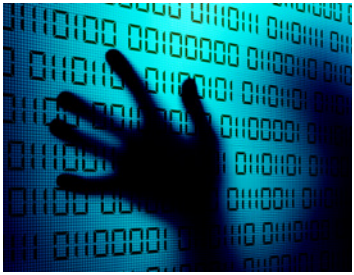
TONY FERRARIS *IT Sales - Collaborating with customers along their digitisation journeys*
Linkedin.com/in/tonyferraris

TIP 1. POLICY (FIRST NOT WIDGET) DISASTER RECOVERY STRATEGY

Whether you're working out of your house, a cafe or office, then there is a potential risk of being hacked. Anywhere, anytime - treat your cyber policy the same way you would treat your risk and compliance for a fire and safety value proposition. ***If you are on the digital transformation journey, like the rest of us: PLAN to add EVERYTHING as to how it fits within your cyber strategy first.*** You know the drill: fail to plan and...For goodness sake, just as if there was a fire - stop blaming the IT department for everything! EVERYONE IS RESPONSIBLE NOW.

TIP 2. PROCESS (NOT JUST CYBER INSURANCE) DATA IS THE NEW KING AS CASH WAS



After planning, now follow a process. MINIMISE risk and BUILD resilience. Hackers will move to easier targets if you set up and improve barriers. ***Do you treat cyber as an investment or a expense? How long could you, and your employees/customers, live without access to data? When did you execute a restore from a FULL back up via MSP exercise to prove it?*** Just because you bought a firewall doesn't mean that you are set. How fast could you restart your business with no infrastructure, both new and old and how would an event like this impact your productivity and overall customer's experience?

TIP 3. PEOPLE - REGULAR ONLINE AWARENESS TRAINING

Every day the threat landscape changes. ***Most cyber incidents are created by human error based on emotion to click and go. Meet everyone in your organisation at THEIR LEVEL OF NEED and standardise change progress.*** You may have the right policy and plan process but, as mentioned, if there was a fire: who is responsible for safety? Set up a monthly (if not quarterly) one hour online cyber course with ongoing INCENTIVES for people to complete and stay up to date with hacker tricks. For instance: offer a dinner raffle incentive … and make it fun!

TIP 4. EXTERNAL AUDIT - EARLY AND OFTEN

OHS - everyone has regular fire drills, knows the muster area, where the fire extinguishers and blankets are located. You regularly get the electric kettles, cords etc checked? ***Consistently undertake an independent cyber audit team and conduct an audit of your strengths and weaknesses.*** Like a football team:- execute, rehearse and check. Get your MSP to incorporate AI and machine learning processes/services so that you can sleep at night.

TIP 5. DEFAULT LOGINS/PASSWORDS HEALTH CHECK ON ROUTER, PRINTER/MULTIFUNCTION

So you have a new router/firewall at home, or an existing one? Download Trend Housecall for free on a Smartphone (not to your corporate device) and scan devices. Will it bring up IP addresses and show risk levels for everything at home? ***Look at that router thing that is the policeman to the bad guys. Change the admin/admin to something else immediately before hackers can bypass. Oh, and if you want a fair dinkum print audit there is an 80 point check list only one point for setting up Secure Print at home and also at the office. Please be secure responsible and don't forget about saving trees and print two-sided.***

TIP 6. HEARD OF THE ESSENTIAL EIGHT?

…or the privacy notification breach act 2018? Need compliance For Tenders? For instance 2FA does not mean what you think. Ha! Rather; don't blow your brains out when you read them, "to know and not to do is not to know". ***Back to***

policy, get the MSP or IT to help - it's the basic fundamentals for improving resilience, standardises your organisation for working with potential suppliers and customers, you may be compromising them as well!

TIP 7. RANSOM WARE ISSUE? SHOULD I PAY OR SHOULD I NOT?

Did you know that it's estimated that 40% of businesses that pay the Bitcoin Ransom don't get the data released? Also, how do you know if the virus is limited to where you think it is, or lying dormant? You've seen forensic cop shows like Colombo? It takes an average of four months to find the extent of an incident. Bottom line is, if you have to start over: *EXTERNAL OFFSITE DATA retrievable and archive with instantaneous restoration to FULL back up is the bottom line. You have multiple bank accounts because they are only insured to a certain balance? Back up 3-2-1.*

TIP 8. WINDOWS 10 OR TICKING TIME BOMB - HACKERS NOW AUTOMATING ATTACKS

Have you been marooned on an island with a volleyball, with no access to civilisation? *If you are still using that old Windows 7 Operating System lying around, and connecting to your network because it's easy, or have old servers that have not been updating, or have no more support - DO NOT USE OR CONNECT - PERIOD!* As the saying goes: hard enough to live a long and stress free life but you're allowing an inevitable business SUICIDE if you use these devices with no plan. In most cases it could, and will, void any Cyber insurance claim.

TIP 9. WE ARE ALL GOOD AT DOING SOMETHING BUT...

So, you still wear 18 hats at the office as owner, MD, IT and have limited time and budgets? *Stick with your CORE OFFERINGS and consider outsourcing. You get what you pay for - and I refer to tips 6 and 7. Find an IT partner that knows you the customer and can help you grow based on your unique business outcome experiences. "People don't care how much you know until they know how much you care."*

TIP 10. CONSIDER TO BUY OPEX AND VIA CONSUMPTION BASED MODELS

Can't afford every disruptive cyber innovation that is being thrown at you? Think long term and deal with fluctuating staff numbers. ***These days, treat Cyber as an investment and you can incorporate the same concept as you do buying Microsoft licenses.*** Allows them to share the security and storage issues, allows you to plan and grow your business with state of the art software/services and additional new features that impact your business outcomes for the long term (not just the outdated widgets you are spending support people for). Helps you standardise and save $$$ on unplanned surprises.