ESTHER OH, *CEO of Agile 8*
LinkedIn: https://www.linkedin.com/in/ohesther/
Website: https://www.agile8.com.au

Esther is committed to help SMEs navigate the ever-evolving challenges of digital transformation. She is the founder of Agile 8, an Artificial Intelligence and eXtended Reality tech company that helps frontline and remote workers complete mission critical work much Smarter. Faster. Safer with multiple qualifications in cybersecurity, risk management, governance and information systems.

DID YOU KNOW?

According to Cisco's latest 2021 Security Outcomes study, small businesses are more successful than large companies in implementing agile security approaches that enables them to compete in a crowded marketplace.
Having a robust IT risk management framework not only creates a competitive advantage, it is expected by your customers as absolutely essential to protecting their data and privacy entrusted to you.

Here are some practical ways you can increase your credibility with customers and protect your business from cybersecurity attacks.

TIP 1. CYBER RISK STARTS FROM YOUR PHONE

You answer the phone from an unknown number, asking for your personal details because: "You are under investigation", "Your parcel is withheld at Fedex" or "Your car had an accident". Once your details are leaked, criminals steal from you, or even sell your identity on the dark web. If you get such phony-baloney calls, hang up and block that caller immediately.

TIP 2. CHECK TRUSTED REVIEWS

COVID-19 accelerated e-Commerce as people turned to buying online. However, that also increased the opportunities for scammers to target small businesses that do not have sophisticated IT resources. Before you download apps or procure online from Alibaba, Amazon or eBay, or direct on your supplier's website, check their trustworthiness, such as Google, Facebook and Trust Pilot reviews. Use the power of social media to your advantage.

TIP 3. ENSURE YOUR SECURITY CERTIFICATE IS CURRENT

If you sell online, it is important to ensure that your website security certificate is up-to-date, or else customers may leave your website when a pop-up shows that your certificate has expired and hence losing the sale. If you outsource your website to Fiverr or Upwork freelancers, ensure that you change the password once they have finished their work. Put a reminder on your calendar to ensure you don't miss those renewal dates.

TIP 4. NEVER EVER CLICK ON SUSPICIOUS LINKS

Have you ever received "You won an iPad or Surface Pro!" with a hyperlink? These are likely phishing emails. Some of these emails may even look legitimate, as if they are coming from Apple, Microsoft or a company you know. Always check that the email addresses are the official ones before opening attachments or clicking on the hyperlinks. E.g. support@microsoft.de is fake as opposed to support @accountprotection.microsoft.com

TIP 5. UPDATE YOUR OS REGULARLY

Update your mobile phones, laptops and computers Operating Systems (OS) regularly to ensure that you have the latest security patches. If you are on Windows 10, Windows Defender is the default security application. If you subscribe to Microsoft 365 Business or Enterprise, it also comes with added security. However, if you are on the older OS, you should invest in Norton or similar anti-virus, anti-malware types of subscription to protect your systems.

TIP 6. BEWARE OF USING PUBLIC WI-FI

Tapping into free Wi-Fi may sound like a data and cost saving idea while bingeing on Netflix, but it might cost you more if your device is not protected. Your data may be intercepted while you are using free public Wi-Fi. Consider Norton 360, CyberGhost, ExpressVPN, NordVPN or PrivateInternet Access if you are often out and about while paying bills over public internet.

TIP 7. CHANGE PASSWORDS PERIODICALLY

Whilst this sounds old-fashioned, it is a best practice to force change passwords via automated system controls. Ensure that staff do not re-use, share or reveal their passwords for multiple applications. It is a pain for most but, thanks to the many apps now incorporating Single Sign-On and automatic passwords saving on Google, changing passwords regularly do deter hackers from penetrating into your systems. Ensure that passwords are not easy to guess.

TIP 8. GET CYBER AND PRIVACY PROTECTION INSURANCE

In this modern age, it is impossible to fool-proof your business from cyber attacks. So consider getting insurance to cover for cyber fraud, data privacy breaches and business interruption due to network or electrical outages. Often the application form provides a checklist that is useful for SMEs to implement, such as having a Disaster Recovery Plan, Business Continuity Plan and annual security audit which will reduce your premiums.

TIP 9. INVEST IN CYBERSECURITY

If you store lots of clients' confidential data (like their credit cards, date of birth and contact details), it is important you invest in robust encryption, firewalls and intrusion detection systems. Ideally, you should get an independent cybersecurity expert to run network penetration tests at least annually. The good ones will provide a comprehensive report with recommendations on improving your cybersecurity.

TIP 10. REPORT TO AUTHORITIES

So what happens if you get hacked? Secure and backup your systems and data, close the security loopholes immediately and get cybersecurity help. Report to the authorities, such as your bank, credit card provider or even the Police or ASIC where applicable. ReportCyber is the Australian Government's online cybercrime reporting tool for Australian individuals, businesses and government, and you can access it via www.cyber.gov.au

Well, these are some common-sense tips that businesses often regret overlooking in hindsight. Do take action to protect your business today. Remember, prevention is always better than cure.