Trekking in a clear and present danger cyber world

By
BILL CHANG
CEO, Group Enterprise, Singtel

You know that the issue of cyber security is in the spotlight of the business world when regulators make it mandatory for boards to be educated and trained in the area and to also take part in cyber drills so they are better prepared in case of a breach.

Such new requirements are a move following an increasing trend of cyber attacks – which have been cited as one of the top five risks facing economies in the World Economic Forum's Global Risks Report 2016 – across the world.

And the frightening news is these cyberattacks are being carried out in greater sophistication, scale and frequency, while companies are struggling to catch up in understanding the nature of these threats and keeping up with them. Company boards and top management are increasingly recognising that cyber threats are one of the top three risks that their organisations can face and is an issue that no longer sits in the jurisdiction of the chief information officers (CIOs) alone.

From boardroom to ops room

Rather, board directors have to provide the oversight and governance with management in cyber risk assessment as part of their overall enterprise risk management framework.

To be able to do so, boards and the management themselves need to be trained in the areas of

cyber security. Such trainings should therefore be comprehensive and endeavour to cover areas like greater awareness of cyber risks, risk assessments with the decisions and investments made to mitigate them, the on-going review with management (given the very fast pace of cyber threat evolution) on the cyber defence strategy and ensure adequate funding is allocated while reviewing the associated level of risk tolerance.

The training should also help boards and management build a framework to set a culture of cyber security readiness, what to request for periodic updates with management to help evolve their cyber security maturity curve over time.

Beyond training boards and management, it is also key to train their CIOs, CISOs (Chief Information Security Officers) and cyber security operations staff. This is to continuously sharpen their defence skills in the midst of a fast-changing cyber threat landscape.

Additionally, the board should also assess the skills and experience of their bench to ensure they have the adequate digital and cyber talent.

What is encouraging is boards are starting to realise the importance of talent needed to not only help the company leverage digital technologies to accelerate growth and transform their business but also to advise and provide the

key oversight and governance with management in cyber security.

Within and beyond company walls

Today, six out of 10 cyber breaches are a result of internal lapses, which could either be caused by a weak enforcement of policies, employee negligence or involves the latter with malicious intent.

In a recent Singtel-Trustwave survey conducted in Singapore, areas in which lapses can occur include a general lack of security training, unauthorised files transfers and weak passwords, among others (see diagram "Internet threat concerns among Singapore companies"). There is a therefore need for progressive internal user education to be more aware of the "dos and don'ts" in cyber security, otherwise sensitive systems can be seriously compromised.

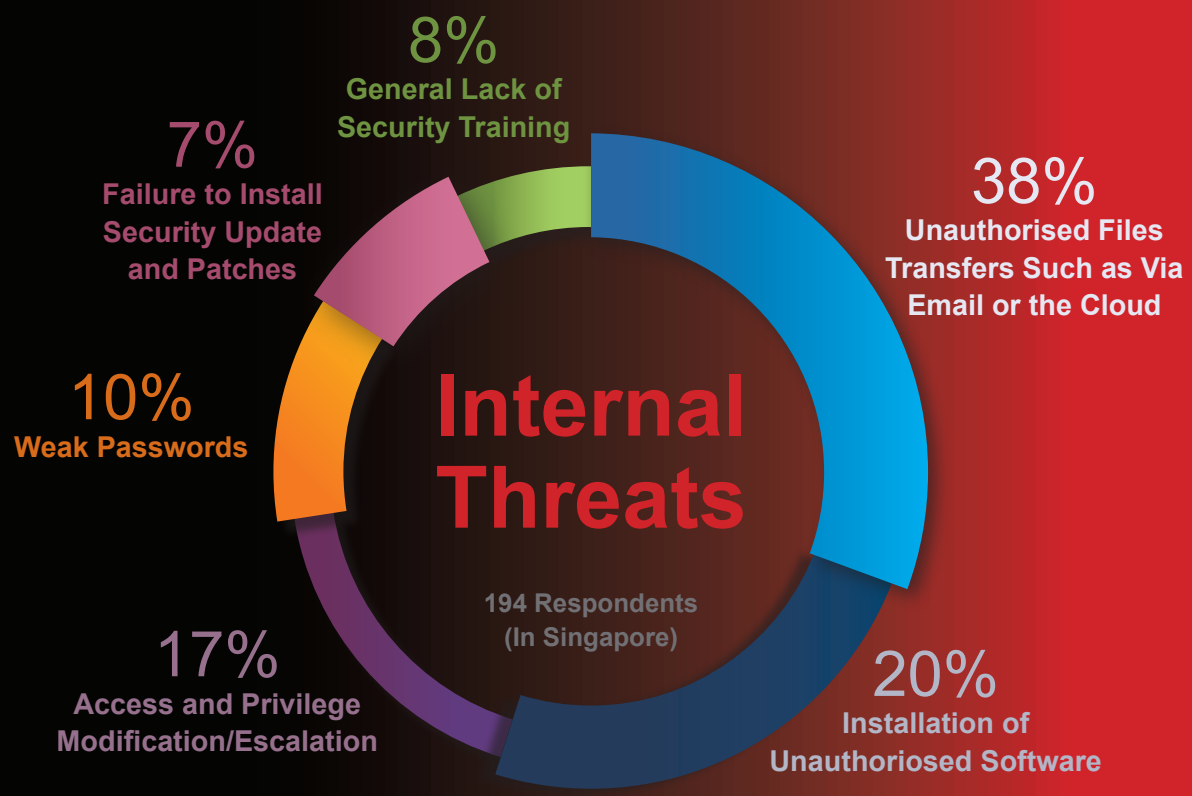
CISOs also have a key role in advising and reviewing with their boards the areas of priority in order to enhance their cyber defences as it would be too costly to defend everything that the enterprise covers.

Companies have to look at their supply chain where cyber risks are at an equal, if not higher chance of occurring, oft-times due to negligence and lapses by contractors and suppliers. The breach by its sub-contractor that cost US retailer, Target, 70 million customer records, is a good example.

Changing mindsets

Beyond awareness, risk assessment and tolerance, boards should also be trained to cover the post breach crisis management and communications process. In many high profile breach cases, the poor handling of post breach

Internal Threat Concerns Among Companies In Singapore



Source: Singtel Trustware Security Pressures Report 2016

crisis management and engagement with stakeholders actually resulted in the destruction of the company's value, loss of trust with customers, even incurred serious probes and penalties from regulators and class action suits from shareholders.

For many companies, the extent of the breach and how it even occurred is often unknown, at least during the initial stages, and this is often made insurmountable when the breach is made public.

Succumbing to the pressure, most companies make the mistake of giving partial or even incorrect information, resulting in further loss of stakeholder confidence.

Boards and management should be trained in the post cyber breach management to develop their protocols, developing their data narrative, even regularly updating and conducting drills between boards and management not with the mindset if a cyber breach would happen but when it will happen.

Cyber talent shortage

The increasing reliance of the world on sharing and exchanging information and operating on the Internet can only mean an accelerated exposure to the clear and present dangers the cyber world has to bring. And when danger mounts, people to protect us from the cyber menace are needed more and more. However, there appears to be a shortage of these "soldiers" to defend us from these invisible enemies. As of 2016, the world is one million short of cyber-trained professionals and this number is set to swell to six million by 2019, according to Forbes.

In Singapore, our total cyber security professionals make up only one per cent of our overall ICT workforce.

This will not be sufficient for Singapore's needs as we strive towards our vision to be a Smart Nation, which will require much higher numbers of cyber security professionals to battle in a number of fronts. Compounding to that challenge, more businesses are also accelerating their digital transformation, which means they will also require more cyber defenders to hold their forts.

Towards this end, the *National Cybersecurity Master Plan 2018* recently announced by Dr Yaacob Ibrahim, Minister of Communications and Information, seeks to grow Singapore's pool of ICT security experts. Some of these initiatives include:

- Promotion of R&D to attract and cultivate more cyber security expertise
- The Company-Led Training Programme for Fresh Professionals by IDA to develop ICT security specialists
- The Singtel Cyber Security Institute to offer holistic training for company boards, management, technology and operations personnel to deal with cyber attacks.
- The Cyber Security for Directors course offered as part of the SID's Business Future series.

So in a very tight cyber talent market globally, it is key that companies invest in the on-going training and development of their boards, management and cyber professionals to better defend themselves and also retain their rare talent.

For companies without the core talent of cyber professionals and have to defend themselves against ongoing cyber threats, they should consider partnering with a managed security service provider (MSSP). In this aspect, they have to consider MSSPs with deep and global capabilities, considering the nature of this global threat phenomenon that we will face for a long time to come.