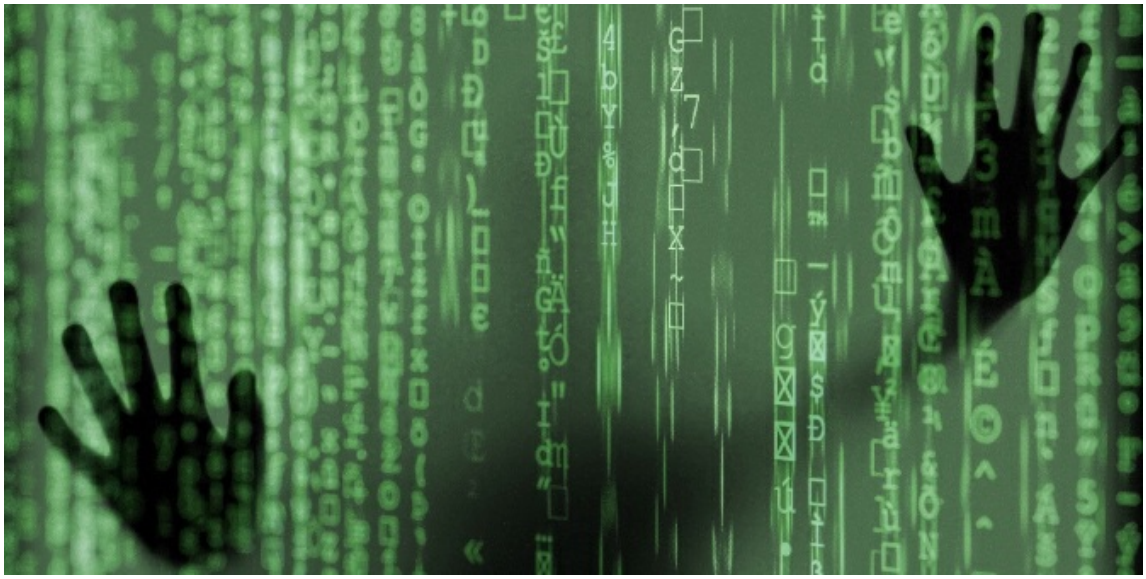
Cyber risk governance should take centre stage in financial services



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 email 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 ten business leaders believe that they are adopting new technologies faster than they can address related security issues. It also estimates that nearly $350 billion of value could be lost by the banking sector to cybercrime in the next five years.

Publicly-known examples across various sectors include the *NotPetya* cyber 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.

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' amongst us, system resilience could be compromised by the weakest link.

At the same time, the backdrop for international cooperation amongst 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 issues of cyber.

There is a conflict between the need for the 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. Finally, 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.

Date originally posted: 2019-12-04

Permalink: https://blogs.lse.ac.uk/businessreview/2019/12/04/cyber-risk-governance-should-take-centre-stage-in-financial-services/

Blog homepage: https://blogs.lse.ac.uk/businessreview/

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. A cyber event could trigger a loss of confidence possibly through compromising the integrity of data on which the flow of finance relies. It could in turn trigger bank runs, liquidity freezes or jumps in market prices. Whether this sustains into a system-wide crisis or not would depend on the prudential response of regulators, as argued by Danielsson et al (2016).

In the words of Catherine Bessant, chief operation and technology officer at Bank of America, "The threat is huge and what makes it difficult for boardrooms is that it's hard to model; it's a risk where past is not prologue".

As it is, unlike credit risk or market risk, operational risk (of which, cyber risk is a subset) can be more nebulous in its framing. The Basel Committee on Banking Supervision (BIS) issued guidance on sound practices for the management and supervision of operational risk in 2003, later updated in 2011. A more recent BIS publication "Cyber-resilience: Range of Practices" (December 2018) catalogues a sweep of activities by both banks and regulators.

Quantifying cyber risk is difficult. Any rigorous process requires data (internal and external), assumptions and subjective estimates made by a risk committee. That is why the qualitative aspects of the approach and framework are so important. As is the need to perform table-top war games.

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. Staff in cyber-related functions must have the required capabilities and some jurisdictions have implemented specific cyber-certifications. There is ample spotlight on the contractual framework and governance of outsourcing activities, seeking to ensure 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.

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? Are there sufficient separation, communication and challenge amongst the 'three lines of defence'? Does the chief information security officer (CISO) have the required seniority or stature within the organisational chart? Does 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?

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. This may include the requirement to submit a root-cause analysis and a post-mortem of lessons learnt. However, there are gaps in the other lines of communication: between regulators across jurisdictions, from regulators to banks, and amongst banks (possibly due to perceived stigma). According to the BIS (2018), "full adoption of all types of information-sharing arrangements within a jurisdiction is still exceptional".

Finally, banks need to continue to refine their taxonomy of controls, risk classification, indicators and a book of tangible items that can serve as metrics for their cyber risk control environment. That dashboard could include items such as cyber-incident response playbooks, recovery plans, vulnerability scans to password and encryption policy to training statistics, near-miss events etc.

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.

Also from Lutfey Siddiqi:

> Can a post-Brexit UK trade more in financial services with ASEAN?

♣♣♣

- *This blog post is based on the author's remarks at the World Economic Forum Annual Meeting on*

Date originally posted: 2019-12-04

Permalink: https://blogs.lse.ac.uk/businessreview/2019/12/04/cyber-risk-governance-should-take-centre-stage-in-financial-services/

Blog homepage: https://blogs.lse.ac.uk/businessreview/

Cybersecurity, 13 November 2019, and the LSE Systemic Risk Centre event "Engineering Financial Instability on 2 December 2019.

- *The post gives the views of its author(s), not the position of LSE Business Review or the London School of Economics.*
- *Featured image by pixel2013, under a Pixabay licence*
- *When you leave a comment, you're agreeing to our Comment Policy*

Lutfey Siddiqi, CFA, is a visiting professor-in-practice at LSE and an adjunct professor at the National University of Singapore. A member of the World Economic Forum Global Future Council on the New Economic Agenda, he was previously global head of emerging markets for foreign exchange, rates and credit at UBS investment bank.

Date originally posted: 2019-12-04

Permalink: https://blogs.lse.ac.uk/businessreview/2019/12/04/cyber-risk-governance-should-take-centre-stage-in-financial-services/

Blog homepage: https://blogs.lse.ac.uk/businessreview/