Integrating cybersecurity and digital defence into SMEs

Many of us do not know what cybersecurity is and the importance of it. Cybersecurity is the practice of protecting systems, networks, and programs from digital attacks. These cyberattacks are usually aimed at accessing, changing, or destroying sensitive information; extorting money from users; or interrupting normal business processes. Implementing effective cybersecurity measures is particularly challenging today because there are more devices than people, and attackers are becoming more innovative.

At the individual level, a cybersecurity attack can result in anything from identity theft to extortion attempts and loss of important data such as family photos. On the macro level, as the society relies heavily on infrastructure such as energy and water plants, hospitals, and financial service institutions, it is hence critical to secure these organisations to ensure that businesses can function normally.

Impact of breaches, legal requirements, and the changing technology landscape

Many businesses process large amounts of confidential customer or employee data. Hence data breaches can exact a heavy toll on businesses. From the short-term perspective, such breaches will cost the organisation time and resources to manage concerned clients. Moreover, additional resources will have to be spent on performing service recovery. From the medium-to-long-term perspective, brand reputation could be adversely affected, impacting annual revenue and business sustainability.

Like most small and medium-sized businesses in Singapore, especially start-ups, business owners are most likely to create an online presence to help their businesses reach out to more customers. It is also likely that business owners will rely heavily on the Internet as a key enabler for carrying out business transaction needs such as payroll, ordering supplies or Internet banking. However, this also exposes business owners to a myriad of cyber-attacks. The costs of cyber-attacks are staggering as estimated by the Ponemon Institute, amounting to a crippling average of $2.2million – involving a combination of clean-up costs and business disruption costs.

This serves as a wake-up call to business owners to be prepared in the event of a cybersecurity incident. Factors such as business downtime, loss of confidential client data and productivity loss need to be considered seriously. With the implementation of Singapore's Personal Data Protection Act (PDPA) and the ever-evolving cybercrime landscape, it is even more critical today for business owners to take accountability in increasing their business' capability in preventing cybercrimes – by adopting best practices in awareness training, and applying adequate security controls to protect their digital business.

Gearing up for digital defence – SMEs

The building of a robust digital defence need not be a daunting challenge for SMEs. Data breach management is an important aspect of the current digital economy. Hence the idea that it happens only to other business owners or companies is almost an unacceptable business proposition to begin with in an economy heavily driven by personal data. In addition, there are legal frameworks governing personal data protection in Singapore that companies are required to comply legally.

Modern hackers and cyber criminals are getting inside help, knowingly and unknowingly, to launch cybersecurity attacks on the organisation. At times, these perpetrators also make use of social media to identify a potential target employee who could potentially break security controls. Such target employees could be those who have been demoted, made redundant or have been dismissed from the organisation. Thus, every HR department needs to be aware of the cybersecurity risks their organisations could potentially face when such matters arise. This is where the HR department should actively ensure that an employee's exit is managed well to deter any potential cyberattacks on these "high-risk" employees.

Strengthening security controls within an organisation can be challenging given that cyberattacks are becoming increasingly difficult to detect. However, with the help of every employee within the organisation, potential cybercrimes can be detected early, mitigated and ultimately prevented.

Gearing up for digital defence – Individuals

In the fight against threats from the digital domain, detection and prevention are key and everyone has a part to play. Singaporeans should keep a lookout for and proactively protect themselves from threats such as phishing and attempted intrusions. They should be aware of ongoing cybersecurity issues and learn how to take personal actions to counter these threats. One example is the use of strong passwords and to ensure that passwords and user IDs are not based on personally identifiable information such as names and birthdates.

Individuals should also practise good cybersecurity habits such as exercising caution and checking for signs of phishing before clicking on unknown links or attachments in suspicious emails, as well as enabling automatic software updates and Two-Factor Authentication (2FA) for online transactions. Other good practices include upgrading antivirus software regularly and obliterating personal financial information in the online public space.

Singaporeans can learn to discern hallmarks of fake or sensationalised reports by checking against credible sources of information such as those of government agencies and official sources. They can also make use of available resources such as Factually **(https://www.gov.sg/factually)** or Scam Alert **(https://scamalert.sg)** to verify news. It is important to develop an understanding of how and why fake news is created and disseminated, and to report on fake news to stop it from spreading.

Singaporeans should recognise that our individual actions have an impact on others in the community. We need to build our digital literacy as individuals and as a community. We can also help friends and family members who need further assistance to learn to use technology safely and confidently. E

Tok Yee Ching | Committee Member | Association of Information Security Professionals (AiSP)

Yee Ching is a PhD Candidate at the Singapore University of Technology and Design (SUTD) under the Information Systems Technology and Design (ISTD) pillar. His research interests include attack detection, digital forensics and Internet of Things (IoT) devices. He volunteers at the Association of Information Security Professionals (AiSP) and is involved in a wide range of AiSP initiatives such as the Cybersecurity Awareness & Advisory Programme (CAAP), Student Volunteer & Recognition Program (SVRP) and the National Cybersecurity R&D Laboratory (NCL).