Enhancing the Financial Sector's Cyber Security in the Digital Economy

By Cambell Benjamine and Sivanathan Subramaniam

In an increasingly digital economy, a necessary condition for financial stability is an enabling and effective cyber security framework and effective practices that are both technologically innovative and resilient to cyber threats. While enabling greater connectivity between individuals and organisations with significant benefits to consumers and other users of financial services, disruptive technologies also have the potential to increase vulnerabilities to cyber-attacks which can lead to financial losses and disruptions to essential financial services.

The domestic financial services industry sees an average of one million cyber-attack attempts a day. Most of these attacks are successfully blocked, with no breaches resulting in significant impact or monetary losses experienced to date. However, financial institutions face increasingly sophisticated cyber threats where breaches may remain undetected for several months or even years. Vigilant of the need to stay one step ahead, financial institutions continue to invest heavily in the latest security technology and top talent, to increase their resilience to cyber risks. In July, the Bank also issued specific regulatory requirements for the management of risks in technology, including cyber risks, by financial institutions.

Merely securing or ring-fencing individual financial institutions is however insufficient. New cyber risks are emerging at the fringes of the financial ecosystem which is continually expanding as the adoption of digital technologies becomes more ubiquitous. These new vulnerabilities can emerge from systems that are outside the immediate influence or control of financial institutions. This can include telecommunication, utilities and third party service providers. For instance, a telecommunications outage in July 2019 took down the digital services of the four large Australian banks[1]. In another case, a modern cyber-attack on Metro Bank in the United Kingdom intercepted[2] codes sent via Short Message Service (SMS) from telecommunications companies.

Increasingly, attackers have also directed their focus on retail consumers typically regarded as the weakest link in cyber security. In most cases, vulnerabilities in an individual's digital touchpoints are exploited to obtain their online banking credentials to facilitate unauthorised fund transfers, or otherwise affect the integrity of customer data. The expanding scope and sophistication of these attacks underscore the need for a national level response to complement efforts by financial institutions and financial regulators in strengthening cyber resilience. This should aim to deliver a cohesive, coherent and comprehensive national strategy on cyber security.

The need for a national coordinated response was already recognised sometime back. In 2006, the National Cyber Security Policy (NCSP) was established. It identified ten Critical National Information Infrastructure (CNII) sectors including financial services that need to be safeguarded to a level commensurate with the risks. Following this, a National Cyber Crisis Management Plan (NCCMP) was developed in 2011 which sets out the processes and procedures to be observed by the CNII sectors for detection, response, communication and coordination in the event of a cyber-attack. An updated NCSP is expected to be launched later this year, incorporating among others, enhanced cyber security incident response and digital forensic capabilities.

Building on these important foundations, the focus of ongoing and future initiatives to strengthen Malaysia's cyber security capabilities should consider several imperatives. First is a need to establish and strengthen existing guidance around cyber security and risk management. This should also aim to promote greater consistency in such guidance to reduce vulnerabilities in the weakest link of the digital ecosystem. Within the financial sector, the Risk Management in Technology (RMiT) policy document issued by the Bank addresses expectations for banks, insurers, eligible e-money providers and payment operators to significantly strengthen cyber risk management practices in the areas of governance, cyber security control measures, proactive

[1] Automated teller machines (ATMs) and several branch services were affected by a telecommunications outage. Available at https://www.theguardian.com/business/2019/jul/11/telstra-outage-brings-down-eftpos-and-atms-across-australia.

[2] Hackers exploited flaws in SS7, a protocol used by telecommunications service providers to coordinate how they route calls and SMS messages around the world. Available at https://www.telegraph.co.uk/technology/2019/02/01/metro-bank-hit-cyber-attack-used-empty-customer-accounts/.

Diagram 1: Six Key Building Blocks for National-Level Cyber Security Coordination

National-level cyber security coordination is vital to manage cyber security in a cohesive, coherent and comprehensive manner

Source: Bank Negara Malaysia

monitoring and surveillance, and response and recovery. Payments Network Malaysia Sdn. Bhd. (PayNet), the operator of RENTAS, also issued a cyber resilience guideline in 2018 to specify protective measures to mitigate cyber risks relating to PayNet, and the payments ecosystem as a whole. Similar standards and guidance which are consistently applied in other sectors will be important to strengthen overall cyber defences, including in parts of the digital ecosystem that interface with financial services. The evolution of such standards and guidance at the national level also presents opportunities for authorities and institutions to consider trade-offs between measures that allow institutions to focus on managing residual risks, and measures that create redundancies to reinforce defences at multiple levels.

Secondly, building a common understanding of relevant cyber security, resilience and incident response terminology at the national level will facilitate more effective cyber information sharing across industry sectors and communication when responding to cyber incidents. For example, the terms “Cyber Event” and “Cyber Incident” tend to be used interchangeably despite having distinct differences in their meaning and implications. (The former refers to any observable occurrence in an information system while the latter refers to any cyber event that jeopardises cyber security). Globally, the Financial Stability Board has recently published a lexicon of terms relating to cyber security and resilience for use by the financial sector.

Thirdly, there is a need to identify and reduce barriers to effective information sharing on cyber threats across sectors. Entities are typically hesitant to share cyber threat information for several reasons including legitimate concerns over the handling of such information which is highly sensitive. Currently, financial institutions that are regulated by the Bank are required to report cyber incidents and near misses to the Bank. However, outside the financial sector, requirements to report cyber incidents to the relevant authorities are either absent or lack specificity in terms of timelines and scope of information to be reported. This allows attackers to use the same modus operandi to carry out cyber-attacks on different entities in different industry sectors over a sustained period before the threat is effectively neutralised.

These barriers to information sharing need to be addressed at several levels. For the financial sector, a financial sector cyber threat intelligence platform (FinTIP) is being established by the Bank to collate, aggregate, analyse and share cyber threat information from multiple trusted sources. Suitably anonymised information will be shared with the industry, the National Cyber Security Agency (NACSA) and other regulators. At the national level, NACSA is currently responsible for coordinating information sharing of any critical cyber incidents across industry sectors. This could be expanded to support more pre-emptive access to and sharing of information by NACSA on cyber-attack trends and insights across entities and industries. Efforts to improve cyber information flows should address the type of information to be shared,

clear expectations around responsibilities of the entities within the CNII sectors to share and properly handle cyber-related information, well-defined procedures for transmitting and receiving information, and the development of relevant infrastructure to improve the efficiency and speed of information sharing.

Fourth is a focus on strengthening the collective capabilities of institutions and authorities to respond to and recover from a cyber incident. The traditional focus for cyber security has been to identify and prevent a cyber-attack. Increasingly, financial institutions are adopting an 'assumed breach' posture in their risk management approaches. This assumes that a breach has already occurred, thus shifting the focus to the institution's ability to detect, respond to and recover quickly from an attack across institutions and industries. A good way to strengthen cyber defence collaboration and enhance cyber incident handling is by conducting cyber crisis simulations. This is designed to test coordinated response and communication protocols, while identifying gaps that may otherwise remain undetected. The National Security Council organises national cyber security drills known as x-Maya to test the readiness of entities within the CNII sectors in responding to cyber threats once every two years. It is important that the frequency and scope of such simulations be continuously reviewed to take into account changes in the scale, scope and nature of cyber threats. This may entail expanding crisis scenarios to include a broader spectrum of entities, locations extending beyond national borders and different time zones.

Fifth, it is critical to ensure a sustained, strategic focus on deepening the pool of domestic talent to meet the increasing demand for professional cyber security roles. Such talent strategies could include collaborative partnerships between the financial sector and academia, private entities and government agencies. In Malaysia, the Asia Pacific University of Technology and Innovation (APU)'s Cyber Security Talent Zone established in collaboration with the Malaysia Digital Economy Corporation (MDEC) and other industry partners is an example of public-private sector collaboration to develop competent cyber security professionals. Outside Malaysia, another example is Hong Kong Monetary Authority (HKMA)'s collaboration with the Hong Kong Institute of Banks and the Hong Kong Applied Science and Technology Research Institute (ASTRI) to develop a localised certification scheme and training programme for cyber security professionals[3]. Similar collaborative efforts were pursued by the Bank and security professionals of the penetration testing industry to set up the *Persatuan Penguji Keselamatan Siber* (PPKS) in 2017. PPKS administers a certification programme for penetration testing activities in Malaysia and publishes related best practices and guidance for the financial sector. The coordination of certification and professionalisation schemes at the national level can help promote and elevate common standards across different industries.

Finally, effective engagement to support investigations and enforcement actions against perpetrators of financial cyber-crimes will increase the likelihood that cyber criminals are caught and punished, thus acting as an effective deterrent. Due to the nature of cyber-crimes which are transnational, anonymous and often perpetrated on the dark web, investigative and enforcement actions are often arduous and notoriously difficult. For actions to be effective, a significantly higher level of cooperation and coordination across both domestic and international regulatory and law enforcement agencies, particularly in cyber security intelligence sharing, are required.

As cyber criminals become more sophisticated and coordinated in their attacks, the imperatives outlined above will be increasingly critical to preserve strong cyber security defences in the financial sector and provide the necessary agility to respond to the changing cyber threat landscape.

[3] https://www.bis.org/fsi/publ/insights2.pdf.