STANLEY LI, *Securli Limited, CEO*
https://www.linkedin.com/in/securli-stanleyli/

TIP 1. UNDERSTAND THE RELATIONSHIP BETWEEN YOUR INVESTMENTS AND YOUR RISK

As a business leader, you need to understand your business GRC (Governance, Risk, Compliance) Controls and Technical Controls to justify your investment in cyber security. The GRC controls can simplify administration tasks:– who has all my I.T. systems' passwords and, if that person left without notice, will anyone be able to recover all the passwords? These simple tasks of a "Super Admin" right will protect your investments from being frozen.

TIP 2. NOT TAKING INTANGIBLES INTO ACCOUNT

Although damage to brand image and reputation is of major concern to most cyberattack victims, it is notoriously challenging to express these losses in financial terms. But, in any industry with significant competition, customers can be lost because they no longer trust you in the wake of data compromise and will almost certainly never return.

TIP 3. THINKING THAT AN "HONOR AMONG THIEVES" MENTALITY STILL PREVAILS AMONG ATTACKERS

2022 Data Security Incident Response Report from BakerHostetler. Highlights that 82% of ransom notes contained a claim of theft of data before encryption. Of these 82%, 73% found evidence of data exfiltration and 81% resulted in notice to individuals

TIP 4. DEFINE THE TERMINOLOGIES WITH OUR STAKEHOLDERS.

We identify three groups of stakeholders (Business Executives, Governors, and Technologists) who have different objectives when it comes to "Cybersecurity" leading to miscommunication. Failure right out of the gate. An example of terminology muddle:- some vendors use "Penetrating Test," when it is just a vulnerabilities scanning, devil in the detail.

TIP 5. BRING TOGETHER COMMON OBJECTIVES WITH A UNIFIED LANGUAGE.

Organisational teams often use different words to describe the same idea, so they do not know what each other means. To fix this problem, we want people to "speak" a single language and collaborate with one another's objectives. Make your data visible and come alive, it will reveal risk trends and allow the organisation to refine objectives and prioritise tasks.

TIP 6. UNDERSTAND RISK WITH AN UNBIASED RISK ASSESSMENT AND AUDIT.

Even if organisations have invested in cyber security, the Assessment should ensure that the data coming out of any solutions is meaningful, correct, and mapped against enterprise risk. Larger companies have the resources to thoroughly assess their supply chain, but SMBs should engage with third parties to assess the risk of unknowns and create a progressive roadmap.

TIP 7. START WITH YOUR TEAM MEMBERS

Organisational culture starts with the business leaders to change the behaviours of staff to improve cyber security. It is often not about the cost or type of solution; it is about people. Invest into Security Awareness Training and it will be your best ROI in cyber resilience.

TIP 8. TRYING TO PREDICT THE COSTS OF A RANSOM WARE ATTACK

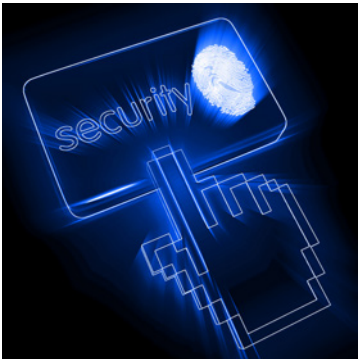
With most attackers now demanding payment in Bitcoin, or other cryptocurrencies, it's becoming increasingly difficult to estimate (in dollars) how much a ransom might actually cost you. If your business is not equipped with the Business Continuity Plan, then you must be sure that you have the cryptocurrency ready to pay the ransom, or you can have the pencil and paper ready as your BCP.

The average ransom paid increased to US$812,360

The average cost to recover from a ransomware attack was $1.4 million

https://www.sophos.com/en-us/press-office/press-releases/2022/04/ransomware-hit-66-percent-of-organizations-surveyed-for-sophos-annual-state-of-ransomware-2022

TIP 9. FIND YOUR NORTH STAR IN THE MAZE OF THE GALAXY



For non-technical business leaders, the maze of cybersecurity can be overwhelming. The question always comes back to "where do I start?" Increasing Staff Awareness is the lowest cost or no cost when you are willing to spend some time searching through the Internet. The next thing is a Non-profit organisation that provides recommendations that you trust, and you can follow with your budget. DNS Firewall or Filter is one of them we recommended to block some of the malicious IP addresses associated with ransomware. It is like an onion, one layer at a time.

TIP 10. "TRUST & VERIFY."

Garbage in garbage ,out - clarifying data from current solutions for trust and aligning them with stakeholder objectives to verify the ROI. Then, adjust your "Building Blocks" accordingly, to continuously monitor and verify the integrity of data... so the team can "see" the KPIs and Business Executives can measure the ROIs. Transform data from intangible into tangible so everyone can see and contribute to the efforts of collaboration.