Mohd Adhari Belal Din: Cybersecurity – safeguarding the future for innovative financial inclusion

Remarks by Mr Mohd Adhari Belal Din, Assistant Governor of the Central Bank of Malaysia (Bank Negara Malaysia), at the "Cybersecurity: Safeguarding the Future for Innovative Financial Inclusion", Kuala Lumpur, 1 August 2017.

* * *

It is my privilege to welcome you to this landmark event – A very important policy forum for policymakers and regulators to discuss on the significance of cybersecurity in safeguarding the future for innovative financial inclusion.

Intersection of financial inclusion and cybersecurity

As digital financial services expands in reach, scope and scale, cybersecurity matters a great deal for policymakers and regulators with financial inclusion mandates. The fast-changing digital landscape has brought the financially excluded and underserved populations into the formal financial system, bringing about a positive impact on economic growth and stability. However the rapid paced innovation of digital financial services also opens up opportunities and incentives for cyber-attacks, which challenges the fundamental principles of information risk and cybersecurity management. Leaders must understand the risks associated with digital innovation, and balance the imperative to protect their organisations and consumers with the need to adopt innovative technology approaches.

The likelihood for cyber-attacks and fraud is exacerbated by those who are inexperienced with formal financial services and unfamiliar with consumer rights. Low financial and technology literacy amongst consumers could translate to greater vulnerabilities and exposures. More worryingly, we have seen major cyberattacks occurring globally which caused disruptions to essential financial services and destroy savings or financial assets that the underbanked depend on. Financial institutions are not only prime targets for cyberattacks but bear tremendous fiduciary and legal, regulatory, and compliance responsibility to protect customer data and privacy. Safeguarding trust in the formal financial system is now particularly important for the newly included grassroots.

In financial services, the push for digital innovation, disruptive technologies, delivery of more personalized customer experiences, and seamless access to consumers for more inclusion continuously introduces new threats. Forrester Research calls this dynamic an “epic” battle between privacy and digital innovation, and predicted that by 2020 financial services and insurance companies expect to generate the biggest portion of their total sales from digital products, services, or items sold online. Alongside this drive toward digital business, many organisations rely on legacy IT systems that are expensive to maintain and susceptible to more vulnerabilities, greatly compounding the cybersecurity challenge.

Importance of cybersecurity

The current chairman, president and CEO of IBM, Ginni Rometty had described cybercrime as “the greatest threat to every profession, every industry, every company in the world.” While cybersecurity used to be considered an issue primarily for the IT folks, these days it is an agenda item for the entire C-Suite. What has really changed? It is not just the frequency of media reports on cybersecurity breaches. If anything, these are merely symptomatic of a larger shift underway. Cyber-attacks are fueled by increasingly sophisticated technologies along with relatively new trends in mobility usage, social media, and rapidly expanding connectivity, all in the hands of organized online criminal networks.

The first six months of 2017 have seen an inordinate number of cyber-attacks and they were not just the standard corporate breaches. Already there has been viral, state-sponsored ransomware, leaks of spy tools from US intelligence agencies, targeted denial-of-service attacks and full-on campaign hacking. Unfortunately, this is likely a prelude of more cyber-attacks to come.

Let me share with you some key statistics on cybersecurity:

- The global cost of cybercrime will reach USD2 trillion by 2019, a threefold increase from the 2015 estimate of USD500 billion.
- Last year, cybersecurity researchers estimate that criminals made over USD1 billion through ransomware, with victims ranging from the chief executives of Fortune 500 companies to mom-and-pop businesses and private individuals.
- 1 in 131 emails contained malware in 2016, the highest rate in 5 years.
- 76% of organisations worldwide reported being victim of a phishing attack in 2016
- Only 38 percent of global organizations claim they are prepared to handle a sophisticated cyberattack.
- Global spending to combat cybercrime will top USD80 billion this year, with organisations increasingly focusing on detection and response. I shall deliberate more on this shift of focus.

Shift cybersecurity focus to detection and response

Traditionally, the main focus of cybersecurity traditionally has been on prevention. However, organisations which have been taking preventative approaches to combat cybersecurity threats are coming to realise that this strategy have not always been successful in blocking malicious attacks. A paradigm shift is required to move from the ‘old ways’ of trying to prevent every threat. Organisations need to emphasize on detecting and responding to malicious behaviors and incidents, because even the best preventative controls will not prevent all incidents. There is just no such thing as perfect protection. As there are more and more innovative financial inclusion initiatives coming on-board, we will all need to continually reassess how much risk and controls are appropriate.

The disparity between the speed of compromise and the speed of detection is one of the starkest failures discovered in breach investigations. According to a 2015 report by Mandiant, the average targeted malware compromise was present for 205 days before detection. The longest malware presence was 2982 days, and 69% were actually discovered by external parties and not internal IT security functions. Additionally, the 2015 Verizon Data Breach Investigations Report highlighted that, “in 60% of cases, attackers are able to compromise an organization within minutes."

In this digital world, the pace of change and innovation is already too fast to anticipate and, combined with advanced and persistent attacks, it will be impossible to defend against every type of cyber-attack. Organisations must invest in technical, procedural and human capabilities to detect when a compromise occurs. They must provide the tools for first responders to react quickly and investigate the source and impact of breaches, compromises and incidents.

Most essentially, there is a need to balance the right mix of investments across prevention, detection and response capabilities vis-à-vis an organisation’s risk appetite. Not only are new and advanced tools needed to supplement existing protection solutions, but also new skills and culture need to be developed within existing security teams and the larger organization, more so within the ambit of digital financial services whereby regulatory compliance plays a major role in cybersecurity.

Regulatory compliance does not equal cybersecurity

Regulations are designed to protect organisations, clients, and consumers against the potentially devastating consequences of cyber-attacks. Regulatory requirements for financial institutions have undeniably become tougher, and organisations are continuously burdened by the need to interpret what a fragmented global regulatory landscape means for their operations. Financial institution often find themselves chasing regulatory compliance, rather than leading independent security planning. Regulatory compliance by itself is not cybersecurity.

When new cybersecurity requirements or frameworks are published, organisations must first determine their current security state and identify gaps. If routine testing and remediation are conducted, being compliant or meeting regulations should be easier to achieve. Of course, some parties will want or need to go above and beyond regulations. Too often, however, organisations find themselves in reactive mode.

Rather than taking a "check the box" approach, organisations should implement an integrated and cross-discipline effort in order to adopt an enterprise-wide program of cyber risk management that is tailored to business objectives, while also maintaining a tolerable level of risk. By taking an integrated approach to the broad objectives of cybersecurity management, organizations can achieve these business and security-focused goals, while also achieving regulatory compliance in an effective and efficient manner.

Ultimately, cyber resilience which is the ability to defend, respond to, and recover from a breach, should be the end goal for organisations. Although compliance is rightly prioritized in the highly regulated financial services industry, being compliant should be viewed as a result of having good security practices rather than as a check-the-box exercise that is expected to guarantee security. The focus should be shifted toward conducting good cyber due diligence and assessments, implementing proper detection controls, having effectively enforced third-party risk and insider risk programs and conducting testing such as red teaming in order to simulate the organisation's response in the event of a serious attack. If such practices are implemented, organisations can stay ahead of industry regulations and embrace innovation, because their response to any new cybersecurity requirement is less likely to demand a dramatic overhaul of their current program.

The world today is remarkably different from the world we were living 20 years ago. The world is fast converging in aspirations and ideals because of globalization and technology, and with that comes different risks. These forces of change present equal measure of challenges and opportunities but are exciting. I would like to share some open questions for everyone to ponder upon. What is the top cyber security concern for innovation in financial inclusion which we face today? Have we allocated enough resources to properly address the most significant cyber security threats? What specifically have we done? What is our plan for identifying and addressing cyber threats? Is it current? And what does your organization need to do to ensure continuous cybersecurity vigilance moving forward?

May we keep these questions in our mind as we have fruitful discussions and take home great lessons in order to keep pushing the boundary of what we could achieve.

With that, I hope you will have an engaging, successful and fruitful discussion in the next 2 days. I strongly believe this forum would be a valuable platform for members to learn and share their knowledge and experiences as well as generate new ideas, approaches and innovations as take-aways that could be emulated in your respective countries.

Thank you.