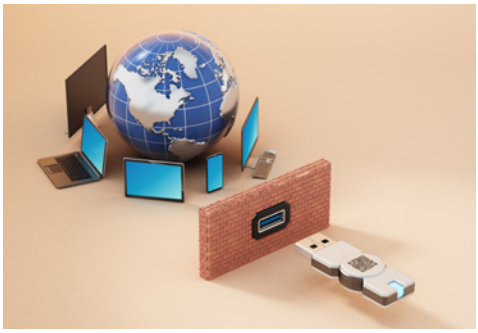
BIBI ROUKSAR DUSSOYEA *Consultant, KPMG*
linkedin.com/in/bibi-rouksar-dussoyea

Bibi Rouksar is a highly motivated Consultant at KPMG within the Technology Risk and Cyber Division. She has recently completed her master of Cyber security with distinction, along with a solid academic background and a comprehensive skill set. Additionally, as a first-class honour graduate in Actuarial Studies, she has developed excellent analytical abilities and creative problem-solving skills.

TIP 1. ADOPT A CYBER SECURITY FRAMEWORK



In addition to serving as a system of guidelines and best practices, an appropriate cyber security framework may help your organisation assess its current level of cyber maturity and help determine how secure your network and data are. Implementation of a framework helps assessing the effectiveness of existing controls and may greatly contribute to security goal setting and may also help achieve cyber maturity uplift as, and when, required. Examples of widely used frameworks include NIST CSF, Essential Eights, and ISO 27001.

TIP 2. MAINTAIN PASSWORD HYGIENE AND POLICY

Practicing good password hygiene is a must when it comes to enhancing security in the digital world. Simple measures within a strong password policy include recommendations such as use of long passphrases, use of password managers, review of password lifecycle and regular change frequency. Moreover, it is recommended to avoid use of personal information and/or dictionary words, discourage password sharing and avoid use of similar passwords for multiple accounts.

TIP 3. IMPLEMENT MULTI-FACTOR AUTHENTICATION

In order to reduce security breaches and prevent unauthorised access, instead of using only usernames and passwords to secure an online account, multi-factor authentication (MFA) requires users to provide two or more login credentials before they can be authenticated to gain access to their device, or to a system/network. Examples of MFA include email/SMS verification code, another set of passphrase/pin, authenticator key applications, biometrics such as fingerprints, or security badge.

TIP 4. SECURITY AWARENESS TRAINING

It's often argued that "humans are the weakest link in cyber security" due to issues mostly linked to human error such as misconfigurations, weak passwords, or falling victim to cyber-attacks like ransomware. To address the problem at the source, it's essential to promote cyber security awareness so that employees understand the significance of their role in protecting the organisation against hackers and cyber-attacks. (Bonus tip: Cyber security gamification makes training more fun and interactive!)

TIP 5. BEWARE OF PHISHING SCAMS

As the concept of cyber security is becoming more prevalent, the use of phishing scams is getting wider and smarter. To steal personal/company information, threat actors are targeting email inbox of employees by sending messages consisting of malicious links and/or attachments. By using social engineering tactics, cyber criminals try to trick the user into thinking that the message is from a trustworthy party and that the malicious link/attachment is legitimate or harmless.

TIP 6. BACKUP AND ENCRYPTION

Backup of information and systems allow organisations to enhance their resilience against cyber incidents such as ransomware attacks, and also help ensure continuity of operations, data protection and recovery. Moreover, encryption of data-at-rest (stored data that is not being accessed or transferred) and encryption of data-in-transit (data that is being communicated from one system/network to another) are equally important to avoid sensitive company data from being accessed, modified, or stolen by cyber criminals.

TIP 7. SET UP BOTH A FIREWALL AND A VPN (VIRTUAL PRIVATE NETWORK)

A firewall is a network monitoring system which controls incoming and outgoing network traffic based on a set of security rules and preferences. Given its ability to block suspicious (and malicious) network traffic, a firewall may help reduce cyber breaches. To further strengthen your company's security posture, a VPN can be used as it helps create a more secure internet connection while hiding online activity and location, keeping end users safe from cybercriminals.

TIP 8. DATA CLASSIFICATION

Classifying data based on its value and sensitivity helps organisations to better secure their information against accidental or unauthorised access, alteration, destruction, or loss. The most common data classification categories comprise of public, internal, confidential, and highly confidential/restricted. In addition to ensuring data confidentiality, integrity, and availability, data classification also helps organisations to remain compliant to legal and regulatory standards, especially those relating to sensitive client data or PII (Personal Identifiable Information).

TIP 9. CONSIDER CYBER INSURANCE

Not only do cyber-attacks cause business interruptions and system downtime (leading to unforeseeable financial loss and reputational damage), but they also often result in costly regulatory investigation expenses and fines. Having a cyber insurance plan in place will help deter the consequences that may follow cyber incidents by helping your company to recover and also by covering for revenue losses, legal fees, and any other costs associated with remediation of the attack.

TIP 10. BE CYBER AWARE OF CYBER RISKS AND THREATS

It is essential for organisations to remain updated on the latest cyber security risks and threats that surround both their industry peers and other firms within unrelated industries. Be it emerging system vulnerabilities or latest attack methods used by cyber criminals, companies should always stay informed and alert to ensure they are able to protect their data, systems, and networks from the increasing number of cyber criminals.