovery, extortion and any crisis management costs to help your business reputation after a data breach from a cyberattack.

The policy also covers the financially crippling costs of defending yourself, mandatory notification costs and other associated legal costs.

6. What is your reporting plan?

Many businesses may not know that mandatory disclosure laws now require companies to report cyber security breaches to the office of the Privacy Commissioner, where there is a risk of serious harm to the individual and where the company's turnover is more than $3 million, or you handle personal information.

But even though companies may not be forced to disclose those breaches, David Markus says businesses ought to have a reporting plan in place even for their own customers.

"If you're not ready for that, you're going to have a PR disaster."

What do you do if your business falls victim to a cyber scam?

All the preparation in the world can only go so far. As thousands of Australian SMEs can testify, a cyber crime or scam can leave you crippled, confused and decidedly out of pocket.

But if you do suffer an attack, how should you respond? While there is no set formula, these experts generally recommend a set of actions that will help you identify what needs to be done, and what can mitigate the harm your company suffers.

This set of actions will obviously need to differ based on what cyber scam or attack is involved, but generally the experts agree on this set of circumstances:

If you are ordered to do anything by the attacker, don't – at least not immediately

Ransomware attacks usually threaten to delete data if a ransom isn't paid, and increasingly that ransom is being demanded in Bitcoin.

This can be a tough decision. But Jacque Jacobs says on the face of it, paying up can be an easy solution – but not necessarily the right one.

"Our experience so far is that it is by no means guaranteed you're going to get some or all of your data back. And it potentially increases your risk of being targeted again," he says.

Contact an expert

It is imperative that any business suffering a breach doesn't try to go beyond their expertise. Forensic experts exist for a reason, and our panel recommends getting in contact with one as soon as possible.

"If you don't have the skills to identify what's going on, that's where you should use an IT service provider specialising in that space," says Murray Goldschmidt.

Jacque Jacobs also points out that this is where cyber liability insurance can be a benefit.

"Cyber insurers usually have a rapid response team who can help you with any breach that may have occurred," he says.

Understand the nature of the breach, and start restoring from backups

Understanding what has been targeted is the first step in knowing how to respond. If any cyber attack has touched customer data, you need to know that straight away so you can inform them. However, if the only data being disrupted is non-personal information, that changes the nature of your response.

This is not an easy process, and for some businesses can last weeks or months. This is why it is important to develop some governance around an investigation before it occurs: who is involved? What powers do they have? Who can review what data has been breached, and why?

Having those tasks designated beforehand will make any investigation smoother. (Working with forensic experts, including insurance rapid response teams, can also help.)

"It's really like a crime scene. You want to make sure you're not disturbing any evidence in terms of how things happened, but at the same time you need to stop whatever occurred," says Jacque Jacobs.

"You need to know the best way to handle the information, if the data has been lost, if someone has seen it, and so on."

Put your reporting plan into action

This is where the latest mandatory disclosure laws come into effect.

If your business turns over more than $3 million and suffers a data breach that is likely to result in serious harm to any person whose personal information is involved, you are obliged to report this to the Office of the Australian Information Commissioner. Not doing so can result in fines, so having that governance in place is crucial.

But even if you don't reach that threshold, it's still crucial you announce this to your customers. Not doing so could result in a worse reaction later, as David Markus points out:

"When something has been breached, find out who's been hit, notify them straight away, then notify the government. If you don't have a plan in place, you're going to be left wondering what you should be doing when it happens – and any effects will be amplified."

The final word

It is important to remember these attacks are not going away. They will only change their shape and form. As Murray Goldschmidt points out, even the Facebook-Cambridge Analytica scandal highlights just how much businesses need to be aware of the information they're putting out there:

"This is an issue for consumers, but also for corporations who are putting data into Facebook and using its analytics," he says. "It basically relates to any entity who collects personal information and mines that information for business purposes."

As for what you can do now? Jacque Jacobs says if nothing else, start drawing up a plan for if a breach occurs then run it once a year – just like a fire drill.

Also ensure your business is protected with cyber liability insurance, to help you cover the costs associated with a data breach or being hacked.

If nothing happens, you'll have wasted little time. If something does? Well, you'll be glad you were prepared.

"You need a plan. But if you don't test that type of plan? It's worth nothing."