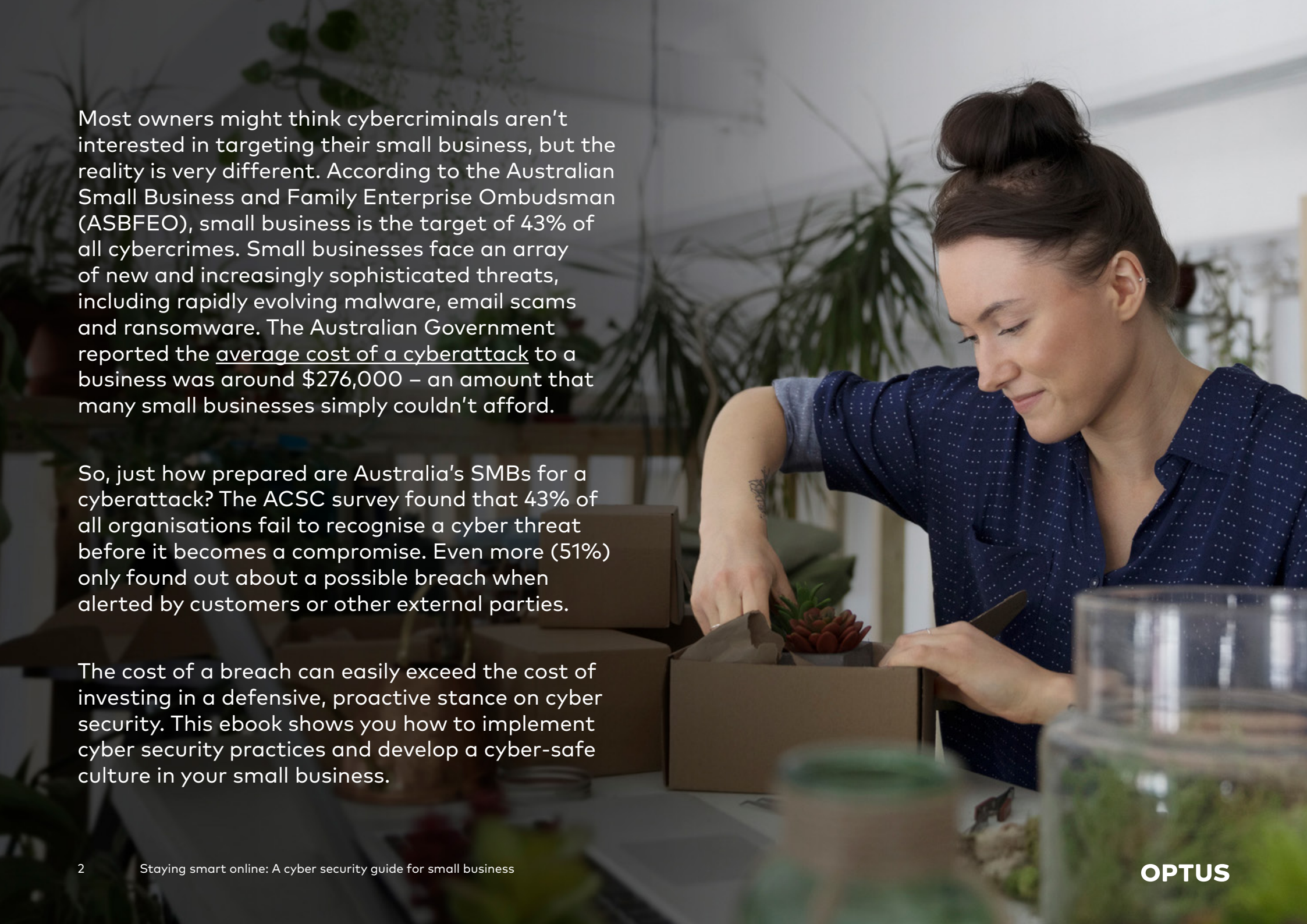


A small business guide to effective cyber security





Most owners might think cybercriminals aren't interested in targeting their small business, but the reality is very different. According to the Australian Small Business and Family Enterprise Ombudsman (ASBFEO), small business is the target of 43% of all cybercrimes. Small businesses face an array of new and increasingly sophisticated threats, including rapidly evolving malware, email scams and ransomware. The Australian Government reported the average cost of a cyberattack to a business was around \$276,000 – an amount that many small businesses simply couldn't afford.

So, just how prepared are Australia's SMBs for a cyberattack? The ACSC survey found that 43% of all organisations fail to recognise a cyber threat before it becomes a compromise. Even more (51%) only found out about a possible breach when alerted by customers or other external parties.

The cost of a breach can easily exceed the cost of investing in a defensive, proactive stance on cyber security. This ebook shows you how to implement cyber security practices and develop a cyber-safe culture in your small business.

Cyber security: The reality for small business

When it comes to cyber security, your business is never too small to be targeted by hackers. How exposed are you?



43%

of all cybercrimes target small business, according to the [Australian Small Business and Family Enterprise Ombudsman \(ASBFE0\)](#).

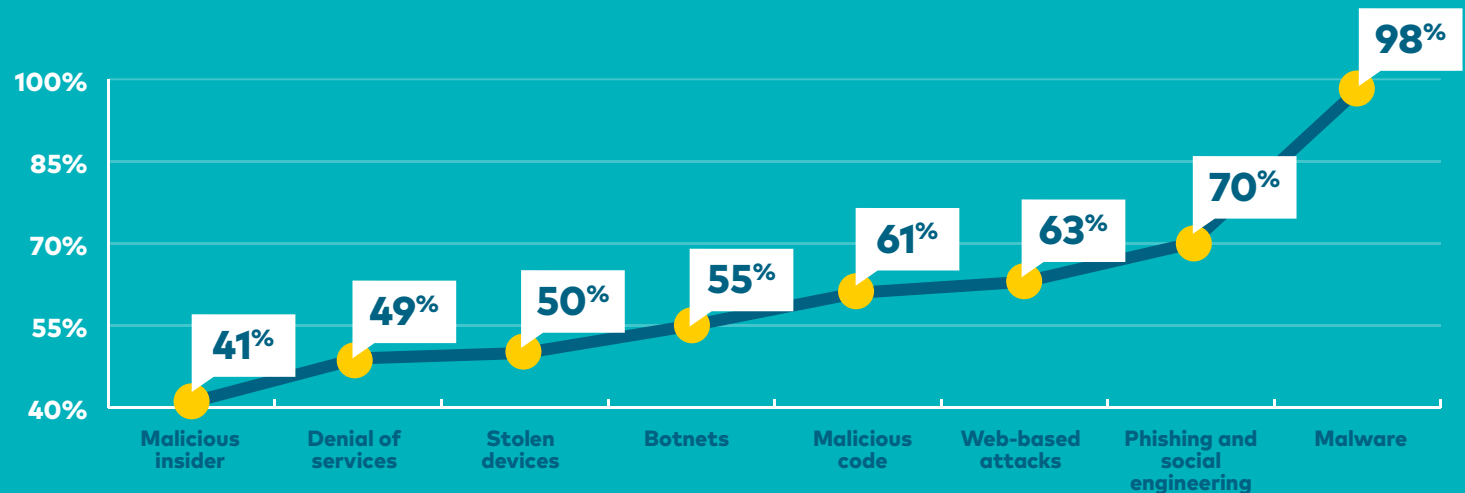


60%

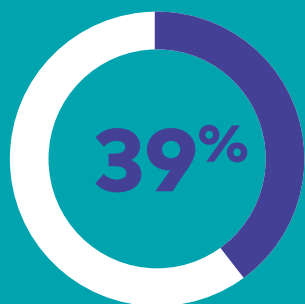
of these businesses who experienced a significant breach went out of business in the next six months.

SMBs operate in a landscape of new and increasingly sophisticated threats

The top types of cyberattack experienced by [benchmarked organisations](#) in 2016 were:



The largest cost impact from cybercrime is:



Information loss



Business disruption



\$276,323

Average cost of a cybercrime attack

The best cyber security is preventative

According to the 2017 Ponemon Cost of Cybercrime study, the **cyber security strategies with the biggest return** on investment were:

67%



Security intelligence systems

63%



Advanced identity & access governance

In 2016, the Australian Cyber Security Centre (ACSC) found that among Australian organisations:

43%



don't recognise a cyber threat until it's too late

51%



don't usually find out about a breach until alerted to it by an external party

New Australian data breach disclosure laws apply to Australian businesses from 22 February 2018. SMBs with an annual turnover of \$3 million or more **must notify affected individuals** of a data breach or face stiff penalties.



How prepared are you?

Chapter 1.

Knowing the risks:

How vulnerable is

your business?

According to the [ASBFEO](#), 87% of small businesses believe antivirus software alone keeps their business safe from cyberattacks. This is in stark contrast with the reality. In fact, the [ACSC survey](#) found that 90% of Australian organisations were targeted in some way by hackers during the 2015–16 financial year, sometimes up to hundreds of times a day.

To mitigate the risks effectively, you'll need an accurate picture of your company's security vulnerabilities. This can be found through a formal cyber security assessment. The ACSC looked at the most cyber-resilient organisations, and found that the five most valuable steps in a cyber security evaluation are:

1. Active technical testing

Also called a penetration test, this is a simulated attack on the company's network to evaluate its security measures. It can include computers, mobile devices, printers and other network endpoints.

2. Expert advice and support

A specialist advisor or consultant can review the business's cyber security requirements, advise on the best solutions to overcome a cyberattack and help formulate preventative measures.

3. Senior management feedback

The view from the top is an important part of any cyber security evaluation. What would a serious cyber-incident cost the organisation? Who would benefit? Does the business have a strong security culture?

4. Compliance auditing

Is the business's compliance to cyber security regulations monitored on an ongoing basis? Are corrective actions documented and followed through?

5. Staff awareness

What security training do employees have access to and is it effective? Are they educated on the different types of cyberattacks committed, mobile device security and appropriate use of social media?

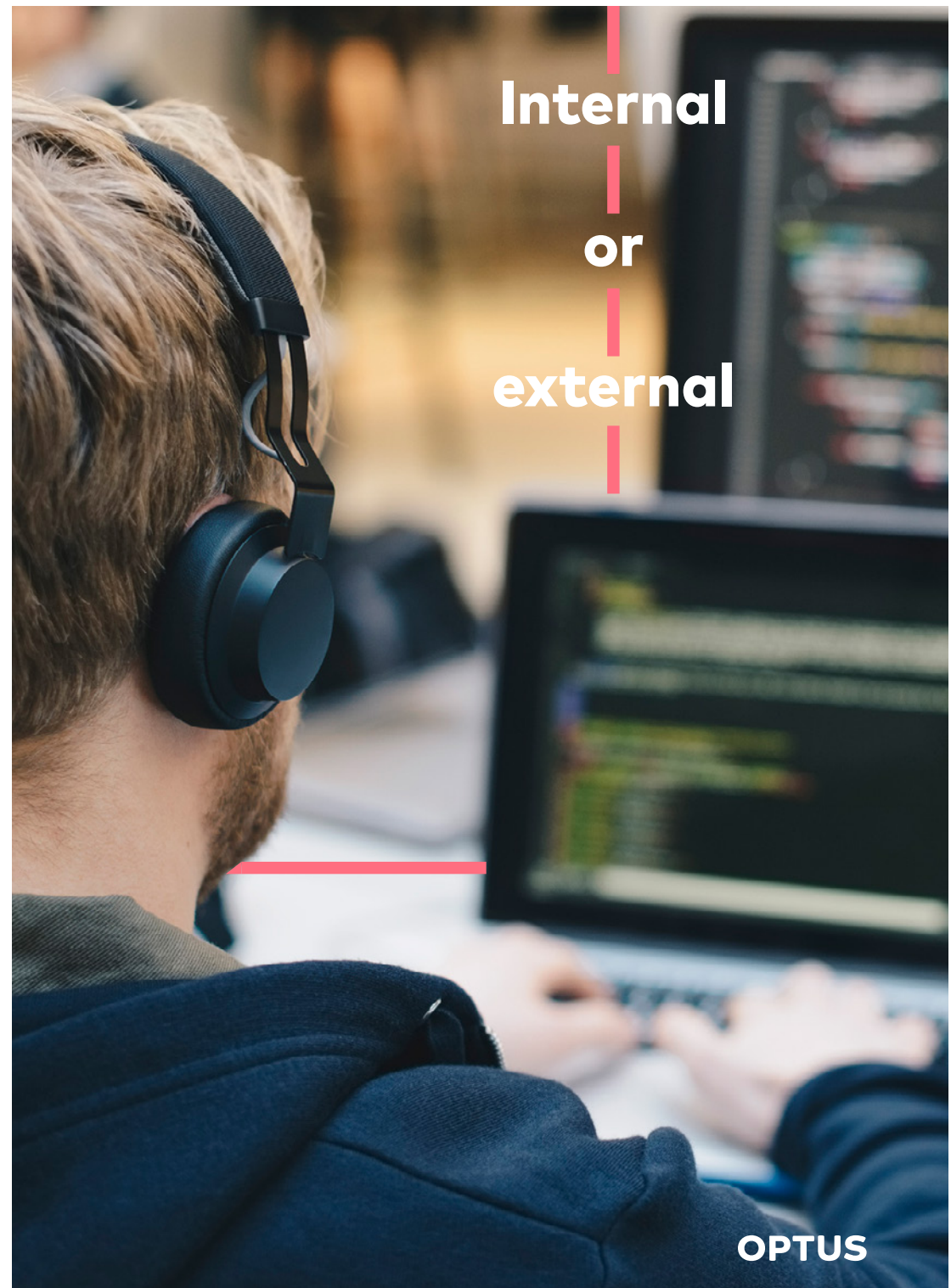
Chapter 2.

Recognising an attack: The most common cyber security threats

There are a number of malicious operators around the world attempting to steal information to profit and to disrupt businesses and governments. If they're trying to hack into your business, they're likely to draw on a known arsenal of attacks that have proven to be highly effective. These attacks can be instigated in two ways: by individuals inside the company, or by external agents.

Here's an overview of the most common threats affecting small businesses.

**Internal
or
external**



Insider threats

According to the [October 2016 HP/Ponemon Cost of Cyber Crime Study](#), 41% of companies surveyed had been attacked or breached from the inside – an increase of 6% on the previous year. The most common types of internal breach are:

- **Social posting:** An employee revealing confidential information on a social networking site
- **Data theft:** An employee stealing data on a device such as a USB key or leaking information to competitors
- **Unintentional breaches:** An accidental loss of a laptop or mobile device or an employee distributing confidential data unintentionally

External threats

Hackers will go to great lengths to breach an organisation's cyber defences. Their methods could be in the form of sophisticated malware, automated attack bots or attempts to trick employees into revealing information. According to the [ACSC survey](#), the most common types of external attacks include:

- **Malware or email phishing:** The use of malicious software or deceptive emails to fraudulently obtain money or carry out other illicit activity
- **Hacking attempt:** Unauthorised access to the company's network with the intention to control or damage its systems
- **Ransomware:** Hackers demanding payment (often in Bitcoin or other cryptocurrencies) in exchange for unblocking access to your data
- **Identity fraud:** In addition to targeting consumers, hackers can seize a company's identity and use it for fraudulent purchases or other illegal activities

What to do when you've been hacked

Think you've opened a dodgy email attachment? Has your computer slowed to a crawl or is it behaving strangely? If the signs point to your business's network having been compromised, you'll need to take action quickly. If you think you've been hacked, you might need to:



Reset passwords

Change all your passwords immediately. This could be a good time to add two-step authentication, such as an SMS code, to protect your most critical data.



Disconnect devices:

Isolate the affected computer or device by unplugging its network cable or disconnecting it from wireless networks.



Report the incident

Inform affected staff, customers and other stakeholders that there has been a breach.



Recover your data

Regular backups are your best insurance against damage from a hack. Daily incremental backups as well as weekly or monthly backups are always recommended.

! For a detailed run-down of how to recover from a cyberattack, download this [step-by-step checklist](#) to hang up in your office or send to your team.

Chapter 3. How to stay cyber-secure: Top security tips

Just one successful cyberattack can seriously damage your business and create financial burden for you and your customers. It can also have disastrous effects on your business's reputation.

Fortunately, there are some simple steps you can take to safeguard your business from the most common types of cyber threats. These include:

Back up regularly

Backing up your financial, business and customer data can help you recover from data loss caused by an attack. Using multiple backup methods, such as portable hard drives and encrypted cloud storage, will reduce the risk of catastrophic data loss. It's recommended you perform both incremental daily backups and full backups at the end of the week, quarter and year.

Passwords & multi-factor authentication

Use strong passwords that avoid dictionary words and use a combination of letters, numbers and symbols. Stale passwords are more likely to be compromised, so make it compulsory for staff to reset their passwords every three months. Want better protection of your data? Supplement the password with a two-factor authentication method, such as a token-generated PIN or SMS code.

Security updates, scans and patches

Operating systems, software, mobile devices and applications often get security updates from vendors, so make sure they are connected to the internet and updates are applied automatically. Remember to install virus scanners and a firewall program on your portable devices and keep them updated and patched to block threats from entering your network.

Administrative accounts and access control

Change all your default passwords and consider limiting (or disabling) administrative access to prevent an attacker from gaining access to your network. Also, make sure you restrict access to sensitive locations and resources – for example, only allowing authorised IT staff to access the server room.

Chapter 4. It starts at the top: Cyber security best practice

According to [CSO.com from IDG](#), SMBs make attractive targets because they tend to have less secure networks than big corporations. It's also become easier for hackers to carry out automated attacks on thousands of businesses simultaneously.

Leadership and culture are important factors in reducing your chances of being affected by a cyberattack. Here are five proactive cyber security strategies for small businesses.

Engage senior management

The ACSC found that companies that regularly discuss cyber security at the senior management level tended to be more cyber-secure than those that don't. Almost half of such discussions focus on how to deal with the latest cyber threats, empowering the organisation to adopt a more proactive approach to its cyber security.

Proactive cyber security strategies



Create a cyber-aware culture

Another key trait that separates cyber-resilient SMBs from cyberattack victims is the understanding that good cyber security is everyone's responsibility, not just the IT department's. Hackers are always finding new ways to access information, so it's critical to create a culture where employees are aware and understand the impact of new threats.

Educate staff and clients

Never assume that your staff and customers have enough knowledge about how to secure company and personal data. Security training can take many forms, such as a security-awareness website, helpful hints in a weekly or monthly email, visual presentations or online training sessions. More in-depth training should be provided to IT staff to help them keep abreast of the latest cyber security trends.

Prioritise actions

No single security policy or tool can fully prevent cyberattacks, so it's vital your organisation uses a range of different security controls. These will need to be prioritised to match the needs of your business. Take into consideration the type of information at risk, where it's stored in your systems, who can access it and how it's currently protected.

Invest in cyber security

In addition to being stressful and expensive, damage caused by a successful cyberattack can take a long time to repair. Making your SMB more cyber-resilient will require an allocation of time and money, but it should be weighed against the potential costs that could be incurred if a serious cyber incident affected your network.

When it comes to cyber security, humans can either be the weakest link or your best line of defence. Given that smaller businesses rarely have a lot of resources to spare, it's critical that both your employees and their managers stay up-to-date on cyber security best practice.

The most cyber-resilient organisations use a range of cyberattack prevention and incident management strategies to reduce both the risks and impacts of cybercrime. Investing in a solid baseline of cyber security will help your business avoid any unwarranted cyber intrusions.

Stay
up-to-date



OPTUS

Yes