



Cyber resilience through collaboration: Visions and actions of the HKMA

Howard Lee

**Senior Executive Director
Hong Kong Monetary Authority**

21 September 2016



Outline

- I. Industry Landscape on Cybersecurity**

- II. Latest Development on HKMA's Cybersecurity Fortification Initiative (CFI)**

- III. Key Messages**



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: Many banks 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.
- **Many banks are looking for more experts**
 - Evidenced by the ever-increasing training efforts by banks and training providers, and specialisations of expertise



Global players are bigger targets, but generally better prepared; progress of others may be more varied; industry efforts could remain fragmented.



Industry Landscape on Cybersecurity: Top of regulators' agendas

- **HKMA: Cybersecurity Fortification Initiative**
 - Three-pronged approach: framework, training, platform
 - Announced its launch in May 2016
- **Similar efforts made by other bank regulators**
 - **US:** Federal Financial Institutions Examination Council (FFIEC) developed a Cybersecurity Assessment Tool to help banks identify risks, determine preparedness
 - **UK:** Bank of England (BoE) developed an Intelligence-Led Testing Framework, known as CBEST



HONG KONG MONETARY AUTHORITY
香港金融管理局



**HKMA and other regulators are drawing up different plans;
We all need to find our “cybersecurity solution” that best serves our needs.**



HKMA's Cybersecurity Fortification Initiative (CFI)

HKMA's Cybersecurity Fortification Initiative (CFI)

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



Cyber Resilience Assessment Framework (C-RAF)

For assessing banks' inherent risks, testing resilience, identifying gaps, charting routes for improvements

- **Consultation with the banking sector (25/5 – 31/8)**
 - Industry welcomes the framework; over 170 valuable comments
- **Possible improvements on document include:**
 - A glossary of terms (to clarify definitions)
 - For different “control principles”, we may
 - ✓ re-position some to a different classification (maturity level)
 - ✓ re-word some to allow more flexibility (e.g. ...one should do something “in a timely manner” instead of “simultaneously”)
 - ✓ remove some in view of technical difficulties (e.g. assigning potential losses by cost centres)
- **Way forward**
 - Revision of framework underway
 - To further discuss with HKAB on proposed revisions soon
 - Implementation details available around the end of 2016



As all inter-connected banks raise resilience and become less vulnerable, the whole banking sector becomes more robust.

Professional Development Programme (PDP)

A training and certification scheme; graduates may carry out assessment/testing required by CFI

- **Consultation with the banking and IT sectors (19/7 – 31/8)**
 - Draft sent to over 10 parties, including industry associations, universities; received 22 comments
- **Industry welcomes the proposed scheme**
 - Provide the financial industry with much needed cybersecurity talent
 - Support recognising equivalent qualifications
- **Way forward**
 - To roll out the first training courses by the end of this year
 - Setting up a panel to consider equivalent qualifications (comprising representatives from academia and the banking and IT industries)



With the PDP and banks engaging more qualified cybersecurity practitioners, their professionalism will be better recognised.



Cyber Intelligence Sharing Platform

A one-stop shop for threat intelligence, alerts and solutions, with professional help

- **Defined key functions:**

- Hub for sharing of threat intelligence by participants
- Regular intelligence reports (including daily alerts)
- Actionable solutions
- Trend analysis

- **Other features:**

- Covers intelligence in the Chinese language
- Secured communication channels with robust encryption


- **Recent progress of developments:**

- Hardware being deployed and configured; application development underway
- Intelligence from commercial sources being evaluated

- **Way forward**

- First version of the platform will be operational by end-2016

**Behind the platform is the spirit of industry collaboration:
It takes the whole banking community to protect the banking community.**



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

- Cybersecurity not just a matter for IT staff, but all users of systems
- The human factor is often the (overlooked) root cause of incident; and a system is as strong as its weakest link
- As required by CFI, important to cultivate the *right environment* to prevent and prepare for attacks:
 - Constant attention of senior management
 - Governance arrangements and processes
 - Staff awareness and alertness
 - Robust third-party management



Engage internal and external stakeholders to enhance resilience.



3. The HKMA's CFI provides a good platform but banks 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 banks 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



Banking is a business of managing risks, cyber risks are not new but given the new challenges, more systematic and collaborative response is needed.



Thank you