LEONARD KLEINMAN *- Field CTO and Evangelist - Cortex Palo Alto Networks JAPAC Adjunct Professor, Deakin University*
LinkedIn/Website https://www.linkedin.com/in/leonard-kleinman-713481/
Website: www.paloaltonetworks.com

Career cyber geek, with a mission to work with executives and business stakeholders to make cyber security a strategic priority that translates into business value and assisting in the development of a risk-based cyber security culture aimed at protecting our digital lives.

TIP 1. RECRUITMENT

Do your preparation! Ensure your duty statement and selection criteria are accurate and reflect the actual role. More importantly, make sure your interview panel comprises people with the necessary knowledge and experience to effectively recruit for cyber related roles. Having a passing interest in cyber does not cut it. Finally, use scenario based questions - these are far more effective than just academic questions.

TIP 2. LEGISLATION AND REGULATION

Whichever sector you are in, take the time to understand the various regulations and legislations that impact your organisation and ultimately affect how you practice cyber-security. Worldwide regulation and legislation has grown significantly with many impacting business beyond the traditional geographical borders. Understand firstly if it impacts you and next, what you have to do to comply.

TIP 3. INVEST IN YOUR PEOPLE

Retaining good cyber folk is just as hard as finding them. These are the people you rely on to operationalise your cyber-security program. Focus on keeping their skills current and grooming them for future opportunities by taking the time to connect and understand them and their needs.

TIP 4. CULTURE

Aim to develop a strong risk based cyber-security culture predicated on 'prevent, detect and respond'. There is much we can do to 'prevent' and the savings speak for themselves. However, this should not be at the expense of 'response'. Despite our best efforts to 'prevent', bad things will undoubtedly still happen. You will still need responders to deal with incidents, incursions and other failures.

TIP 5. BASIC CYBER-HYGIENE AND RECOVERY

Religiously execute the fundamentals: updating systems (turn on automatic updates for operating systems and applications), applying patches and managing your passwords. Often overlooked by SMEs are other activities such as performing regular backups and restricting privilege access: not everyone on your network needs to be an Admin. Test your backups at regular intervals and have a disaster recovery plan.

TIP 6. MULTI FACTOR AUTHENTICATION (MFA)

Enable and use MFA wherever possible. MFA requires two or more proofs of identity to enable access. Many systems and services now offer MFA including banking, social media platforms (Facebook, Linkedin, WhatsApp etc), cloud platforms and webmail. MFA makes it harder for cybercriminals to attack you and your business.

TIP 7. STAFF EDUCATION AND AWARENESS

People are the first line of defence. Ensure you have a cyber-security training and awareness program in place and make sure it evolves to keep pace with the evolving threat landscape. This enables you, and your employees, to be aware of what the latest cyber attacks look like so, when faced with one, they will be able to take the right actions.

TIP 8. SECURE YOUR PRINTERS

Often overlooked is the security of printers, many of which contain similar technology as computers and importantly, are connected to your network! Make sure to set them up properly, configure the right settings including security software and components (including secure logins for printing). Additionally, have a policy for secure document management and train your staff in the correct procedures.

TIP 9. FREE WI-FI EVERYWHERE

Be conscious of what you are doing when using free Wi-Fi and hotspot services. Free internet is everywhere - cafés, shopping centres, hotels, etc. and many of these services are often unsecure. Being unsecured means anyone can access it and intercept information and data, spread malicious software or even set up fake wireless access points (otherwise known as a 'honeypot'), to trap unsuspecting users.

TIP 10. HAVE AN INCIDENT RESPONSE PLAN - KNOW WHAT TO DO WHEN COMPROMISED

You have to be aware of what to do in the event that you, or your business, is hacked. What if you (or a staff member) accidentally clicked a malicious link or downloaded malware? You must know who to contact (internally or externally), how to report the incident and what is required in the reporting process. Having an incident response plan teaches your staff what to do and how to react in a timely manner in the event of an incident.