SWIFT Institute: Cyber Security 3.0 – Better Together

In ancient Mesopotamia, Babylon's population is estimated to have reached more than 200,000 – the first known example of large numbers of people living in close proximity with one another. It was very nearly a colossal failure. Cities quickly became breeding grounds for infectious diseases and epidemics that threatened to wipe out mankind. But for the rise of basic hygiene, vaccines and medication, the earliest city dwellers might well have been forced to disband the experiment altogether.

This was the analogy drawn by SWIFT chief executive officer Gottfried Leibbrandt at the start of the SWIFT Institute conference, *Cyber Security 3.0 – Better Together*, held in London on 30 March. There is no doubt that cyber-attack has become the great existential threat of our age, compromising the online existence of companies and individuals alike. But just as in ancient Babylon, a combination of basic hygiene and detection measures can and are being used to manage and reduce the threat.

During a programme that comprised three academic research presentations and a practitioner panel discussion, delegates were given detailed insight into the evolution of both the threat landscape and the defence mechanisms being employed across the financial services industry today.

In the first presentation, delivered by William Carter, associate director at the Washington-based Centre for Strategic and International Studies (CSIS), the full scale of the threat was laid bare. The global cost of cybercrime was estimated at more than $400 billion per year in a 2014 CSIS study, while the value of the cybersecurity market in 2017 is estimated at just $81.6 billion. Meanwhile the UN estimated in 2013 that as much as 17% of the online population are victims of cyber-crime and digital theft each year, whereas just 5% of the population are victims of physical crime.

The statistics clearly show this to be a rapidly growing problem that is not yet being effectively combated, but some of the underlying trends are even more concerning. The growth of mobile banking, particularly in the developing world, has multiplied the number of potential points of attack, increasing the vulnerability of the sector. The Internet of Things is connecting more and more everyday devices such as fridges and ovens, all of which can be used to launch cyber-attacks in ways that had never previously been anticipated.

The geography of cyber-crime is also evolving, with cybercriminals increasingly launching attacks from and targeting banks in the developing world. Banks in Asia have become a prime target as criminals can take advantage of comparatively weak regulatory environment and security practices.

Infrastructure development in the developing world has led to significant growth in digital banking in Africa, Latin America, and developing Asia, and has also fuelled the growth of a cybercrime economy in these regions. Brazil, in particular, has become a hotbed of digital fraud. This is driven in part by the World Cup in 2014 and the Olympic Games in 2016, which brought many wealthy tourists to the country, but also by the growth of digital banking among Brazilians – an estimated 45% of banking transactions in Brazil are digital.

Attacker incentives are also evolving, Carter explained. The nation-state threat to financial institutions is growing again, and is motivated either by pure financial gain, or political gain by countries that might seek to influence their adversaries by threatening the financial system.

Criminal groups are also becoming increasingly organized and sophisticated, and capabilities that were once exclusive to nation-states are becoming the norm in the high-tier criminal market. Much of this growth is driven by the overlap and intermingling between nation-state hackers and cybercriminal organizations. For example, in some countries criminal groups are often comprised of former hackers from military and intelligence agencies, and many continue to operate as proxies for their government.

Law enforcement, meanwhile, is struggling to keep up with attackers in cyberspace, hampered by limited resources, lack of clear authorities and established procedures to investigate and prosecute cybercrime, and cross-border challenges that make it difficult to share evidence and arrest criminals operating transnationally. Cybercrime is also underreported, as many victims fear reputational or regulatory repercussions from admitting they've been attacked.

In the second research presentation, the focus shifted towards individual institutions and their customers, as Visiting Professor Richard Benham of Coventry University Business School and Dr Jason Ferdinand of ISKM Ltd delivered the findings of their research. Their work builds on an Institute of Directors survey of 1000 business leaders, which showed 95% of businesses consider cyber security to be important, but 45% do not have a formal strategy in place.

Surveying 67 individuals across a range of sectors, Benham and Ferdinand identified similar issues, including a widespread failure to properly classify cyber threats, a tendency to consider it an IT problem rather than a business problem, and a lack of detailed understanding of cyber threats and how to deal with them.

Benham encouraged governments to give clearer guidance on the European Union's forthcoming General Data Protection Regulation and to incentivise directors to treat cyber as a business risk and conduct appropriate cyber awareness training. Businesses, he said, must run attack simulations to ensure processes are suitably robust and investigate whether cyber insurance is necessary, as well as ensuring employees remain vigilant for false invoices or emails.

Ferdinand outlined one possible taxonomy for cyber incidents, which starts with access, whereby an organisation must determine whether physical or virtual access by hostile actors is possible and then review security policies and practices where necessary. He also presented a taxonomy of cyber threat that connects threat actor to cyber harm, thereby providing a better understanding of cyber threat. In the next step, organisations must limit their vulnerabilities through technology, such as intrusion detection systems, and then they must assess what additional limits and controls can be put in place to prevent attacks. Organisations can also use defensive measures to reduce the availability of targets for attackers.

As banking customers are just as vulnerable to cyber-attack as the banks themselves, but typically less well protected, banks have an obligation to help their clients fully understand and mitigate the risks, Benham concluded.

In the final presentation, delegates were given insight into the practical application of a tool to help share information to identify threat activity from insider cash-out behaviour. Poor information sharing among intelligence agencies was identified as one of the key failures that led to the 9/11 terror attacks, and experts believe there is an equally concerning failure to share intelligence on cyber threats, including insider cash-out behaviour.

Suspicious activity reports', which are required by US law for any institution doing business in the US, and 'intelligence information reports', which were created after 9/11 for the US intelligence community to share information to build up a comprehensive picture of threats, were used as the basis for the design of a SWIFT based Threat Indicator Sharing Tool.

The draft of an 'Insider Threat Report' was showcased by its architects; Casey Evans of American University's Kogod School of Business and Elizabeth Petrie, director of strategic intelligence in the Office of the Chief of Information Security at Citicorp. This concise report allows banks to clearly and simply classify the nature of a potential threat and any remediation actions that have already been taken. The report has been submitted to SWIFT Standards to render it compatible with the SWIFT network, formatted into the MT999 messaging format, so that it could be easily shared across the SWIFT network.

Following the Bangladesh Bank cyber-attack in February 2016, SWIFT launched a customer security programme (CSP) to work on a number of initiatives, including the sharing of information and intelligence. With 11,000 customers around the world and varying levels of cyber awareness, one-to-many information sharing must be a top priority, said Brett Lancaster, SWIFT's global head of security programmes. When polled, an overwhelming 84% of the conference audience felt a threat indicator sharing tool should be piloted as a mechanism to share information over the SWIFT network, with an initial focus on insider threats.

The conference concluded with a panel discussion that explored many of the themes from earlier presentations, with practical insight from practitioners at banks and market infrastructure operators. While a certain level of awareness and understanding of the threats has clearly been reached, the commonly voiced concern is the gaps that may still exist and the points of vulnerability that institutions may not be aware of.

The key objective, panellists agreed, should be to promote a shared responsibility for the necessary hygiene measures within every business, so that cyber resilience is not allocated to a few select individuals but becomes embedded within the DNA of every organisation. Increased awareness, robust controls and proactive information sharing should all flow naturally from that initial objective.

In summarising the key findings of the conference and presenting his own conclusions, KPMG's Paul Taylor noted the concerning rise of ruthless and rational cyber criminals that operate increasingly as businesses rather than gangs. But it is encouraging to see the progress that is being made, he said, and the most constructive outcome will be for institutions to continue to work together as an industry, as well as with governments and academia.

- End -