SWIFT Institute: Cyber Security 3.0 – Better Together

On Friday 18 August the SWIFT Institute, in partnership with Nanyang Technological University, hosted its second cyber security event of the year. The aim was to share new research, and bring together cyber experts from academia and the financial industry.

Alain Raes, SWIFT Chief Executive for APAC and EMEA opened the conference underlining the importance of collaboration, and the responsibility of industry to manage cyber security risk, particularly in light of unprecedented levels of innovation. The cost of cyber attacks is estimated at USD 1.4 trillion in 2016. He drew parallels to Babylon – which in ancient civilisation had a population of up to 200,000 people; ground breaking at that time but with inherent risks such as disease, but which was ultimately successful – underlining the importance of not disconnecting, and working together.

Alain highlighted steps SWIFT has been taking to play a part in this collaboration, including basic hygiene measures to protect the banking environment through SWIFT's customer security controls – encompassing 16 security measures; counterparty payment controls; and information sharing. He also highlighted how the cybersecurity risk is increased with the disruption driven by the region's FinTech giants.

Will Carter, Deputy Director of the Technology Policy Program at the Centre for Strategic and International Studies, gave a comprehensive overview of the forces shaping the next generation of attacks. He highlighted that investment was not keeping up with attacks, and that there is a new generation of attackers, launching massive co-ordinated attacks at scale across the industry. He considered the forces shaping the threat landscape examining the attack surface, attacker incentives and new defences. The attack surface is generally wider than the defender's narrow view of a computer – take for example the Internet of Things and mobile banking, which are providing new access points for cyber attackers and changing the geography of cybercrime. Financial cybercrime is growing rapidly in developing nations, driven by the proliferation of mobile banking. Attack incentives are changing as the nature of threat actors has changed. Attackers are in countries where it is typically hard to enforce laws against cybercrime, and we are seeing nation state actors robbing banks. There is a wide availability of tools for attackers available on the dark web, and law enforcement is struggling to keep up, particularly given the cross border nature of attacks. New defences are being developed, but attackers are adapting as well – including developing new strategies for social engineering to compromise bank employees and launching attacks which make fraudulent transactions appear legitimate to evade new fraud prevention measures. Attacks are taking a hybrid nature – for example, DDoS attacks are increasingly used as a cover for other forms of attack happening in parallel. Will emphasised the importance of a collaborative ecosystem to combat these attacks. An audience discussion emphasised the importance of cyber attacks being treated as a strategic business issue and not just a technology issue – a theme elaborated further during the panel discussion.

Casey Evans, from the American University's Kogod School of Business then gave an overview of an approach to share insider threat indicators, leveraging SWIFT's messaging platform to combat cyber attacks. Casey highlighted that the growth in cyber attacks requires a new approach to defences, as highlighted by Will. The cyber landscape has diversified – in particular the scope and nature of attacks. She highlighted that it takes on average 146 days to detect a sophisticated attack. She also highlighted that Singapore came top of the UN Cybersecurity index, with Malaysia coming third. Casey provided an overview of a tool to facilitate sharing cyber attack information using the SWIFT messaging platform. Based on research on intelligence failings of the 9/11 attacks, key findings were

the importance of having in place a centralised management system, a uniform system to transmit and cultural support for the sharing of information. Casey's team considered intelligence sharing tools and suspicious activity reports to develop a tool for sharing cyber threat/attack information. They also considered FS-ISAC information sharing platforms, which was not chosen as it is a one to many broadcast rather than a secured one-to-one communication. Their proposed tool has been developed to collect cyber attack information based on insiders, which can potentially be disseminated over the SWIFT network. It includes an assessment of defined threat indicators relevant to the threat/attacks. The legal consequences of sharing this information have been considered from a US law perspective, including privacy and monitoring of employees. Saqib Sheikh, Head of Sales Services Asia Pacific at SWIFT then gave an overview of the innovation and steps being taken at SWIFT to mitigate cyber risk, and the dissemination of this approach amongst SWIFT's members across the region.

Tim Maurer from the Carnegie Endowment for International Peace then gave an overview of the importance of collaboration for cyber security risk at the international level – and the commitments that the G20 have made in respect of G20 members collaborating in respect of cyber risk. He considered the success of an agreement between China and the US at presidential level to prevent cyber enabled theft of IP, and as a result the number of these thefts has decreased. He discussed how hacking can impact financial stability. The G20 Finance Ministers have recognised that there is a real risk to the financial community at large regarding cyber attacks. Based on these concerns, the Carnegie Endowment has proposed an international agreement to be agreed at the G20 level with states committing not to conduct any activity that manipulates the integrity of financial institution's data and algorithms or undermines the availability of critical systems.

There was a panel discussion on how to collaborate to prevent cyber attacks, led by Caitriona Heinl, Research Fellow, Cyber Policy & Strategy, Nanyang Business School. The panellists included Roy Wilmoth, Head of Liabilities and Financial Lines, AIG Asia Pacific Insurance Pte Ltd; David Leach, CISO, APAC at J.P. Morgan; David Ng, Head of Singapore Technology Information Security Office at OCBC Bank; and Saqib Sheikh, Head of Sales Services, Asia Pacific, SWIFT.

Topics discussed included the sharing of intelligence. The panel touched on the reluctance to share intelligence due to brand and reputational concerns, but how events have driven some banks to share intelligence, precipitating greater co-operation. It was highlighted that regulatory frameworks have limited the ability of institutions to share intelligence, which is a barrier. Lack of harmonisation of different laws across markets compounds this issue. The importance of identifying the weakest link in the value supply chains was emphasised, and the need for collaboration to address these risks. The unintended consequences of going after bad actors were highlighted, as they may increase the levels of attacks. The panel recognised that cyber risk is not a technology problem, but a business problem – and the importance of cyber audits and Board training. The importance of industry collaboration was emphasised, as well as internal, although some panellists did not see internal silos as an issue. Cyber risk is not mitigated solely by technology controls, but also requires organisational and process controls. The tone has to come from the top, and be cascaded through the organisation. The panel discussed facilitating collaboration through an industry wide table top exercise, in conjunction with regulators. They reflected that the financial services industry has demonstrated in the past that it comes together well during a crisis.

The final session featured new research findings of the NTU Singapore Cyber Risk Management project (CyRiM), moderated by Caitriona Heinl, and presented by Professor

Shaun Wang, Director of the Cyber Risk Management Project, Nanyang Business School, and Professor Lam Kwok Yan, School of Computer Science and Engineering, College of Engineering, NTU. The project is a government-industry-academia research endeavour supported by the Monetary Authority of Singapore, the Cyber Security Agency of Singapore, a number of leading global insurers and the Geneva Association. The project aims to examine how the effective adoption of cyber insurance can enhance cyber resilience. Its goal is to develop a valuation framework combining business and technology, addressing multi-faceted risks, using analytical models to quantify cyber risk and determine optimal level and allocation of cyber security investment. This framework will provide stronger measurement and indicators to support better foundations for public policy. A four-dimensional valuation model for cyber risk was presented. The four dimensions are (1) the level of security investment to address vulnerabilities – increase of spend reduces vulnerabilities but the rate of improvement declines after a certain level of spend; (2) the effect of private sector collective spending to contain the growing number of threats such as proliferation of malware in the dark web and organized cybercrime; (3) how timely response can reduce the impact of cyber breach; (4) ensuring a baseline cybersecurity posture to increase the cyber security of the whole business network. Using this framework, a strong case is made for coordination and collaboration within the financial sector internationally, and the synergy for the first-layer of cyber security defence measures and the second-layer of cyber insurance protection.

Stella Cramer, a partner at Norton Rose Fulbright Singapore and a member of the Advisory Council of the SWIFT Institute, closed the conference by highlighting key themes of the day, and provided an overview of what cyber legal practitioners are seeing across the region. A key theme was the importance of collaboration to battle cyber threats, at the government level, the industry level and internally within organisations. Cultural changes were required to ensure the sharing of information in the post 9/11 intelligence world, and lessons from that incident set a benchmark for developing information sharing tools and processes in other realms – including cyber. The risk of cyber threats is compounded in emerging market economies, where FinTech giants have disrupted the provision of financial services to the unbanked by leveraging technology in China, and as these giants internationalise and bring disruption to other markets in Asia – the risk of cyber attacks will increase. Stella provided an overview of data supporting the increase of attacks in Asia, and considered some of the results from the latest Ponemon Institute's "Cost of Data Breach Study: Global Analysis 2017", in particular the increase of cost of breach for financial services, and how some of the tools discussed at the conference can bring down the cost of breach – in particular threat sharing and cyber insurance. Stella highlighted that the number of patents being filed by financial institutions in respect of cyber and FinTech has increased by 83% since 2013. The use of cyber insurance is increasingly prevalent. Stella noted an uptick in Asia of insureds relying on cyber insurance, particularly with the recent WannaCry and NoPetya attacks. In summarising the new wave of cyber laws across the region, she drew parallels to the wave of data protection laws implemented across the region 4 to 5 years ago. Singapore is at the forefront – it leads the UN Cybersecurity Index, and has recently published a consultation on a new Cybersecurity Law. Stella closed on the lack of harmonisation across the region and different motives by legislators for imposing the new requirements, increasing the complexity of the cyber landscape across the region. At an industry and a national level, we are making progress, but there is still work to be done.

- End -