Source: *The Business Times,* p21
Date: 7 December 2019

CFA SINGAPORE INSIGHTS

By Lutfey Siddiqi

Should cyber risk governance take centre-stage in financial services?

While the convenience and efficiency of extreme connectivity is well-understood, the resultant risks are considerably less appreciated

IT FEELS as though cyber risk has crept up on us without warning and with great intensity.

We have come a long way from the days when our palm pilots had to be hot-sync'd through a docking station and the occasional hazard was from viruses transmitted as e-mail attachments. Over the years, we have embraced extreme connectivity combined with extreme automation in a never-ending drive towards convenience and cost-efficiency.

However, even as banks continue to nudge, cajole (and perhaps occasionally threaten) their customers towards impersonal e-channels, we learn about record amounts of losses from online fraud and theft. Furthermore, all of us – not just the specialists – are asked to act as conscription soldiers in the fight against this threat.

According to a report by Accenture, almost eight out of 10 business leaders believe that they are adopting new technologies faster than they can address related security issues. It also estimates that nearly US$350 billion of value could be lost by the banking sector to cybercrime in the next five years.

With more of our devices integrated through the Internet of Things and more of our services provided by an assemblage of outsourced specialists, there are simply more points of entry for potential attacks or lapses. With a wide diversity of digital maturity, capability and habits of "cyber hygiene" among us, and unless there is agile regulatory response, our entire system of payments, borrowing and savings could be compromised by the weakest link.

It is not hard to imagine a cyber event impairing the integrity of data on which the flow of finance relies. A loss of confidence could in turn trigger bank runs, liquidity freezes or jumps in market prices.

High profile examples of malicious infiltration across various sectors include the NotPetya attack on the shipping Group Maersk, the WannaCry attack on the British National Health Service (NHS), the theft of reserves from Bangladesh central bank via the SWIFT network, and the hacking of confidential data from Sony Film Studios.

New challenges

This landscape of a rough neighbourhood coupled with a seemingly underdeveloped security apparatus at the international level poses new challenges of risk management for the financial services sector.

At the same time, the backdrop for international co-operation among authorities appears particularly bleak. Back in April 2009, at the height of the global financial crisis, governments of the G20 came together with a robust, comprehensive and effective plan of action. By contrast, with alleged state involvement in certain attacks, countries operate as "frenemies" with a guarded stance on cyber issues.

There is disagreement even among close allies

such as the United States and the European Union on how to tax digital companies or how to regulate the use of personal data. More generally, there is a conflict between the need for a seamless sharing of threat-intelligence on the one hand, and the desire to localise data within national borders on the other. There may also be cultural differences in attitudes towards citizens' privacy vis-à-vis the state. Furthermore, cyber threats appear to be highly dynamic as attackers harness digital tools with great agility. It is possible, for example, for quantum computing to make it easier to break current encryption methods.

The threat is hard to model and quantify. Any rigorous process requires data (internal and external), assumptions and subjective estimates made by a risk committee. Unlike credit risk and market risk for which banks can utilise historical data, in the words of Catherine Bessant, chief operation and technology officer at Bank of America, "past is not prologue" when it comes to cyber risk. That is why the qualitative aspects of the approach and framework are so important. Scenario analyses and "war games" are also more important than traditional value-at-risk measures to ensure that banks have adequate capital set aside.

Regulators expect that institutions would build systems that are "secure by design" with an emphasis on resilience against threats rather than compliance to a standard checklist. The roles and responsibilities of members of the board, senior management and other key posts must be articulated explicitly and without ambiguity. There is a shortage of skills in this domain at all levels. Staff in cyber-related functions must have the required training and some jurisdictions have implemented specific cyber-certifications.

The contractual framework and governance of outsourcing activities require extra care, ensuring that nothing falls through the cracks. Regulators are also keen to calibrate the regulatory burden to the size and significance of the service provider so as not to discourage innovation by fintech start-ups. This is the philosophy behind the "sandbox approach" taken by the UK and Singapore authorities which allows qualifying start-ups to test their products in a controlled environment.

Tool of last resort

As the managing director of Singapore's central bank, Ravi Menon, told *Euromoney* (https://www.euromoney.com/article/b1h69gyk2kkcw1/how-mas-propelled-singapore-to-the-top-of-the-class), sandboxing is a tool of last, not first, resort. He elaborated how it took several years for the regulator to get comfortable around the risks of cloud computing.

For large traditional banks, the organisational design and cultural slant towards cyber risk is still a work in progress. Should compliance officers sit with operations or the legal department? Does the chief information security officer (CISO) have the required seniority or stature within the organisational chart? Does he or she come from a technology, legal or crime-enforcement background? Do the board and senior management appreciate that new products, markets or cost-reduction measures must be road-tested against their impact on cyber risk, or is that an after-thought?

As digitisation becomes less of a buzzword and more of the core of a bank's business model, it is important that members of the C-suite are fluent on the associated risks.

Banks need to continue to refine their vocabulary of controls, risk classification and indicators. The risk dashboard should include items such as cyber-incident response playbooks, recovery plans, vulnerability scans, password and encryption policy, ongoing training statistics and analysis of near-miss events.

Finally, what are the norms of information sharing within banks, between banks, and between banks and regulators? Incident reporting from banks to regulators is mandatory in most places. However, there are gaps in the other lines of communication: between regulators across jurisdictions, from regulators to banks, and amongst banks themselves (possibly due to perceived stigma). According to the Bank for International Settlements, "full adoption of all types of information-sharing arrangements within a jurisdiction is still exceptional".

Unfortunately, cyber risk is here to stay. The sooner we can adopt a shared language, a convergent framework and an elevated awareness of this risk, the better prepared we would be to strengthen our defence and resilience to this risk.

Lutfey Siddiqi, CFA, is an adjunct professor at the Risk Management Institute (RMI), National University of Singapore where he is also an advisory board member of the Centre for Governance (CGIO). He is a visiting professor-in-practice at the London School of Economics (LSE-IDEAS) and advisory board member of the LSE Systemic Risk Centre. A former board member of CFA Singapore, he is a member of CFA Future of Finance.

A version of this article has appeared on the NUS-RMI Newsletter (rmi.nus.edu.sg/about-us/enewsletterrmi/issue41/in-focus.html) and the LSE Business Review (https://blogs.lse.ac.uk/businessreview/2019/12/04/cyber-risk-governance-should-take-centre-stage-in-financial-services/)