WORLD BANK GROUP
Finance & Markets

Cybersecurity in the Financial Sector

Aquiles A. Almansi
Lead Financial Sector Specialist
aalmansi@worldbank.org

Cyber incidents in the financial sector today

- The average financial institution monitored by IBM Security Services experiencing 65 percent more attacks than the average client across all industries in 2016, and a 29 percent increase in attacks from 2015.

- Distributed Denial of Service (DDoS) and "ransomware" attacks disrupted financial services in many countries, money was stolen from several banks, and confidential data "exfiltrated."

Growing regulatory response

- FSB: *Stocktake on Cybersecurity Regulatory and Supervisory Practices*, October 2017.
- World Bank-FinSAC: *Financial Sector's Cybersecurity: A Regulatory Digest*, October 2017.
- A. A. Almansi: *Financial Sector's Cybersecurity: Regulations and Supervision*, October 2017.

Regulatory response: key ideas

- Some jurisdictions approach cybersecurity and/or information technology risk explicitly, others address it implicitly, as just a type of operational risk.
- Existing cybersecurity regulations typically address:
    - roles of the Board, Senior Management and, if present, the Chief Information Security Officer (CISO)
    - mandatory reporting of cyber/ICT incidents
    - outsourcing of ICT services

Regulatory response: other ideas

- Some regulations also address:
  - risk assessments
  - system access controls
  - incident recovery
  - simulations and testing
  - training
  - encryption protocols
  - etc., etc., ...

Cyber risk is Operational Risk, but …

…in the world of interconnected computers (a.k.a. "cyberspace"), complexity is extreme and cyber incidents (like "ransomware") can be highly contagious, so ….

Cyber risk is Operational Risk, but …

I

…the "proportionality" of regulatory requirements and supervisory attention may not apply: all of us, rich and poor, fat and skinny, may need the same "vaccines."

Cyber risk is Operational Risk, but …

…it’s no longer clear what role a supervised institution’s “risk appetite (or tolerance) for operational risk” (BCP 25) should play in supervisory considerations.

Cyber risk is Operational Risk, but …

… "managing" the risk of outsourcing ICT services to providers such as Amazon, Google, IBM, and Microsoft does not look quite similar to outsourcing cash transportation to Brink's, or cafeteria and cleaning services to SODEXO. Who can discover the potential "bugs" and "malware" hidden in the millions of lines of code that make up current software applications?

WORLD BANK GROUP
Finance & Markets

Who should regulate and supervise cyber risk management in the financial sector?

- 46% of bank customers are already digital-only, compared with 27% in 2012, and human-only customers continue to shrink, falling from 15% to 10% during the same period. (PwC 2017).
- As more dimensions of the "production function" of financial services migrate to "cyberspace", authorities other than financial regulators and supervisors will, sooner or later, have a say on what financial institutions must do, or cannot do.

Who should regulate and supervise cyber risk management in the financial sector?

- Financial sector authorities should get actively involved in the process of defining their country's National Cybersecurity Strategy, to better understand with whom they will have to coordinate regulatory and supervisory functions.

Mandatory reporting and incident response

- Financial sector authorities need to know that a cyber incident has taken place in a supervised institution, to estimate its actual or potential impact. Consequently, regulations tend to mandatorily require reporting.
- Technically assisting a supervised institution in handling a cyber incident may, however, not be the financial authorities competitive advantage (vis-à-vis other state agencies) and, if things go wrong, may lead to severe contingent liabilities in some national legal frameworks.

Mandatory reporting and incident response

To share information about cyber incidents, many countries are setting up computer emergency response teams (CERTs), privately or under different State agencies.

What can be done to improve cybersecurity in the financial sector?

Educating Financial Sector Authorities, Board members, Senior Management:

- Cybersecurity is not just a “technical issue” for “geeks” working in IT departments and cybersecurity companies.

- Responding to a cyber incident will frequently require “business continuity decisions” that cannot be delegated to the “geeks”: the “buck” stops at the CEO’s desk!

What can be done to improve cybersecurity in the financial sector?

Educating the consumer of financial services:

- Computers can do the same things that a phone, a typewriter, or a music player do, but they can also do anything else that we program them to do.
- Because computers are interconnected, somebody can remotely tell our computers to do something we don’t want them to do (like revealing the password to our bank account!).
- iPhones and Androids are not “phones”, they are permanently interconnected computers with a phone line, among many other things!

WORLD BANK GROUP
Finance & Markets

Thanks!

aalmansi@worldbank.org