REGULATORY ASPECTS OF CYBER-SECURITY IN FINANCE: EXISTING APPROACHES AND FUTURE CHALLENGES

Dr Anton Didenko
Research Fellow, UNSW Sydney (Australia)

04 SEPTEMBER 2018

afi 10 YEARS OF BRINGING SMART POLICIES TO LIFE

Bank of Russia

THE 2018 AFI GLOBAL POLICY FORUM

INNOVATION
INCLUSION
IMPACT

OUTLINE

1. Relevance of cybersecurity in finance
2. Distinct nature of cyber threats
3. Designing cybersecurity regulation
4. Future challenges

RECENT SUCCESSFUL CYBER ATTACKS

- January 2016: DDoS attack on HSBC UK
- February 2016: $101 million stolen from Bangladesh Bank
- ??? 2016: hackers gain access to SEC's EDGAR data
- ??? 2017: website vulnerability exposes the data on 147.9 million consumers held by Equifax

INCREASING DIGITISATION IN FINANCE

- Replacing paperwork with direct electronic communication via secure channels
- Fast payments systems
- Paperless documentary operations and other services
- Smart contracts
- Biometric data
- In the long run: reporting by providing data, not forms

RELEVANCE FOR THE FINANCIAL SECTOR

- Systemic importance
- IT-intensive
- Dependent on information inputs
- Interconnected via the payment systems
- Time-critical services
- Banks have the most points of contact with third parties

DISTINCT NATURE OF CYBER THREATS

- Information asymmetry
- Inefficiency of measures preventing operational disruption
- Different nature of threat: (i) dynamic, (ii) intelligent, (iii) adaptive
- Do not respect national borders
- Not limited to technology

"ASSUME BREACH" ATTITUDE: expect that not all attacks can be prevented => the key is to identify and respond to threats

TWO APPROACHES TO CYBERSECURITY REGULATION

- Hands-off/soft approach
- Compliance-based approach
  - Benefit: increase board/management attention to cyber risks
  - Challenge: can be too prescriptive

G7 FUNDAMENTAL ELEMENTS OF CYBERSECURITY FOR THE FINANCIAL SECTOR

- Cybersecurity strategy and framework
- Governance
- Risk/control assessment
- Monitoring
- Response
- Recovery
- Information sharing
- Continuous learning

EXISTING TECHNICAL STANDARDS

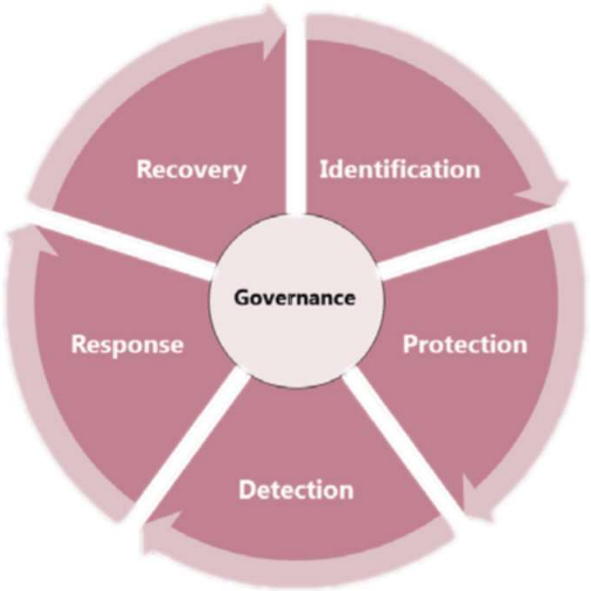
- NIST (National Institute of Standards and Technology)
  - Framework for Improving Critical Infrastructure Cybersecurity
- CIS (Center for Internet Security)
  - Controls
- ISO (International Organisation for Standardisation/IEC (International Electrotechnical Commission)
  - 27000 family of standards

COMMON ELEMENTS OF NATIONAL CYBERSECURITY FRAMEWORKS

- Documented cybersecurity programme/policy
- Self-assessment by financial institutions
- Vulnerability testing
- Reporting cyber events
- Cyber threat intelligence sharing
- Increasing cybersecurity expertise
- Cybersecurity of third party providers

CYBERSECURITY POLICY

- General framework
- Accountability regime
- May include appointment of a *Chief Information Security Officer* (CISO)



Source: BIS (2017)

SELF-ASSESSMENT BY FINANCIAL INSTITUTIONS

- Identification of Critical Information Assets
- Starting point – generally data protection rules
- Can be multi-phase to address industry concerns

Case study:

- Hong Kong's Cybersecurity Fortification Initiative (2016)

VULNERABILITY TESTING

- CBEST program in the UK (voluntary)
- Penetration Testing Guidelines For the Financial Industry in Singapore (2015)
- iCAST (intelligence-led Cyber Attack Simulation Testing) in Hong Kong

NB: some banks perform tests without regulatory guidance

REPORTING CYBER EVENTS

Different approaches:

- Special reporting rules for cyber events having a material effect
- Cyber reporting is already covered by existing reporting requirements

CYBER THREAT INTELLIGENCE SHARING

- Not a common requirement
- Part of G7 ‘fundamental elements’
- Hong Kong’s Cybersecurity Fortification Initiative (2016)
- Private initiatives

INCREASING CYBERSECURITY EXPERTISE

- Hong Kong: certification and training for C-RAF
- UK: CBEST accreditation for professionals involved in CBEST testing

CYBERSECURITY OF THIRD PARTY PROVIDERS

Different approaches:

- Duty of banks to ensure adequate levels of cybersecurity of third parties engaged by them
- Regulator's authority to regulate third parties directly
- A requirement to include in contracts with third parties a clause allowing the regulator to examine their systems

SUPERVISORY TOOLS AND METHODS

- Spreading protected data across different databases
- Using trusted parties to handle/store protected data
- Thematic reviews on cybersecurity
- Intelligence-led vulnerability testing
- No single approach to designing the framework

FUTURE CHALLENGES

- RegTech
- Protecting Digital ID databases
- Raising the level of regulators' cybersecurity expertise
- Understanding cyber risks across entire financial sector
- International supervisory cooperation
- Regulation of decentralised technologies

THE 2018
AFI GLOBAL
POLICY FORUM

INNOVATION
INCLUSION
IMPACT

5 – 7 SEPTEMBER 2018, SOCHI, RUSSIA

THANK YOU