DR. OLIVER GUIDETTI *Post Doctoral Researcher, Edith Cowan University, Security Research Institute*
LinkedIn https://www.linkedin.com/in/oliver-guidetti-23069a94/

Oliver has a double major in mathematics and psychology (with first class honours in the latter) and has recently completed his PhD in cyber psychology, an applied inter-disciplinary field which leverages the brain sciences in studying network defence. His research focuses on seeing the human in complex data, including human computer interaction behaviour and psychophysiology

TIP 1. UNDERSTAND THE THREAT LANDSCAPE

Familiarise yourself with common cyber threats. The Open Web Application Security Project (OWASP) Top 10 is a great starting point. It outlines the most critical web application security risks and how to mitigate them. Remember, cyber threats are not one thing, they are ever evolving, so it is critical to treat your cyber security as an on-going matter that should be regularly reviewed.

TIP 2. CONTINUAL EDUCATION

Cybersecurity is an evolving field. Keep yourself updated with the latest technologies, threats, and cybersecurity practices. Regular training and obtaining relevant certifications can be beneficial. However cyber threats can also be industry specific. Small businesses therefore need to bear in mind that there is no one-size-fits-all with respect to cyber education. If in doubt, consult an expert about what specific risks your business may be vulnerable to.

TIP 3. STRONG PASSWORDS

Passwords have proven time and again difficult for human users to use well. A password manager (such as LastPass) is an absolute must for small businesses, because they make good password practices much easier to ensure consistently across all employees within your small business. Make sure that passwords are complex, don't recycle the same password across multiple systems, and change them every few months.

TIP 4. TWO-FACTOR AUTHENTICATION (2FA)

Implement 2FA wherever possible. It adds an additional layer of security by requiring two types of identification before granting access.

TIP 5. PHISHING AWARENESS

Educate employees about the dangers of phishing attacks, which is the primary way ransomware attacks are launched. They should be cautious of suspicious emails, especially those asking for sensitive information or directing to unfamiliar websites. Small businesses should also incentivise employees to report phishing attacks.

TIP 6. REGULAR BACKUPS

Regularly back up essential data. In the event of a ransomware attack or data loss, backups can help restore your system with minimal disruption to business operations. It is essential to have at least two different types of backup, onsite and offsite. If your small business doesn't have a redundant backup, it increases your vulnerability to ransomware.

TIP 7. NETWORK AND SYSTEM ADMINISTRATION SKILLS

Understanding and managing network concepts and devices, monitoring network performance, troubleshooting issues, securing networks and managing system/user accounts are essential skills for small business owners. These capabilities help identify and mitigate potential cyber threats, ensure secure and efficient operations, and protect sensitive data from breaches. For example, keep the number of users with administrator level privileges as minimal as possible.

TIP 8. DATA RETENTION

Unnecessary data storage increases the risk of data leaks. By promptly deleting unneeded data, businesses can significantly reduce the potential for cybersecurity threats and associated damage. This approach ensures that only relevant and necessary data is stored, enhancing data security. Consider a retail business that collects customer information for transactions. This data is not needed after a transaction and should be securely deleted post-transaction.

TIP 9. REGULAR SYSTEM UPDATES

Keep all software, including antivirus software, and operating systems updated. These updates often include patches for known security vulnerabilities.

TIP 10. INCIDENT RESPONSE PLAN

Have a clear incident response plan in place. This includes identifying a potential breach, containing the incident, eradicating the threat, recovering from the incident, and learning from the event to prevent future incidents.