INSIGHTS – CYBER

Risk management across supply chain vital to cyber defence

(L-R): Ms Caitríona Heinl, Professor Shaun Wang, Mr Ashish Thapar & Mr Vincent J Loy.

The interconnected and unbounded nature of the cyber means that each company is vulnerable to risks from each partner in the ecosystem. Cyber security requires a collaborative effort supported by information sharing, said speakers at the 2nd Asia Cyber Risk Summit organised by *Asia Insurance Review*.

By Chia Wan Fen

"A lot of companies spent a lot of money to strengthen their own four walls, but collectively, society is not winning the cyber war," said Professor Shaun Wang of the Insurance Risk and Finance Research Centre, Nanyang Business School, Nanyang Technological University, Singapore. However, it is still not an end of the world scenario, he reassured the audience. He believes a collaborative approach is the way to build a resilient digital ecosystem.

Checking on partners


Mr Geoff Leeming

Mr Geoff Leeming, Ex-CISO, Founder & Consultant, Pragma Strategy, noted from headline cases of cyber attacks that many risks were found to be from a vendor, contractor and other third-parties rather than the main company which was the victim. Thus, companies need security in the entire supply chain and ecosystem.

He showed that it is possible for a CISO or risk manager to build a simple rating of their partners' cyber security and thereby prioritise the company's cyber security investments.

Examples of information to be garnered from the Internet, corporate disclosures and announcements can include technical data exposed to attack, the size of the security team, security standards achieved and willingness to invest in security solutions. These can help a firm's decisions in triage of third party risk management and expenditure.

SMEs more vulnerable

Advising that 61% of data breach victims are businesses with fewer than 1,000 employees, Mr Ashish Thapar, Managing Principal – Investigative Response at Verizon Enterprise Solutions, said SMEs could lead cyber criminals to larger organisations, given trends like outsourcing. He noted that SMEs also invest less in cybersecurity and do not protect themselves well.

Mr Vincent Loy, PWC's Asia-Pacific Financial Crime & Cyber and Data Analytics Leader said big corporations have a responsibility to put pressure on their supply chains in order to get them tuned into cyber risk and improve their resilience against cyber threats.

He concurred with Professor Wang that one way to be prepared for cyber threats is a collaborative approach. Noting that the financial industry has traditionally regarded its information as trade secrets, he said in this new world, the more that is shared across the industry, the better. In his view, staff today also do not share sufficient information within the company, such as alerting their Chief Information Security Officer (CISO) of potential threats.

CyRiM

Endeavouring to get more data as well as fostering an efficient cyber risks insurance marketplace is a Public-Private research partnership between the insurance industry, academia and the Singapore government launched last year called CyRiM.

Providing an update, Prof Wang said that researchers are now collecting data on cyber incidents. Eventually, the scenarios will help in impact quantification and study of accumulation risk in systemic events.

CyRiM's findings could also help achieve a cost-effective way of calculating cyber risk as well as help insurers design suitable and relevant cyber products, he said. With these products, this would help cyber insurance business grow, he added.

"Silent" cyber risks


Mr Victor Kuk

Another cyber threat is "silent" cyber risks. Mr Victor Kuk, Head Hub Casualty Asia, Swiss Re, said silent cyber risks are on the rise with ever-growing digital transformation and interconnectivity and urged companies not to neglect this threat.

Dedicated, comprehensive cyber products cover "affirmative" or explicit cyber risks, while "silent" cyber risks exist when traditional policies which were not designed to cover cyber do not have explicit cyber exclusions. This means insurers could end up "silently" covering losses caused by cyber perils. For instance, criminals, via connected entities, could possibly cause remote car accidents and even shut down critical medical systems. The consequences could be subject to traditional liability claims.


Mr Ashish Jain

Mr Ashish Jain, Vice President & Managing Director of modelling firm AIR Worldwide in Singapore, also shared the view that it is prudent to evaluate cyber loss potential across various business lines. Silent risks and associated policy wordings remain relatively untested in court so far, as cyber remains an evolving peril with much uncertainty in coverage, he said.

Mr Jain also cited other trends which impact cyber coverage. For example, companies moving to the cloud could result in some risk aggregation because a handful of providers have currently captured a significant share of the market. When a single provider is down, a cyber catastrophe could occur where multiple companies close down. Meanwhile, storage of data on devices and transferring data do have their own vulnerabilities too, he said.

> **"Silent" cyber risks exist when traditional policies which were not designed to cover cyber do not have explicit cyber exclusions. This means insurers could end up "silently" covering losses caused by cyber perils.**

Blockchain and biometrics


Mr David Piesse

When an organisation is breached, data integrity, more so than destruction or theft of data should be the main worry, said Mr David Piesse, Advisory Board Member of Guardtime.

This is especially so in APAC, where the long time (520 days according to industry research) between discovery and compromise or no discovery at all is very attractive to criminals. Credit card fraud results in an alert for the user, who could simply change the card, but medical information like blood type can be exploited for a long time, and cannot be changed subsequently to protect the user in future.

Blockchain implementation, which is up and coming, is a measure that could strengthen cyber security and data integrity in an organisation, said Mr Piesse. The distributed database maintains a continuously growing audit trail of data records that are hardened against tampering and revision.

Blockchain also helps in the use of autonomous devices in that the owner of the device and data provenance will be identified. As such, it could offer protection across the data supply chain.

Besides blockchain, some speakers suggested that organisations could move away from over-reliance on passwords. Mr Thapar advised organisations to implement two or even multi-factor authentication. After all, once a key logger is installed in a machine, it no longer matters that a password is strong, complex or has many characters, he said.


Mr Walter Lee

Echoing this view was Mr Walter Lee, Head, Innovation Management Office, Global Safety Division, NEC Corporation. He noted that biometric indicators are the up and coming method of identifying a person for online transactions and processes. For example, fingerprints will soon become a mainstream mode of payment.

Vigilance


Mr Luke Forsyth

In cyber risks, the human factor to detect threats still plays an important role and CIOs should support their staff in being cyber vigilant, noted Mr Luke Forsyth, Principal, Cybersecurity, KPMG in Singapore. He said it is very important to encourage people to speak up even if they are not confident of what they detected—it is better to have multiple incidents reported and only one being real as opposed to having one that goes unreported.

Mr Forsyth concluded: "It doesn't matter how good your cyber security defences are. If you have systems linking through one of your key suppliers, they can introduce risk to your organisations. If they are critical suppliers, like telecommunications, your ability to continue to operate is only as good as their cybersecurity defences. Thus risk management through the supply chain is becoming increasingly important."

The 2nd Asia Cyber Risk Summit was organised by *Asia Insurance Review* and sponsored by Singapore Re.