CYBERSECURITY

TIPS FOR BUSINESS OWNERS

Small Biz
WEB SOLUTIONS

SPECIAL
REPORT
2021

CYBERSECURITY INTRODUCTION

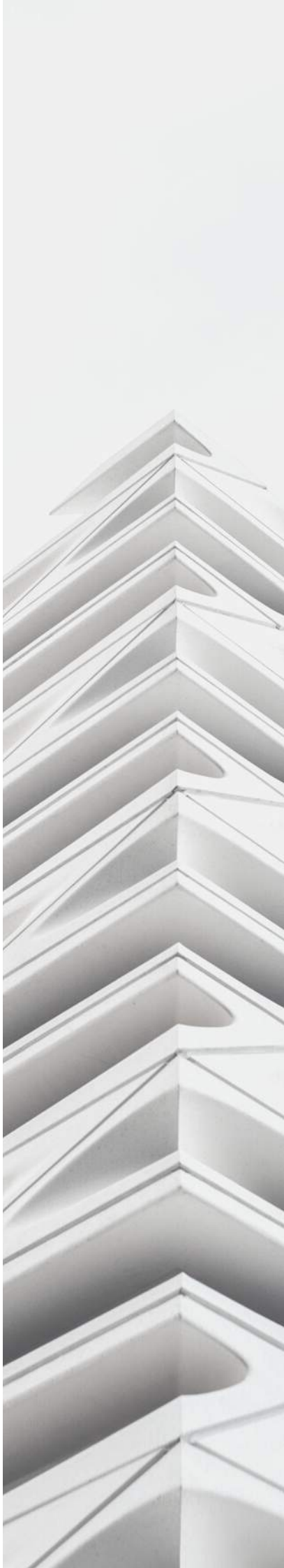
In today's increasingly digital, data-driven world, businesses of all sizes rely heavily on technology to carry out day-to-day operations and perform basic business functions. As a result of increased adoption of technology, connectivity with third-party providers and other technology-led initiatives has exposed businesses to additional cyber vulnerabilities.

For most small businesses, it is not a matter of 'if' you will be attacked but rather when you be attacked, or if you have already been attacked without realising.

Important facts

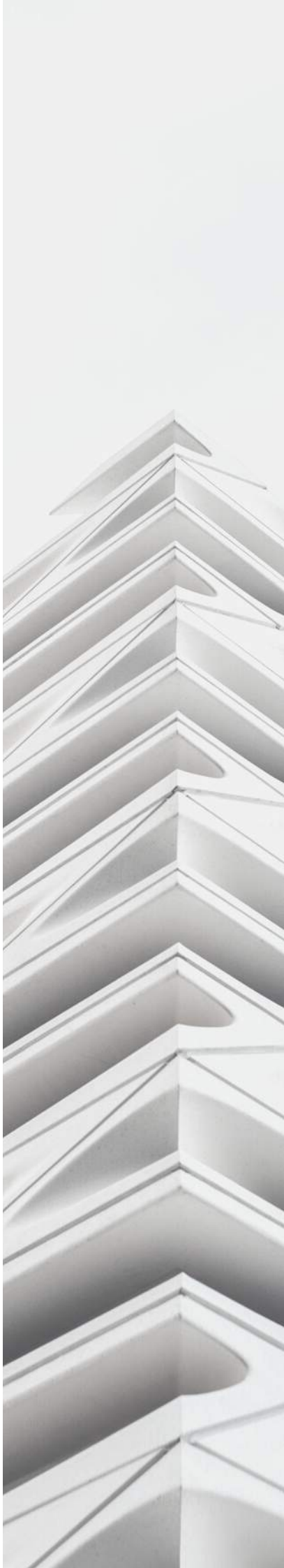
Since the pandemic began,

- the FBI reported a 300% increase in reported cybercrimes (IMC Grupo)
- ransomware attacks increased by nearly 500 per cent
- 27% of COVID-19 cyberattacks targeted banks or healthcare organisations with COVID-19 credited for a 238% rise in cyberattacks on banks in 2020 (Fintech News)
- Google blocked 18 million daily malware and phishing emails related to Coronavirus in April 2020 (Google)
- half a million Zoom user accounts were compromised and sold on a dark web forum in April 2020 (CPO Magazine).



Cyber-attacks often target client data. When client data is compromised, businesses may not only experience financial loss, but also **reputational** and **relationship damage**.

As a business it is critical that you are aware of the risk and take action to protect your customer data and your business.



Cybersecurity is more than just passwords

There are a lot of myths and misconceptions around cybersecurity which often lead to inadequate preparedness and may result in catastrophic consequences.

Here are the most common cybersecurity myths we encountered:

1. I don't have anything worth protecting
You might think your data isn't worth anything as you only keep minimal data and there is nothing sensitive about your customers. In fact, personal data is very valuable and can be used from identity theft to selling your data to marketers who build a detailed demographic of you.

2**. We have invested in security software**
Organisations commonly mistake that investing in high-end security tools and solutions can help them build an invincible shield between their networks and cybercriminals. The security tools and solutions are only fully effective if they are appropriately configured, monitored, maintained and integrated with overall security operations.

3. We should only secure internet-facing applications
Organisations must secure their internet-facing applications. But it should not be their only focus. For instance, your organisation's whole IT system may get compromised if an employee accidentally uses an infected flash drive. Therefore, organisations should have adequate controls to prevent and address insider threats.

4. We have never experienced a cyberattack, so our security is strong enough

Cyberthreats are continually growing, evolving and getting more sophisticated. Organisations need to strive to continuously improve their cybersecurity to match this threat. Unless you are monitoring your logs on a regular basis you will not know how often your systems are under attack, who is attacking them and how they are trying to break in.

Unfortunately, most small businesses will not know if their systems have been compromised until it is too late.

5. Security is the responsibility of the IT department

Undeniably, IT has a big responsibility for managing the cybersecurity of an organisation. It is not limited to them because anyone that has access to your systems plays a role. A security breach can have potential long-lasting effects on the entire business. Real cybersecurity preparedness is the responsibility of every employee.

6. Anti-virus and anti-malware software are enough to keep business safe

Anti-virus and anti-malware software is certainly imperative to keep the organisation's network and systems safe. But software won't protect your entire IT infrastructure from all cyber risks. Human error is the leading cause of security holes.

7. We'll know immediately if any of our systems are compromised

In the present digital era, it can take months or even years to realize that your cybersecurity has been compromised and your computer has been infected with malware. For instance, it took four years for hospitality giant Marriott to notice a massive data breach that disclosed the personal and financial information of their 500 million guests.

It is important to note that there no one solution and that software can only do some of the work. As a business you need to make a conscious attempt to analyse your risk and put strategies in place to prevent potentially damaging attacks on your business.

PRACTICAL STRATEGIES TO KEEP YOUR SYSTEM SAFE

Allocate money in your budget for cybersecurity

Most business owners either forget or completely disregard the need to invest in cybersecurity for their business. If you are an e-commerce, health service provider, complementary therapist, gym, weight loss clinic, childcare provider or have a site that captures visitor information, then cybersecurity is a legal function of your business.

Any business activity costs time and or money so you need to ensure that you budget this activity in your business plan, otherwise it won't get done. For example, when you buy a car you know there are ongoing expenses such a petrol and car servicing. Well, it is the same with your online services. They need to be updated and reviewed on a regular basis to ensure they work as expected. Don't think of it as a business expense but rather a necessary function of your business.

Do an audit and know your risk exposure

I am constantly amazed at the number of businesses that do not know what information they capture, hold and manage on their online systems. What's even more surprising and concerning are shared folders used without any consideration for who is likely to access these, how long they should have access, what is in the folders they share, with no plan to revoke share privileges. BTW I am not just talking about internal folders but also online folders such as Dropbox, Teams, Google Drive, etc.

If you do not know what you have or what data you are managing then you **do not know your risk exposure**.

E-commerce sites are even more exposed as each country has their own privacy laws. Depending on your target market you could be opening yourself to severe penalties if your site gets hacked and you have not taken adequate steps to protect the data you captured. For example, if your clients are from the EU then the GDPR laws come into effect. If proven guilty you can face a minimum of $200,000 EU fine for each occurrence.

Open your eyes and find out what your risk exposure is. Once you know then you can take action to protect your business.

Make sure that your systems are kept up to date

One of the most common reasons we discovered sites were hacked was because their systems were not updated since they launched. Far too often I've seen sites where they get a freelancer to build their websites, launch it and then forget about it.

There is nothing static in the universe as it either evolves or dissolves. Hardware and software is constantly evolving, i.e., enhancing, improving or fixing issues. If you do nothing to maintain your online systems, your defence will continually dissolve since hackers will find ways to break into your system using security holes in the software.

This is not just one big exercise, but a process that needs to be schedule, monitored, and costed.

Have an external person in your review/audit

While most of the work should be and will be done by your team and yourself, you will still need an external person to participate in your review/audit. We all have some level of tunnel vision due to our experience, assumptions and our perceived understanding of the solution. An external person can ask the “dumb” questions. They will question any assumptions and force you to be explicit. This will help to unearth any hidden risks that were not considered before.

The external person does not need to be an expensive consultant, rather someone who it not involved with the current system, understands systems and has a good analytical mind. However, an expert will help you to zero in on issues quicker and explore options you have not considered or are aware of.

Review your passwords policy to ensure they are strong enough and get changed regularly

Like most people, I hate passwords. They are so hard to manage especially when you have so many to remember. It is tempting to have just one password to manage all your account so that you don’t have to remember them all. But, to do that would be criminal neglect and here is why:

- too often passwords are too weak and easy to hack
- computing power has significantly improved, so brute force cracking is more successful nowadays.This was something that used to take years but with today’s computing power it can be done in minutes

- ·Just because you are doing the right thing it does not mean others have. A classic example, awhile back a major software supplier had their system hacked. Hundreds of thousands of login details were stolen. These hackers used the stolen details to break into other online service providers - using the stolen login details because they knew people were inherently lazy with passwords

The key lessons are not have the same username, email and password for all your accounts and make sure to keep changing them regularly. Cybercriminals are more creative than we may think. All is not what is seems.

Make sure important system use 2FA

2FA stands for Two-Factor Authentication. It is an extra layer of security used to make sure that people trying to gain access to online accounts are who they say they are. One of the most common methods used by security modules is to send an SMS to your phone for you to confirm who you are before logging into the account.

The use of 2FA is strongly recommended for all of your financial and critical systems. 2FA just makes it that much more difficult for any hacker to break into your system. Most security software and software tools now support some sort of 2FA.

Ensure that you have a security installed

This may sound obvious, but you might be surprised at the number of e-commerce or other types of websites that do not have any sort of security modules or firewall. A lot of people make the wrong assumption that security is

automatically implemented by your web hosting supplier on your website application.

Web hosting providers have security modules that protect your web hosting and other related systems such as your email, but your application/website lives on the public side, outside the firewall. You are responsible that they are adequately protected. Yes, your web hosting firewall does protect to some degree but as I mentioned before, because your website lives in the public domain and each website is built differently that makes it your responsibility to secure your site.

I don't mean to bash freelancers, after all I was freelancer myself, but they have been one source of this problem. To be competitive and secure the job freelancers often bid very low prices to build the web site. What they are really are quoting are just the bare bones of the website. This does not include any of the extra steps required to make your site fully functional, e.g. security setups, image optimisation, etc.

Note that all websites are fair game to hackers. Just because you are not an e-commerce site or have a high profile does not mean you won't be targeted.

Have a disaster recovery plan

Sometimes things don't go according to plan. How you respond to things can make a huge difference to your customers and your business. Having a disaster recovery plan will help you to quickly respond and take appropriate steps to restore services.

Whatever your plan is, make sure you test it to see if it works. I've seen situations where the backup system did not back up things completely, so when they restored work only part of the system was restored.

Have backups and off-site copies

I cannot tell you the number of small business owners that do not know if their system has backups. Most small business owners assume their web host providers offer this facility and that it must be working. The reality is, it really depends on the web host provider. Some providers include backups for free as part of their package. These backups are either automatically enabled or must be manually enabled. There are a significant number of providers who only offer backups as a premium service with an additional cost.

Just because you have backups enabled, it does not mean they are adequate to your business needs. For example, the frequency of backups will depend on how often the data changes. For the vast majority of websites that are static, you'll most likely need backups once a week. However, on e-commerce sites where the data can change by the hour or minute, the frequency of backups will be much higher.

And please make sure you have copies of your backups offsite, i.e. not with the same web host provider. If something were to happen to your web host provider you then have the ability to access your offsite backups to restore services from elsewhere.

Report attacks

Finally, depending on the size or structure of your business, you may be obligated under the Privacy Act to report Data Breaches to the Office of the Australian Information Commissioner (OAIC).

Some small business covered are:

- a private sector health service provider. An organisation that provides a health service includes:
  - traditional health service provider, such as a private hospital, day surgery, medical practitioner, pharmacist and allied health professional
  - complementary therapist, such as a naturopath or a chiropractor
  - gym or weight loss clinic
  - child care centre, private school or private tertiary educational institution
- a business that sells or purchases personal information.
- a credit reporting body.
- a contracted service provider for an Australian Government contract.
- an employee association registered or recognised under the Fair Work (Registered Organisations) Act 2009.
- a business that holds accreditation under the Consumer Data Right System.
- a business that has opted-in to the Privacy Act.
- a business that is related to a business that is covered by the Privacy Act.
- a business prescribed by the Privacy Regulation 2013.

For more information as to who needs to report visit the OAIC website.

CONCLUSION

Regardless of the size of your business, cybersecurity is needed more than ever to protect your business from the threat of cybercriminals who wreak havoc on your business. It is not just a moral duty but a legal requirement.

Remember, your data is priceless and worth a lot to cybercriminals, so you need to take steps to protect it. If you feel overwhelmed or not sure where to start, then get help. Ignoring the issue will end up costing you a lot more than to remedy the problem.

Make sure you've done everything you can do to avoid becoming a victim of an attack. Don't be a statistic - take action today.

If you need assistance with your Website Security or want to discuss Cybersecurity

Take Advantage of our
FREE 30 Minute Consultation

Contact Gerald
Small Biz Web Solutions
(02) 8091 4399
info@smallbizwebsolutions.com.au