ERANGA GIHAN, *Information Security and Technology Manager, PepNet Technologies*
LinkedIn linkedin.com/in/eranga-gihan Website www.pepnet.com.au

Positioned to lead the next generation of business intelligence - Cyber Security Auditor, Adviser and Enthusiast. Interconnected information management discipline to deliver valued-based programs with commitment, shared purpose, and achievement of enterprise goals.

TIP 1. IMPLEMENT A CYBER POLICY

This is a crucial activity for safeguarding your organisation's digital assets and reputation. Following these essential steps to create and implement an effective cyber policy.

1. Set password requirements.
2. Outline email Security measures
3. Handle sensitive data
4. Rules for handling technology
5. Standards for social media and internet access

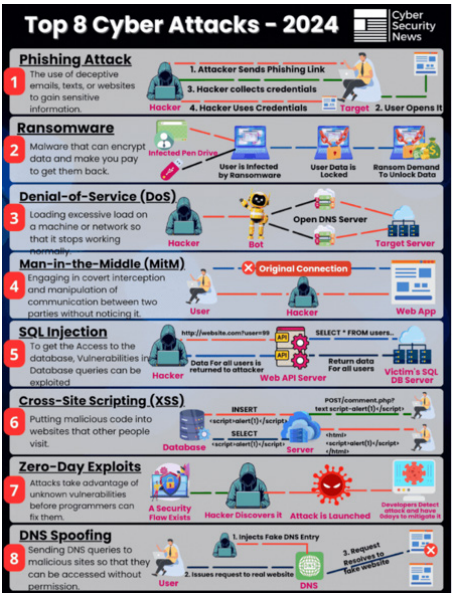
A well-crafted cybersecurity policy not only protects your organisation but also educates employees about their role in managing and maintaining security. Regularly review and update the policy to stay ahead of evolving threats.

TIP 2. USER TRAINING AND AWARENESS - AND IT STARTS FROM THE TOP MANAGEMENT

This is another crucial component of an organisation's cybersecurity strategy.

What is User Awareness Training? – This aims to educate employees about what cybersecurity is and how it applies to their everyday life. It equips them with the knowledge to recognise and mitigate various online threats, including malware, phishing, man-in-the-middle attacks and more. 90% of security incidents are linked to human error and it always starts from phishing attacks - which are preventable.

The management and leaders of the organisation play an important part in driving user awareness. The key is to continually keep security at the forefront of user's minds.



Source – Cyber Security News

TIP 3. ADOPT A KNOWN CYBER SECURITY FRAMEWORK

Adopting a known framework is essential for organisations to establish and maintain effective security practices. These frameworks provide guidelines, standards, and best practices in helping organisations reduce their exposure to vulnerabilities that hackers and cybercriminals may exploit.

By adopting a framework, the organisation will reduce their risks, maintain consistency of services, being compliant, and increase efficiency of the services they provide.

Among all the frameworks, Essential Eight Maturity model is recommended by ACSC that provides basic mitigation strategies for Australian organisations. Remember, adopting a cybersecurity framework is a proactive step towards safeguarding your organisation's digital assets and maintaining resilience against cyber threats.

TIP 4. CREATE A RISK REGISTER

This is an important tool in risk management. A risk register, also known as risk log, is a tool used to identify and track potential risks that could impact your organisation's operation and reputation. The purpose of a Risk Register is to:

anticipate risks, collect potential risks, risk analysis mechanisms and track risks. In creating a Risk Register, you need to gather relevant information, enter potential risks, prioritise risks, assign risk owners, and continually update the register. If a new risk is found that needs to be included in the Risk Register immediately. A well maintained Risk Register enhances organisation resilience and helps proactively address potential challenges.

TIP 5. BACKUPS, BACKUPS AND BACKUPS

Backups are your digital safety nets, ensuring that your important data remains secure even in the face of unexpected events. Keeping copies of your data separately from the original source serves as a fallback in case of data loss due to: hardware failure, accidental deletion, cyber-attacks or natural disasters. Regular schedules, redundancy, test restores, offsite storage, encryption and document procedure are best practices in maintaining backups.
Remember, backups are your digital insurance policy, so implement them diligently to safeguard your valuable data.

TIP 6. CLASSIFY YOUR DATA

This process helps to organise and categorise data based on its type, sensitivity, and value. The purpose of data classification is to maintain security and compliance of that data. In security, it aids in protecting sensitive information from cyber threats, data breaches and other risks. In compliance, it ensures adherence to data protection laws and regulations. Level of sensitivity can be categorised as: high sensitive data, medium sensitive data, and none-sensitive data. So, to identify, categorise, assess risks and select solutions is the process of data classification. Proper data classification enhances risk management, compliance, and overall data security.

TIP 7. IMPLEMENT THE PRINCIPLE OF LEAST PRIVILEGE

This is a fundamental cybersecurity concept that aims to limit access to data and systems to only what is necessary for users, processes, and devices to perform their tasks. Importance of the Principle of Least Privilege is to reduce the attack surface. To mitigate insider threats, prevents lateral movement and ensures regulatory compliances. You can implement this via: define the roles and permissions, invest in privilege access management solutions, enforce multi-factor authentication, segment your networks, and regularly audit network privileges,
Implementing the principle of least privilege enhances security and protects sensitive information from unauthorised access.

TIP 8. LEVERAGE THE EXPERTISE FROM YOUR IT SERVICES PROVIDER

Using the expertise from your IT services provider can significantly benefit your organisation in providing business continuity and strategic guidance and practices and solutions to cybersecurity vulnerabilities. Most IT services providers offer various services such as: workforce, infrastructure, cloud, managed and asset disposition. They bring a value based approach to your organisation, to fill skill gaps, guide digital transformation and accelerate business objectives. They provide expertise, day-to-day operational support, strategic guidance, and technical proficiency to help identify, deploy, and manage the right solution to address the business needs.

TIP 9. IMPLEMENT A BUSINESS CONTINUITY AND DISASTER RECOVERY PLAN

Implementing a robust Business Continuity and Disaster Recovery Plan will help any organisation toward achieving cyber resiliency in the event of a breach. A BCDR is essential to any organisation for minimising data loss, downtime, financial penalties, and reputational damage due to unplanned incidents. Benefits of BCDR are: risk mitigation, data protection, financial resiliency, and reputation management. A well implemented BCDR ensures your organisation's resiliency and continuity even in challenging circumstances.

TIP 10. USE VPN (VIRTUAL PRIVATE NETWORK) IF YOU HAVE THE OPTION

This is a very smart move to enhance your security and privacy, especially when you are using public Internet/Wi-Fi services. A known VPN tool will help prevent man-in-the-middle attacks when you are connected to non-corporate networks. Do not always trust free Wi-Fi services since most attackers broadcast their own Wi-Fi networks in public areas to explore vulnerable users and steal their identify or monitor activity to explore ways to attack user computers. The use of the VPN helps secure your Internet connection and provide an extra layer of privacy.