INTUITION

Asia Perspectives

FEB 2020 - VOLUME III

Could a cyber attack trigger the next financial crisis?

INTUITION PUBLISHING PTE LIMITED

Following our previous article on "Ransomware as a Service" it would appear the risks of organised cyber crime such as recent targeted & state sponsored attacks, are now being viewed as a potential source of systemic risk to the financial system.

In Europe:
Christine Lagarde, president of the ECB, has warned that a combined cyber attack on important banks could trigger financial instability. *"As an operator of critical infrastructures, the ECB obviously takes such threats very seriously,"* noting there were several *"plausible channels"* through which a cyber attack could escalate into a systemic financial crisis. Operational outages that destroy or encrypt the balance accounts of major financial institutions could trigger a liquidity crisis. *"History shows that liquidity crises can quickly become systemic crises"* she said. *"The ECB is well aware that it has a duty to be prepared and to act pre-emptively."*

A report by the European Systemic Risk Board (ESRB) estimates the global cost of cyber attacks could be as high as $654bn USD. The report, set up by the European Commission, has reviewed how a cyber incident could under certain circumstances rapidly escalate from an operational outage to a liquidity crisis, also identifying cyber risk as a systemic risk to the financial system.

The ESRB is focusing on how to mitigate the vulnerabilities identified and on the role of authorities in a systemic cyber crisis. This is particularly important due to the likely speed and scale of such an event and the specific challenges they pose for responsive communication and coordination strategies. Neither the ECB not the ESRB wanted to comment further on Ms Lagarde's remarks.

In New York:
In a pre-mortem analysis on "Cyber Risk and the U.S. Financial System", the New York Federal Reserve has warned a cyber attack on major banks could spread quickly, noting a well-timed cyber attack on a single large bank could impact the U.S. financial system by dramatically impairing the flow of credit between financial firms. *"We model how a cyber attack may be amplified through the U.S. financial system, focusing on the wholesale payments network"* write economists Thomas Eisenbach, Anna Kovner and Michael Junho Lee.

Concerns about financial crises are often linked to excessive risk taking, but the FRBNY paper makes clear policymakers see cyber security as another key risk factor for financial instability. A critical point in assessing whether a cyber incident will develop into a systemic financial crisis is whether the incident escalates from an operational level to take on financial and confidence dimensions.

"We estimate that the impairment of any of the five most active U.S. banks will result in significant spill-overs to other banks, with 38% of the network affected on average." Financial service companies experience up to 300 times as many cyber attacks per year as companies in other sectors, according to the data cited by the FRBNY. *"One distinguishing feature of cyber attacks is that they may be designed for maximum disruption. Past studies highlight that total payment activity is often heightened at predictable, regular days over the course of the year."* There are noticeable spikes in targeted attacks during high volume seasonal activities.

"When banks respond to uncertainty by liquidity hoarding, the potential impact in forgone payment activity is dramatic, reaching more than 2.5 times daily GDP. In a reverse stress test, interruptions originating from banks with less than $10 billion in assets are sufficient to impair a significant amount of the system. Additional risk emerges from third-party providers, which connect otherwise unrelated banks. Similar to a traditional shock, a cyber event may require liquidity injections via the discount window, open market operations or market-wide liquidity facilities. In addition, regulatory requirements such as liquidity or reserve requirements could be temporarily suspended if banks are technologically unable to address violations, limiting the knock-on effects of perceived impairment."

The G7:
Last year, the G7 announced a joint cross-border crisis management exercise on a cyber incident affecting the financial system, saying that cyber risks were increasing and posed a *"genuine and growing threat"* to the stability and integrity of the financial sector.

It was the first exercise of its kind to be organised by finance ministries, central banks, regulators and financial market authorities. The results have not been revealed but the G7 asked its Cyber Experts Group to review financial regulation. The Trump administration is expected to take up the issue when it assumes the G7 presidency in 2020.

Considerations:
Are current cyber security controls & benchmarks robust enough to mitigate such systemic risks? A key concern lies in the shortage of necessary skills. Appropriate People and Awareness training and relevant support is therefore needed to help mitigate these potential systemic risks.

Intuition – Blended Learning

The Intuition online learning library consists several tutorials related to this article:

Cyber Security Awareness
- Passphrases
- Preventing Identity Theft
- Device Security
- Malware & Breach Recovery
- And more…

Other Relevant Tutorials
- UK Cybercrime
- Artificial Intelligence (AI)
- The Financial Crisis
- Risk Management – An Introduction
- Robotic Process Automation (RPA)
- Robo-Advice

For Intuition blended learning related to this article, some of our popular workshops include:

- Cyber-Warfare: The Fourth Dimension of War
- Human Cyber-Security Risk
- Holistic Technology Risk Management Framework
- Insights into Governance, Risk and Compliance (GRC) In New Digital Age and Impact on Financial Advisory and Capital Markets Representatives
- Digital Banking Masterclass
- Data in Banking

Get in touch with your Intuition account manager at apacinfo@intuition.com for more details

The topics covered in Intuition Asia Perspectives are current developments or topics currently in the market. Intuition Asia provides bespoke learning solutions, both eLearning and Instructor-led courses. These can also be blended in a program to provide the most effective form of learning. These workshops can be structured as lunch & learns, webinars or full day deliveries. Clients can use these to keep their workforce updated with the latest developments in the market and complete their mandatory CPD learning hours

Other Asia Perspectives Articles

- The Evolution of Ransomware as a Service
- US-Iran: Far from Finished

Download the Asia Perspectives free app to get the latest article.

Get the app

Related News Articles

- Cyber Attacks: Igniting the Next Recession? – Forbes 05 Jan 2019
- US Banks Face Tighter Scrutiny of Cyber Defences – FT 17 June 2019