Cyber Resilience through Collaboration: Visions and Actions of the HKMA

Nelson Chow
Chief Fintech Officer
Fintech Facilitation Office
Hong Kong Monetary Authority

16 March 2017
Outline

I. HKMA’s Fintech Facilitation Office (FFO)

II. Industry Landscape on Cybersecurity

III. HKMA’s Cybersecurity Fortification Initiative (CFI)

IV. Key Messages
I. HKMA’s Fintech Facilitation Office (FFO)
Roles and Initiatives of the FFO

**Research and Application**
- **initiator** of industry research in potential application and risks of Fintech solutions

**Industry Liaison**
- a **platform** for exchanging ideas of innovative Fintech initiatives among key stakeholders

**Regulatory Interface**
- an **interface** between market participants and regulators within the HKMA

**Talent Development**
- a **facilitator** to nurture talents to meet the growing needs of Fintech in Hong Kong

**FS Budget Speech**
2016

**Establishment**
2016

**Cybersecurity Fortification Initiative**
Feb

**Fintech Innovation Hub**
Mar

**Fintech Supervisory Sandbox**
May

**Industry Survey**
Sept

**Partnership with ASTRI, Cyberport & Science Park, DLT Whitepaper, Fintech Day**
Nov

**Fintech Career Accelerator Scheme, Co-operation Agreement Signing with FCA**
Dec

2017
II. Industry Landscape on Cybersecurity
Industry Landscape on Cybersecurity: Attacks are real and frequent

- **Service disruption**
  - A major UK bank out of internet banking services for several hours

- **Information loss**
  - A major US bank got the data of 83 million customers stolen

- **Financial loss**
  - A central bank account lost US$81 million

Financial services firms are reportedly hit 300 percent more frequently than other industries.
Industry Landscape on Cybersecurity:
Increasing interconnectedness leaving banks more vulnerable to cyber attacks

- Increasing interconnectedness causes risks and cyberattacks to spread quickly and widely in the banking network.

- More and more criminals are harnessing the speed and scale offered by interconnectedness as weapons of attacks.

Cybersecurity is the key foundation for financial innovations.
Industry Landscape on Cybersecurity: Many institutions are taking serious measures

- Global banks are spending top dollars
  - Total annual expenses on cybersecurity of top firms: over US$1 billion

- More information is being shared
  - Banks have been sharing threat information for some time
  - Rising momentum of cooperation; largest players working closer to share intelligence, rehearsal plans, etc.

Global players are bigger targets, but generally better prepared; progress of others are more varied; industry efforts remain fragmented.
III. HKMA’s Cybersecurity Fortification Initiative (CFI)
Cybersecurity Fortification Initiative (CFI)

- Rolled out in May 2016; tailored for banks (also FMIs)
- Help enhance cyber resilience of institutions through three elements:
  - Cyber Resilience Assessment Framework (C-RAF)
  - Professional Development Programme (PDP)
  - Cyber Intelligence Sharing Platform (CISP)

Link to further details of the CFI programme - Circular issued on 21 December 2016
Cyber Resilience Assessment Framework (C-RAF)

3-Step Framework to improve cyber resilience of banks

1. Inherent Risk Assessment
   - Determine cyber risk exposures based on a number of factors
   - Result in an inherent risk rating (i.e. high, medium and low), which is then mapped to the respective “required maturity level”

2. Maturity Assessment
   - Determine the “actual maturity level” via 7 domains

3. Roadmap for Improvement
   - Formulate plans to enhance cyber resilience should gaps exist between “required maturity level” and “actual maturity level”

   **Intelligence-led Cyber Attack Simulation Testing (iCAST)**
   - Simulate real-life cyber attacks
   - Performed by AIs with “medium” or “high” inherent risk ratings
Cyber Resilience Assessment Framework (C-RAF) (con’t)

Implementation timeline

- Consultation with the banking sector (May – August 2016)
  - Industry welcomed the framework; over 170 valuable comments
  - Several rounds of subsequent discussions with HKAB to follow-up on issues raised

- Phased implementation of the Framework (December 2016 – End of 2018)
  - First phase covers around 30 AIs (i.e. major retail banks, selected global banks)
    - Inherent Risk and Maturity Assessments – completed by end-September 2017
    - iCAST (if applicable) – completed by end-June 2018
  - Second phase covers all the remaining AIs
    - Inherent Risk and Maturity Assessments – completed by end of 2018
    - iCAST (if applicable) – timeline to be determined based on assessment results of second phase

As all inter-connected banks raise resilience and become less vulnerable, the whole banking sector becomes more robust.
Professional Development Programme (PDP)

A local certification scheme and training programme for cybersecurity professionals

- Train and nurture cybersecurity practitioners
- Graduates may carry out assessment / testing required under C-RAF

Implementation timeline

- Consultation with the banking and IT sectors (July – August 2016)
  - Industry welcomed the scheme; over 20 valuable comments

- Identification of equivalent qualifications (October – November 2016)
  - A list of equivalent qualifications identified by an expert panel comprising representatives from major IT professional associations, banks and universities

- **Roll out of the programme (December 2016)**
  - HKMA to continue monitoring the overall programme

With the PDP and banks engaging more qualified cybersecurity practitioners, their professionalism will be better recognised.
Cyber Intelligence Sharing Platform (CISP)

A platform for cyber intelligence sharing, alerts and solutions
- An industry wide computer platform for sharing cybersecurity intelligence among banks participants
- Disseminate regular intelligence reports to participants regularly (including daily alerts)
- Offer actionable solutions, such as mitigation steps or best practices for managing a particular cyber threat
- Perform trend analysis on upcoming threats
- Cover intelligence in the Chinese language

Implementation timeline
- First version launched in December 2016

Behind the platform is the spirit of industry collaboration: It takes the whole banking community to protect the banking community.
IV. Key Messages
Preparing for tomorrow’s challenges today
1. Attacks will get more hostile, frequent, and unpredictable

- Malicious attacks are increasingly multifaceted:
  - **Different sources**: cybercriminals, hacking enthusiasts; attackers based locally or overseas, etc.
  - **Different motivations**:
    - *For money?*
    - *For sensitive information?*
    - *For “making a statement”?*
    - *Or, simply, for “showing off” skills?*

Keep vigilant and updated on evolving trends of cyber risks.
2. Cybersecurity is everybody’s business

- It is important for banks to cultivate the *right environment* to prevent and prepare for attacks:
  - Constant attention of senior management
  - Governance arrangements and processes

- Human factor is often the (overlooked) root cause of incidents; and a system is as strong as its weakest link
  - Staff awareness and alertness

- Cybersecurity not just a matter for internal staff, but all users of systems
  - Robust third-party management

Establish proper governance structure and engage internal and external stakeholders to enhance resilience.
3. The HKMA’s CFI provides a good platform but institutions must do more

- Cyberattacks are persistent and ever-changing, we will never “finish the job”.

- The CFI only serves as a baseline requirement:
  - **Assessment Framework**: Minimum requirements are set but institutions have to further address risks based on their specific situations
  - **PDP**: Give due recognition to qualified professionals, and encourage continuous professional training
  - **Intelligence sharing platform**: More useful when everyone shares promptly and act swiftly on intelligence

CFI only serves as a foundation, more efforts and collaborative responses by the industry are needed.
Thank you