



Cybersecurity Solutions Day: Regulatory Keynote Speech

“Balancing Innovation and Risk”

**Howard Lee
Deputy Chief Executive
Hong Kong Monetary Authority
22 March 2019**



Innovate to stay competitive

01

Faster Payment System
(FPS)

02

Enhanced Fintech
Supervisory Sandbox
(FSS) 2.0

03

Promotion of
Virtual Banking

04

Banking Made Easy
initiative

05

Open Application
Programming Interface
(API)

06

Closer cross-border
collaboration

07

Enhanced research
and talent development

08

.....

09

.....



All online services may be hacked, as a matter of time

Online Banking Breaches:

- UK (9000 accounts)
- Canada (~90,000 accounts)

Personal Data Leakages:

- Global (Marriott) (500M users)
- US (Equifax) (143M users)
- US (T-Mobile) (2M users)
- US (Facebook) (30M users)
- UK (British Airways) (0.57M users)
- Singapore (SingHealth) (1.5M users)
- HK (Cathay Pacific) (9.4M users)

ATM Hacks:

- Japan (loss: \$19m)
- India (loss: \$11.5m)
- Thailand (loss: \$0.35m)
- US (loss: \$1m)

SWIFT & Other Wholesale Payment Systems Attacks:

- Malaysia (no loss)
- Chile (loss: \$10m)
- Mexico (loss: \$15m)
- India (loss: \$2m)



Note: Only selected, recent and major incidents are shown




Incident can remain undiscovered for a long time

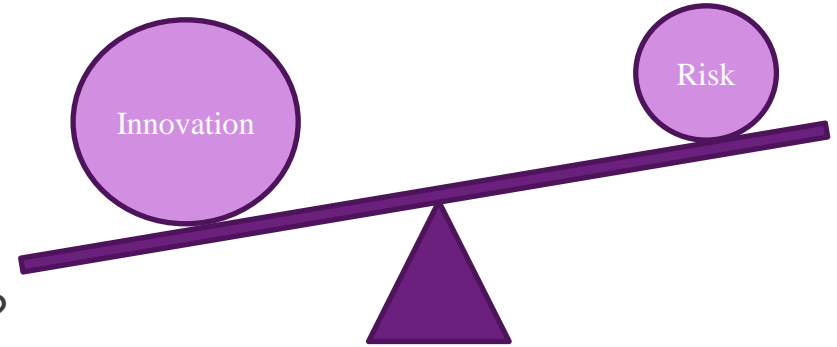
- **Marriott International data breach 2014 - 2018**
 - The 2nd biggest corporate data breach in history
 - Guest reservation system exposed for **4 years**
- **500 Million** customer information exposed
- **Losses**
 - Financial penalties from authorities and class-action lawsuits
 - Damage to company reputation and customer trust
 - Breaches can spread quickly due to interconnectedness of other business entities





Balancing innovation and risk

- Avoidance vs mitigation?
- Traditional IT security vs Cybersecurity?
- Protection  Detection + Recovery?
- Static vs Intelligence-based?





Addressing cyber risk by Cybersecurity Fortification Initiative (CFI)

Goal

Launched in Dec 2016

- ✓ Establish a common risk assessment framework for banks
- ✓ Offer training and certifications in cybersecurity
- ✓ Facilitate sharing of cyber threat intelligence

Three Pillars of CFI



**Cyber Resilience
Assessment Framework
(C-RAF)**



**Professional
Development Programme
(PDP)**



**Cyber Intelligence
Sharing Platform
(CISP)**



Good progress for C-RAF

- C-RAF is an assessment tool to evaluate bank's cyber resilience, it comprises the Inherent Risk and Maturity Assessments, and iCAST.

		Phase 1: 30 banks	Phase 2: 60 banks	Phase 3: Remaining ~90 banks
C-RAF	Inherent Risk Assessment and Maturity Assessment	Completed	Completed	End-Sep 2019
	iCAST	Completed (27 out of 30)	End-Sep 2019	Mid-2020



Some lessons from C-RAF

- Banks generally mature in cyber resilience, but need improvement in
 - Staff security awareness
 - Password management
 - Patching and configuration of systems

- The concept of iCAST is new to some banks

- Checklist-based assessment may bring false comfort
 - No issues identified by Maturity assessment but problems seen in iCAST (e.g. IDS/SIEM implemented but not well configured)

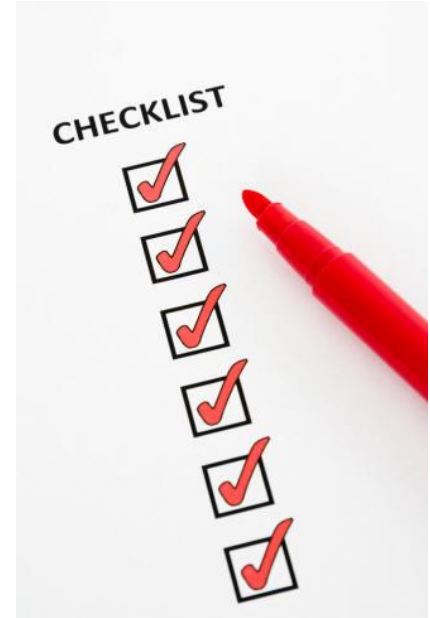




How to better prepare for iCAST

- iCAST testers common attack methods (based on threat intelligence and experience learnt):
 - Spear phishing targeting at selected bank staff
 - Unauthorized access to office premises
 - Simulated attacks originated from banks' own staff

- iCAST testers common targets:
 - Payment related systems
 - Electronic banking systems
 - Core banking systems





Professional Development Programme (PDP)

- PDP is a framework on qualifications for conducting:
 - Inherent Risk and Maturity Assessments: Recognised 7 equivalent certifications from industry
 - iCAST: Certification for individuals, exam statistics since launched

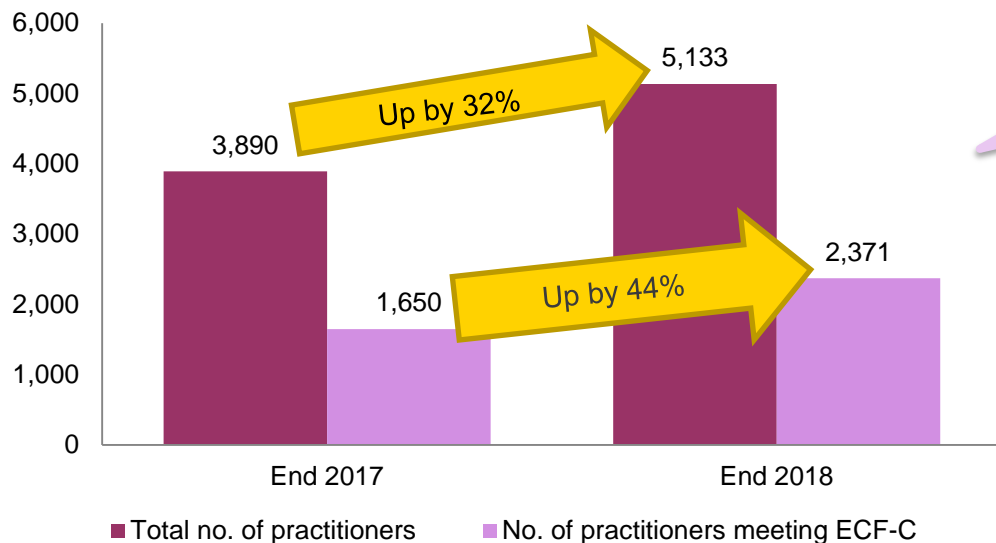
	Level	Attempted	Passed
Level 1	Practitioner	0	0
Level 2	Registered	17	10
Level 3	Certified	37	2
Level 4	Specialist	1	1

- Certification on company level may help to grow the industry



Continue to close the talent gap

➤ Enhanced Competency Framework on Cybersecurity (ECF-C)



Growing Talent Pool Size

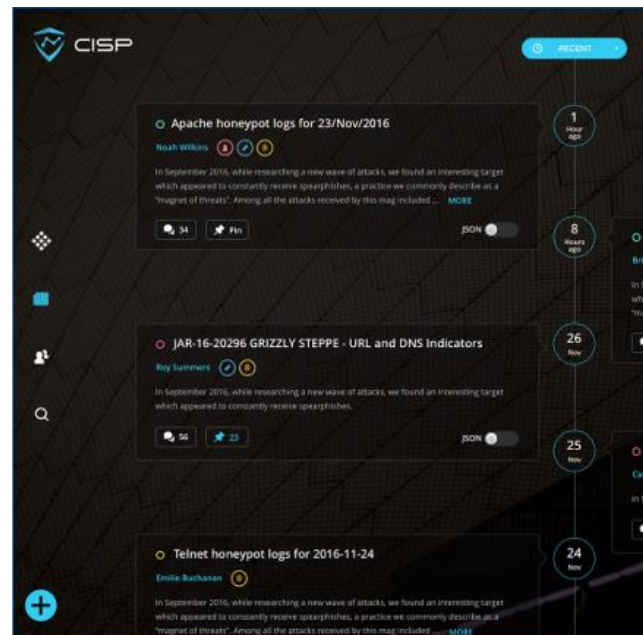
Improving Talent Quality

To further improve talent development, 6 certificates for C-RAF added to ECF-C in Jan 2019



Cyber Intelligence Sharing Platform (CISP)

- To facilitate the sharing of cyber threat intelligence by banks
- Soft launched in Dec 2017 and full launched in April 2018
- Utilisation is yet to pick up





Industry feedback

- Need harmonisation with other standards (reduce compliance efforts)
- Better clarity on assessment criteria
- Better clarity on what and when to share on CISP
- Insufficient talent
- On-going efforts?

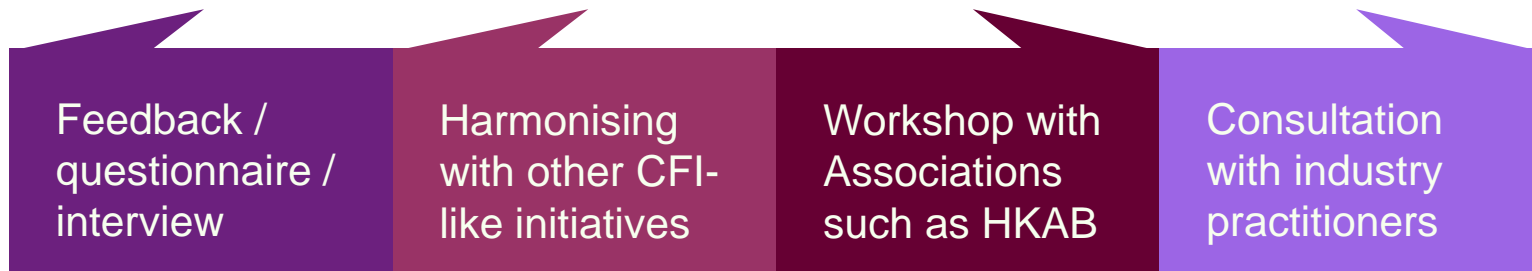




CFI review – Timeline and approach

2019	Jan	Feb	Mar	Apr	May	Jun	Jul	Aug	Sep	Oct	Nov	Dec
Survey and interview				▶								
Industry consultation								▶				
Finalise changes											▶	

Proposed approaches:





Key takeaways

- Innovation is essential and will speed up to stay competitive
- Need to properly address risk in light of increasing cyber threats
- Framework already in place to work with banks to face challenges
- Will continue to improve to cope with evolving circumstances



Thank you