Cyber at War

The nature of conflict has changed, with cyber attacks often preceding military intervention. Is this a change brought about by the current ongoing conflicts around the world, or a natural extension of the cyber landscape as it permeates our lives? And how can we learn and adapt to best defend our organisations? GNGB sat down with three experts at a round-table last month, to find out.

Tommy Viljoen
Tommy is a Partner in the Australian Cyber Risk Services Strategy and Governance team and is based in Sydney. Tommy has close to 30 years of experience in Information Technology, IT Risk and Cyber Security and Governance specialising in financial services. He has help to build the Deloitte Cyber practice to one of the largest in the country. Tommy is at the forefront of delivering management, design, development and implementation solutions to clients manage and mitigate cyber security and privacy challenges. Tommy has assisted many financial institutions develop and implement their cyber security strategies, including in some of the largest banks in the country.

Professor Alex Frino
Alex is a distinguished financial economist who fosters the interaction of business with academe. He is an alumnus of UOW and Cambridge University. He was recently awarded a second Fulbright Scholarship to investigate how companies can protect themselves against cyber crime. He is one of the best published financial economists in the world with over 100 papers in leading scholarly journals. He has won over $10 million in competitive research funding and is frequently cited in the global press.

Evan Carvouni
Evan is a Partner in the Cyber Risk Practice and leads Deloitte's Cyber 'detect and respond' managed service business in Australia. He has 18+ years experience in cyber security and has worked for some of the world's largest banks, systems integrators and consultancies across the UK and Australia and has experience leading major cyber transformation programs. Evan has been at the forefront of helping some of Australia's iconic organisations manage serious cyber incidents and recover from ransomware and other cyber attacks.

The only way is up

While cyber attacks are increasing overall, the Ukraine conflict has not led to an uptick in frequency of attack on Australian organisations – possibly because cyber criminals are busy in their own backyards. The long term trajectory, however, is up. So is the complexity of the software cyber criminals are using, as well as the speed at which it's being released. This is resulting in more frequent zero-day vulnerabilities, with log4j a recent example.

Overseas, there is obviously a lot of increased activity around the conflict. Russian military groups kicked off with disruptive DDOS attacks to try to make it difficult for Ukraine to coordinate their response. This was followed by Wiper malware attacks on Ukranian government departments, rendering their systems unable to operate. The most interesting and concerning attack, however, was on the ViaSat satellite network, where the modems on the ground were wiped. This meant internet access for parts of Ukraine was disrupted, but the bigger outcome was the unintended consequences. Ukraine is not the only user of ViaSat – in Germany, 5,800 wind turbines using this network went down. This attack was one of the first examples of conflict spilling over and impacting other nations.

Cyber criminals themselves are impacted – in some instances, cyber crime organisations have even fractured, as previous colleagues have found themselves on opposite sides of the ideological fence.

Heigh ho, it's off to work we go

Cyber crime organisations continue to invest in their businesses, which are far more organised and professional than most people realise. These highly profitable operations are structured just like legitimate organisations – the Conti ransomware group, for example, which recently had several

years of internal chat dialogue leaked, has over 100 salaried employees, an HR department, a talent acquisition team, and developer and testing teams[1]. The business of cyber crime has low barriers to entry, low potential for getting caught, and very high profit margins, therefore groups like Conti continue to proliferate and mature.

Money money money

The cost of successful cyber attacks remains high for organisations that fall victim to them. There are two types of cost – out of pocket costs, which are remediation costs and may include class action suits and regulatory fines; and reputation cost – how the cyber incident will impact the way an organisation's customers see it, interact with it and potentially choose not to deal with it any more. Professor Alex Frino's research shows that public companies in the US that experience a successful cyber attack will permanently lose around 1% of their value, while Australian organisations will lose 4.5% - both very worrying numbers. An interesting trend is that the cost to companies is trending down over time – so even as the sophistication and frequency of attacks rises, the cost to companies is falling – but it remains very significant.

Secrets

Another interesting insight from Professor Frino's research is that, despite continuous disclosure rules that insist public companies must disclose any information likely to materially impact their stock prices, companies rarely disclose cyber attacks. Of the 40 Australian attacks Professor Frino's team reviewed, only six were reported to the appropriate regulatory authorities. This trend is mirrored in US data, suggesting more prescriptive regulation is needed to protect shareholders from the flow-on effects of malicious cyber activity.

Stop, collaborate and listen

Frino's research, which will eventually cover all NATO member countries, is designed to quantify the cost of cyber crime and inform policy around an appropriate level of investment in cyber security. NATO is a particularly interesting case, because Article 5 in the NATO treaty outlines that an armed attack on a NATO country is an armed attack on all NATO nations, and NATO have stated publicly that cyber attacks are included in the definition[2]. At the moment it's unclear at what level of attack a response would be triggered, but it's clear that cyber is considered a weapon of war, and that a collective NATO response may be appropriate in the future.

For NATO – or any industry or group – to defend themselves against cyber attacks, collaboration is critical. Cyber criminals infiltrate the weakest link in any system and expand their efforts from there, so any group is only as strong as the weakest member. By collectively working to close security gaps, the whole ecosystem in strengthened.

In Australia, ASD and ASIO have flipped their approach to threat sharing from a culture of secrecy a decade ago, to a focus on building capacity to share and push out threat information as fast as possible. Industry groups, including GNGB, are building capacity for industry members to work together to share threats and mitigations as quickly as possible when attacks occur.

[1] https://krebsonsecurity.com/2022/03/conti-ransomware-group-diaries-part-i-evasion/ https://krebsonsecurity.com/2022/03/conti-ransomware-group-diaries-part-ii-the-office/

[2] https://www.reuters.com/world/europe/cyberattack-nato-could-trigger-collective-defence-clause-official-2022-02-28/

Taking care of business

According to Deloitte, there is still some complacency in Australian organisations that have not yet taken the initiative to boost cyber resilience. Where companies don't have the basics in place, such as patching and hardening internet-facing systems, they are very vulnerable to attack. In fact this is how the ViaSat attack happened – through a misconfigured VPN service[3].

Having visibility of what's going on inside the organisation is critical, as well as knowing what to do about issues as they arise. Ensuring the appropriate agents are on the servers for monitoring purposes; identifying which apps are not patched, and the ability to patch at speed are crucial. During log4j, Deloitte saw patching at speed as a key point of failure for many companies.

During an attack, the last thing a company should be doing is discovery. Having automated systems that show the status of systems and patching in realtime is one of the best ways to defend against a future cyber incident.

Phishing and spearphishing attacks, which rely on human fallibility, are also becoming more common, and more sophisticated. Here, organisations must rely on the training and security awareness of users. Continually educating employees not to click on links, but to verify the source, is key. Another big challenge here is logging and detection – many organisations either don't have logs centrally collected for analysis, or don't have logging and audit policies configured to capture the right information.

Finally, exercising incident response plans is one of the best ways to prepare for cyber attacks and minimise recovery time. Deloitte's experience shows that most businesses' business continuity and disaster recovery plans are insufficient to manage a serious ransomware attack. These types of attacks hit on multiple fronts at the same time, so diligently working out how the company will recover when systems are down, communications are unavailable and people are stressed will mean higher resilience if a real attack strikes. The exercises should be based on realistic scenarios, developed from real-world intelligence, and take into account that there may be weeks of recovery work involved and that people will quickly become exhausted, so spreading the burden of responsibility to get through the crisis is an important point of consideration.

[3] https://www.viasat.com/about/newsroom/blog/ka-sat-network-cyber-attack-overview/