Accelerate Your Cyber Protection for the Digital Future

Mr Ricky Woo, Convenor, Cyber Security Specialist Group, Hong Kong Computer Society, explained that when he meets clients, their top concerns are learning about cybersecurity and understanding what needs to be done. Since security operations centres (SOCs) must operate 24/7 and the job is very stressful, it is difficult to find good people to operate them.

It is hard to find new vulnerabilities, so PwC forms red, purple and blue teams to try to hack each other and learn each other's tricks every two weeks. The red team focuses on offensive security, exploiting vulnerabilities, penetration, and web apps scanning, whereas the purple team tries to improve detection and defence, sharpening the skills of blue and red team members, and spot-checking systems in larger organisations. The blue team focuses on defensive security, infrastructure protection, damage control incident response, operational security, threat hunting and digital forensics.

There are many security tools available, but they are expensive and clients still wonder if they are secure, because they usually don't understand what each tool covers. Some are specialised and have different functionalities, so they don't cover all areas, and most of them focus on responding to threats, not predicting them.

A major problem now is the talent gap, Mr Woo said, with an estimated global talent gap of over four million cybersecurity specialists. Sixty-four per cent of this gap is in APAC, according to the 2019 ISC Workforce Study. Some 65 per cent of organisations have a shortage of staff dedicated to cybersecurity, and 51 per cent of cybersecurity professionals say their organisation is at moderate or extreme risk because of the cybersecurity staff shortage.

Engaging professional consultants to provide a managed security service is the best solution, as they can provide a fresh, unbiased perspective on security issues in the organisation. Since they can focus solely on the security issues of the company, companies benefit from their experience in the industry, and they can provide benchmarking to help companies understand where they are and what they need to do next.

Management support is key to developing a good cybersecurity strategy. Top management must be committed to cybersecurity, and recognise the importance of upskilling and retention. Cross-field development can help, Mr Woo concluded, since about 30 per cent of people in cybersecurity are from non-IT or engineering fields, proving that tech skills can be acquired on the job.

Companies must develop effective retention strategies by providing opportunities for staff to develop skills, supporting flexible work arrangements, reinforcing value, and regularly reviewing and benchmarking the salary scheme.

Mr Felix Kan, Partner, Cybersecurity & Privacy, PwC Hong Kong; Co-founder, DarkLab, discussed the results of a survey on priority and investment focus in various cybersecurity domains. The primary focus of most organisations is response and recovery, followed by protection, then detection, and finally

identification. Hackers can get into anything, he said, just as a thief can. They can get into a company's system through an old system, for example, that does not have up-to-date security.

There must be a balance between digital transformation and cybersecurity, maximising data security while minimising attack opportunities and the data footprint. Companies must make security part of their brand, like banks that provide a token which gives customers a sense of security for online banking.

Complete cybersecurity requires a mindset, Mr Kan said, involving capability (buying the tools and building an IT team), and maturity (merging the tools appropriately to protect the data owner). The controls include firewall and antivirus protection, keeping software patches up to date, and ensuring a secure approval system. A good defence strategy is intelligence led, involving layers of defence, and awareness of attack techniques and tactics. Some 90 per cent of attacks involve leaks of user names and passwords.

The PwC DarkLab team staged a live hacking demonstration and incident-response simulation showing the intricacies of the hacking mindset and how a strong cyber defence can protect against attacks. Both the attacker's and the victim's screens were visible to the audience. The attackers conducted a spear-phishing attack, which involves stealing sensitive information such as account credentials or financial information. If attackers get into a computer — through a downloaded Excel file, for example — they have access to all its files and can see everything the victim does on the screen. However, there is a lot administrators can do, Mr Kan explained, such as keeping a whitelist of administrator accounts, so that if there is a change they know something is wrong, and making a list of all software so that they see if something new has been installed.

Ransomware attacks involving encrypting a victim's files with a password and demanding a ransom for the password to access the files were very common in 2019, Mr Kan said.

The key questions PwC's MITRE-enabled Security Operations Centre ask are (1) how promptly the IT team can detect an attack, (2) how many attack techniques it misses, and (3) how long it takes to achieve security posture. Automation and orchestration are the way forward, Mr Kan concluded.