NOTEBOOK

New technologies, new risks

L to R: Mr Jonathan Ranger, Prof Shaun Wang, Mr Paul Hadjy and Mr Doug Witschi.

Cyber attacks are a constant worry for organisation and insurers, with the number of attacks growing and becoming more sophisticated every day. Many experts now encourage becoming resilient instead of trying to achieve the impossible status of 'hack-proof', but what does resilience actually mean? A number of experts chimed in with their thoughts during the 4th Asia Cyber Risk Summit.

By Ahmad Zaki

According to Aon's recent risk management survey, cyber risk is seventh on the list in the APAC region. With cyber attacks steadily on the rise, it becomes a question of when you get attacked, not if. It is then wiser to be able to recover from a breach or ransomware attack faster and more effectively, instead of trying to prevent the attack from occurring in the first place.


Mr Manan Qureshi

"A comprehensive and cohesive paradigm of security across your entire business is the best chance of survival," said IBM APAC head of cyber security strategy Manan Qureshi, during the 4th Asia Cyber Risk Summit.

Cyber resilience requires a three-dimensional approach, he said. "Many organisations, especially in the financial sector, have a multitude of departments – IT, business continuity, disaster recovery, information security, risk – all of which have various regulatory and risk landscapes that govern them. So, to be able to appreciate the multi-dimensionality of resilience, the solution needs to encapsulate this complexity. This solution does not exist at the moment, although it is something many organisations are aiming for."

One important step that needs to be taken is to move away from silos and become a harmonised organisation. These silos might not talk to each other in a unified language, he said. "These departments have overlapping regulatory landscapes, operating models and standards to adhere to. They already have commonalities and a shared language, but what happens in reality is that they do not talk to each other that well."

Protecting your data


Mr Andrew Shepherd

New threats are appearing all the time, and new responses are required, said Charles Taylor Adjusting head of cyber Andrew Shepherd. And in order to create the correct response to a cyber incident, a laundry list of diagnostic questions need to be answered: "What sort of hardware is in your system? What kind of software are you using? Is it still being supported and still current? What type of data are you storing and where is it being stored?" he said.

In the case of data theft, knowing where the data was stored is highly important, as it determines the steps needed to recover said data. "You also need to understand precisely the type of data you have and how sensitive it is,

how to look after it and how not to lose it."

With the implementation of GDPR and similar data privacy regulations, safeguarding data becomes a board-level responsibility and no longer just the purview of the IT team. This includes knowing how well the information security protocols in your organisation can handle an attack, whether simple or complex, and taking measures to protect the asset that is your data. "Is your data offsite, or is it in the cloud? How often do you backup your data and how quickly can you restore it if you lose it?" said Mr Shepherd.

Evolving nature of cyber threats


Mr Alberto Pelliccione

By now, everyone recognises that cyber attacks typically come from opening suspect emails and downloading attachments that have malware embedded into them. However, ReaQta founder and CEO Alberto Pelliccione pointed out that a new trend is of the increasing popularity of fileless attacks. "Basically the attacks are now embedded into our infrastructure, unlike software attacks, which come from outside," he said.

Fileless malware hijacks tools inbuilt into operating systems and uses those tools to carry out attacks. This means that there is no signature for antivirus programmes to detect, increasing the possibility of the network being hacked. According to Mr Pelliccione, 53% of all attacks that ReaQta detects are completely fileless.

Further, malicious actors have begun to change the way they operate. Consumers are attacked less often, as the profit margins are lower. This means a corresponding increase in enterprise targets, with the attacks becoming more targeted and sophisticated. Attacks are also less 'noisy' and harder to detect, mainly due to the rise in fileless 'in-memory' malware.

New technology means new vulnerabilities

It is estimated that the spending towards smart cities, IoT and technology infrastructure will rise into the trillions within the next decade. "There are currently about 6-12bn IoT devices estimated to be out in the world today, compared to the 7.5bn people on the planet," said KPMG cyber security consulting director Dr Paul Lothian.


Dr Paul Lothian

What this means is that alongside the legacy cyber security risks an organisation must implement and manage – such as technology controls on a user's email systems to minimise user error – they also have to contend with the transformation that the world is undergoing and the new risks that are being introduced with that transformation.

For example, blockchain or distributed ledger technology has grown in popularity to provide security for transactions and all the data that is involved. The technology generally works by digitally signing off on transactions to verify its authenticity, but malicious actors will then go after unprotected keys and signatures, said Dr Lothian. "The implementation of the blockchain matters as well. Blockchain is a software that interacts with your mobile and the cloud, but like with any piece of software, it requires a platform. So, if you don't implement it on a proper platform that has been hardened, then it becomes a weak link for the bad guys to go after."


Mr Paul Hadjy

Horangi Cyber Security CEO and founder Paul Hadjy added that it is a fallacy that most organisations believe security is the sole responsibility of the service provider. "It is a shared responsibility and while service providers are responsible for some things, you are responsible for the configuration and ensuring that things are done in a secure manner."

Underwriting challenges

"We are now underwriting in a climate where there is a steep increase in the frequency and severity of cyber related losses. Events such as Wannacry, Petya and NotPetya have illustrated that the resulting economic loss combined are estimated in the billions raising concerns over the adequacy and willingness of available insurance from traditional markets to cover such losses," said AGCS head of financial lines Singapore Jenny Wilhelm.


Ms Jenny Wilhelm

The spectre of aggregation is real on multiple levels, she said. On one level a cyber event can potentially trigger numerous policies; a commonly cited example is an attack on a cloud service provider which then could cause business interruption losses for multiple policyholders in an insurer's portfolio. On another level a direct attack on one customer could trigger a loss across multiple product lines, in addition to a dedicated cyber policy.

Alongside silent cyber – unintended coverage arising from a cyber event outside of dedicated cyber insurance policies – there is the issue of data deficiency. Insurers are underwriting and pricing risks based on a relatively short history of actual loss experience, particularly in Asia where the cyber insurance market is still in the early stages of development.

In the Asian market, there has been an emergence of a segmented underwriting approach for cyber insurance. Some insurers are clearly leaning toward the small business segment, with typical offerings being more standardised and aimed at higher volume of transactions.

The process of applying for cover and receiving quotations is likely to be more automated and cover for SMEs are more restrictive, with lower limits. There is also less willingness to provide tailored solutions outside of the standard forms.

However, the market continues to have a broad appetite and are underwriting cyber across all customer segments and industries, Ms Wilhelm said.

The 4th Asia Cyber Risk Summit was organised by *Asia Insurance Review* and was sponsored by Singapore Re and Horangi Cyber Security.