SASHA HAJENKO, *CISSP Director, Blue Phoenix Systems*
www.bpsystems.com.au

With over 20 years providing IT and cybersecurity services to small and medium businesses, large financial and medical organisations, and delivering workshops and training sessions on cybersecurity topics to a wide variety businesses and industries, Sasha brings his experience, passion and capability to every engagement. Developing tailored strategies and technical controls for SMEs based on their risk profile and budget is his speciality.

TIP 1. THE ESSENTIAL EIGHT

The Essential Eight are best covered under a single tip as all of them will be covered in detail by others in this publication. Preventing applications that are not explicitly allowed. Patching applications and operating systems protects against attackers. Harden applications to close vulnerabilities. Turn off Macros to prevent malware. Enable Multifactor Authentication everywhere. Restrict administrative rights. Take backups regularly and, just as importantly, test them often.

TIP 2. KNOWLEDGE IS POWER

Many fraud, ransomware and breaches start with a well-crafted phishing message. Ensuring your team know how to recognise scams, credential theft, or ways attackers introduce malware is crucial. Simulations, advisories and staff training sessions will arm your team with the knowledge to think before they click and save your business from significant harm.

TIP 3. BE RESPONSIBLE WITH YOUR DATA

Quite often when a breach occurs, data exposed includes information on past stakeholders which you likely no longer needed. Purging or anonymising old information from your CRM, email, and other information systems reduces the likelihood of a breach exposing information which you maybe should have no longer been holding.

TIP 4. KNOW YOUR CLOUD

The cloud is just another computer system. It is important to know your responsibilities for the cloud systems you use. Most cloud providers, and especially Microsoft, AWS and Google, operate on the "shared responsibility" model. In essence they are responsible for the availability and stability of the platforms while the safety, reliability and recoverability of your data often falls to you.

TIP 5. USE AN EMAIL FILTER

Email borne threats are everywhere so you can't really go without a filter that scans emails, links and attachments for malicious data. These filtering platforms should also verify the sender is legitimate by validating the source of the email to protect you from spoofed emails. Also, turn on SPF, DKIM and DMARC on your domain so that recipients can trust your emails.

TIP 6. BLOCK CEO FRAUD EMAILS

Scammers send email with a "From" name that is the same as someone with authority in your business, for example the CEO, Finance manager or Operations manager, and request staff purchase gift cards, pay an invoice right away or other

methods to extract financial gain. If you can, set up your email filter to block emails that have the same name as high level roles in your organisation to prevent staff falling victim to these types of scams.

TIP 7. DEVELOP A PLAN FOR INTERRUPTION

In the event of an incident that impacts your business, you need to understand how you can continue to operate your key processes. Developing a Business Continuity and Disaster Recovery (BCDR) plan allows you to plan out continuity activities and recovery steps with a clear head, and testing this plan at intervals will give you the confidence it can be relied upon. Trying to figure these things out during an emergency is not going to get you the best results.

TIP 8. USE A PASSWORD MANAGER

Password reuse is one of the bad guys favorite things, because once they have your credentials they try them everywhere else. A password manager allows you to create complex passwords, unique for every service and you only have to remember one password again. Make sure your master password is a strong passphrase of at least 18 characters that you can easily remember but will be very hard to guess.

TIP 9. CYBER INSURANCE

Cyber insurance provides support to respond and recover to cyber incidents. Just like you have professional indemnity, public liability, home, car and likely other types of insurance, cyber insurance is something you should definitely have to cover you against a real threat. The costs are not prohibitive and the better you protect your business with the tips in this publication, the lower your premiums are likely to be.

TIP 10. SECURE YOUR DEVICES

If a device is lost or stolen, could someone get access to the information on it? Make sure your devices are encrypted, and secured against theft with physical security measures. Implement a management platform so you can remote wipe or otherwise disable them should they fall into the wrong hands, and make sure they are purged of data before you dispose of them.