BEA東亞銀行

Promoting Cooperation in Cyber Security Management

Prepared for ABA by:

Eric Wong
Group Chief Information Officer
General Manager and Head of Technology and Productivity Division The Bank of East Asia, Limited

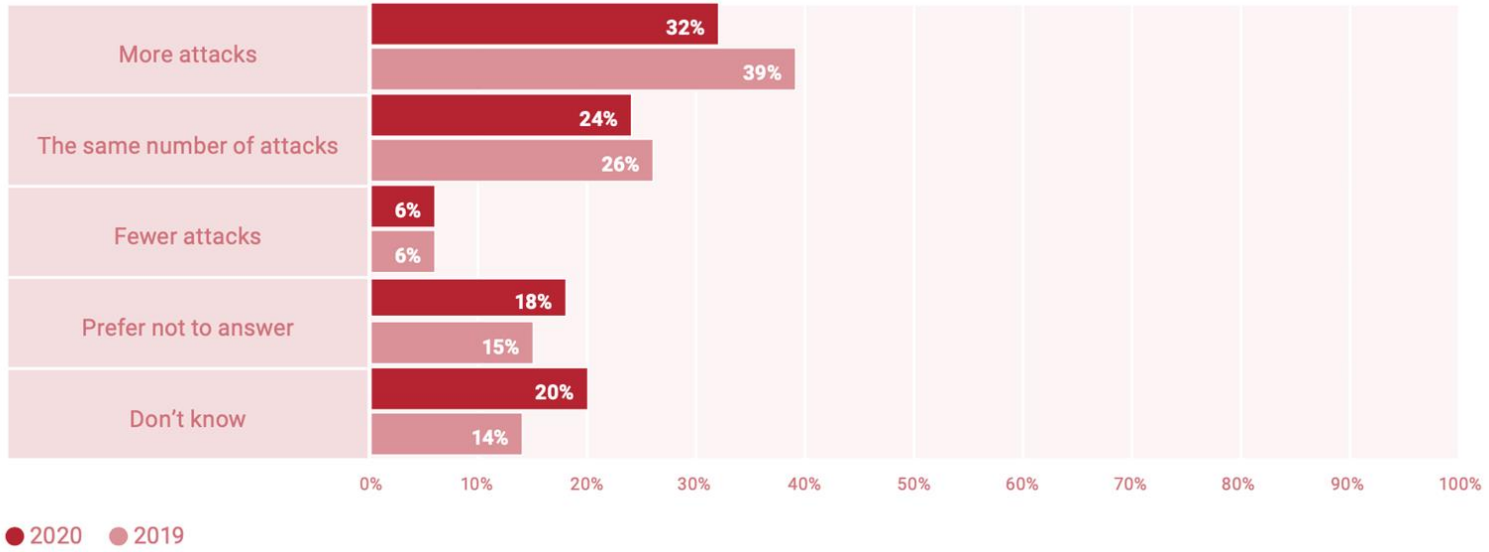
Agenda

1. Overview on Cyber Threat Landscape
2. Importance of Cyber Security Cooperation
3. Three Key Pillars of Cyber Security Cooperation
4. The Road Ahead

Overview on Cyber Threat Landscape

Cyberattacks are still increasing year over year

Statistic on global organizations experiencing the trend in cybersecurity attacks as compared to a year ago



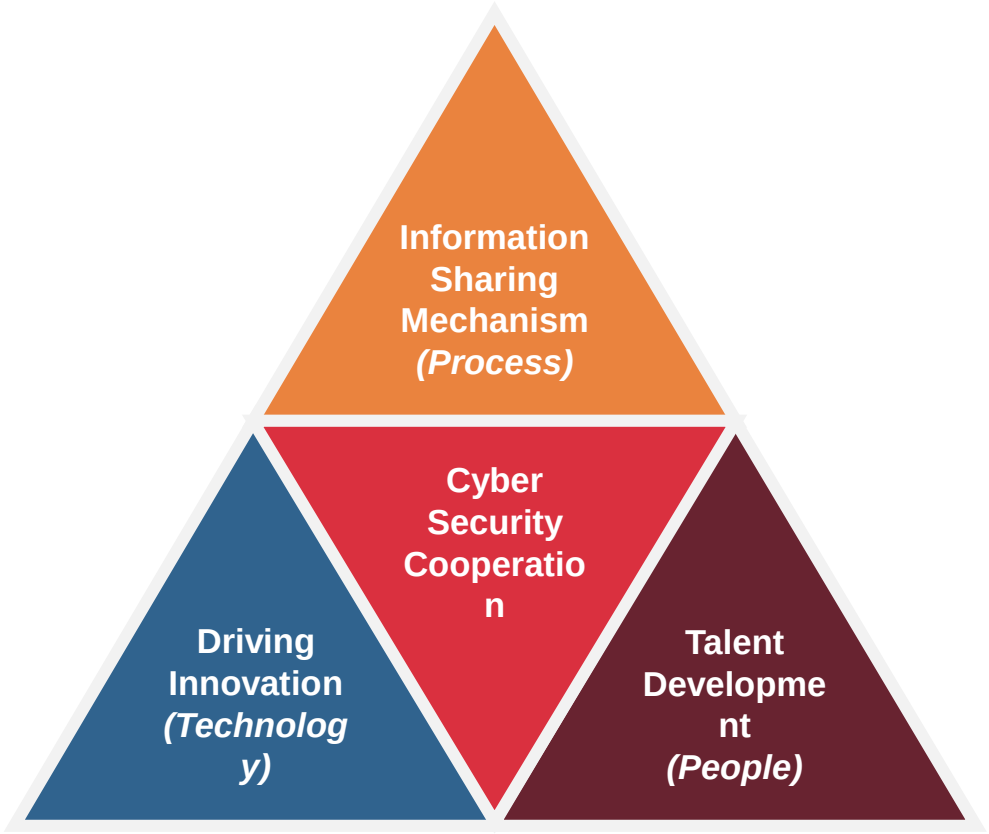
Most Common Threat Actors

1. **22%** Cybercriminals
2. **19%** Hackers
3. **11%** Malicious insiders
4. **10%** Nonmalicious insiders
5. **9%** Nation-state attackers
6. **8%** Hacktivists

Source from State of Cybersecurity 2020, Information Systems Audit and Controls Association, https://www.isaca.org/go/state-of-cybersecurity-2020

Importance of Cyber Security Cooperation

- Cyber threats have become ubiquitous and unseen which usually cause significant losses.
- To tackle with this inevitable trend requires cross-vector cooperation among banks, law enforcement agencies, regulators and the public.
- A **structured** Cyber Security Cooperation model, based on the **People, Process, Technology** Framework, for strengthening the cyber security controls to prevent cyber-attacks and to minimise the impact of successful attacks

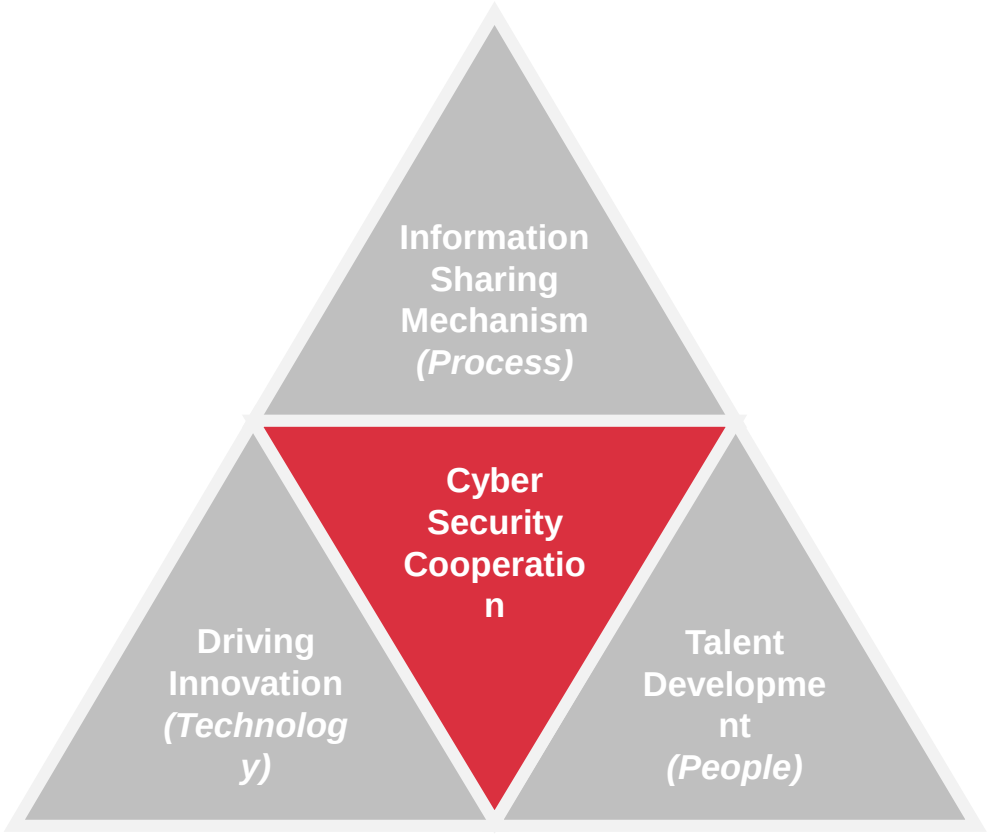


Three Key Pillars of Cyber Security Cooperatio

Importance of Cyber Security Cooperation

Hong Kong continues to strengthen and promote cyber security cooperation at various levels:

- HKMA's Cybersecurity Fortification Initiative 2.0 ("CFI 2.0") to the banking industry
- HKPF's cyber security services to critical infrastructure
- Dedicated taskforces and working groups for various industries

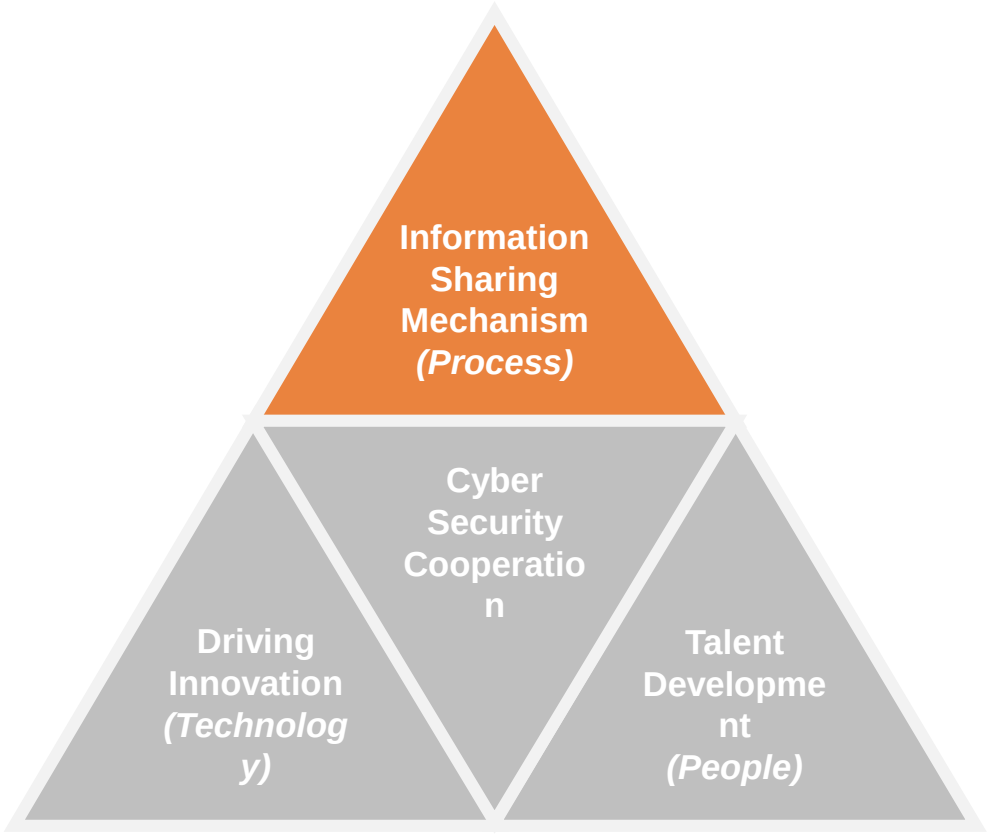


Three Key Pillars of Cyber Security Cooperatio

Three Pillars – Information Sharing Mechanism (Process)

Proactive information sharing to avoid the faults other industry peers come across and to build effective cyber resilience:

- Centralised and regulator/community-driven sharing platform
- Sharing of Indicator of Compromise ("IOCs")
- Sharing of cyber-attacks approach and guidance on defense measures

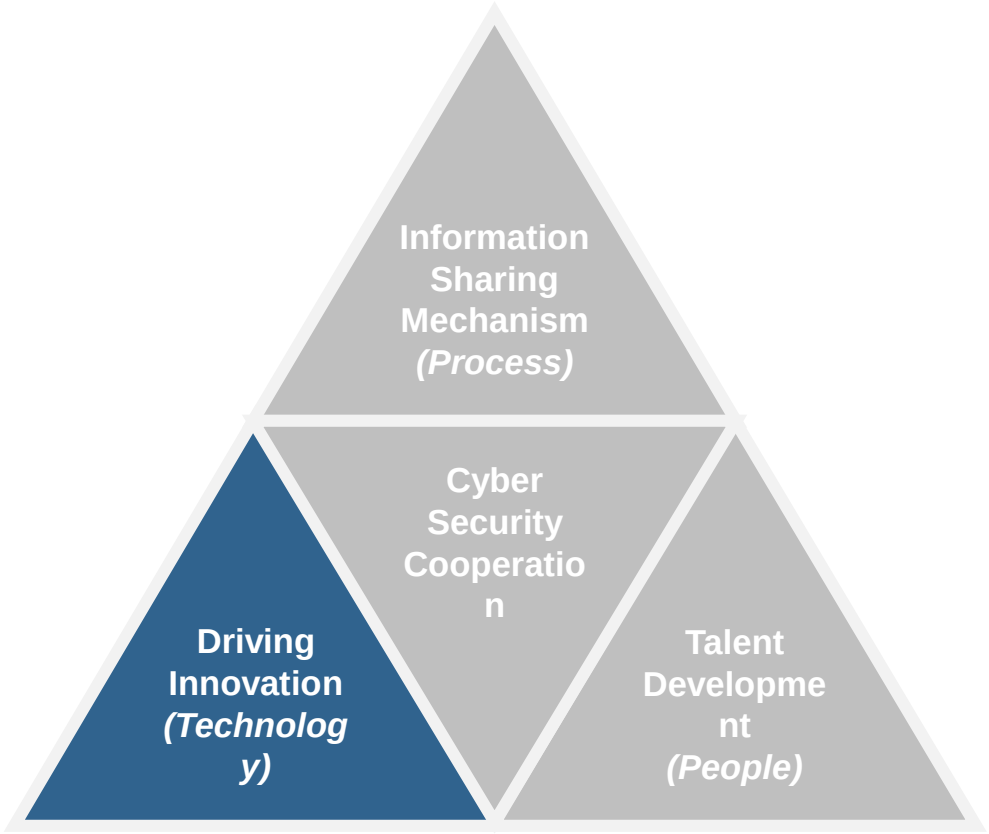


Three Key Pillars of Cyber Security Cooperatio

Three Pillars – Driving Innovation (Technology)

To foster innovation through facilitating a standardised and risk-controlled technology adoption journey:

- Banks' control functions work hand-in-hand to manage cyber security risks
- Regulatory guideline on emerging technology, e.g. OpenAPI, remote account opening and RegTech
- Regulatory sandbox approach

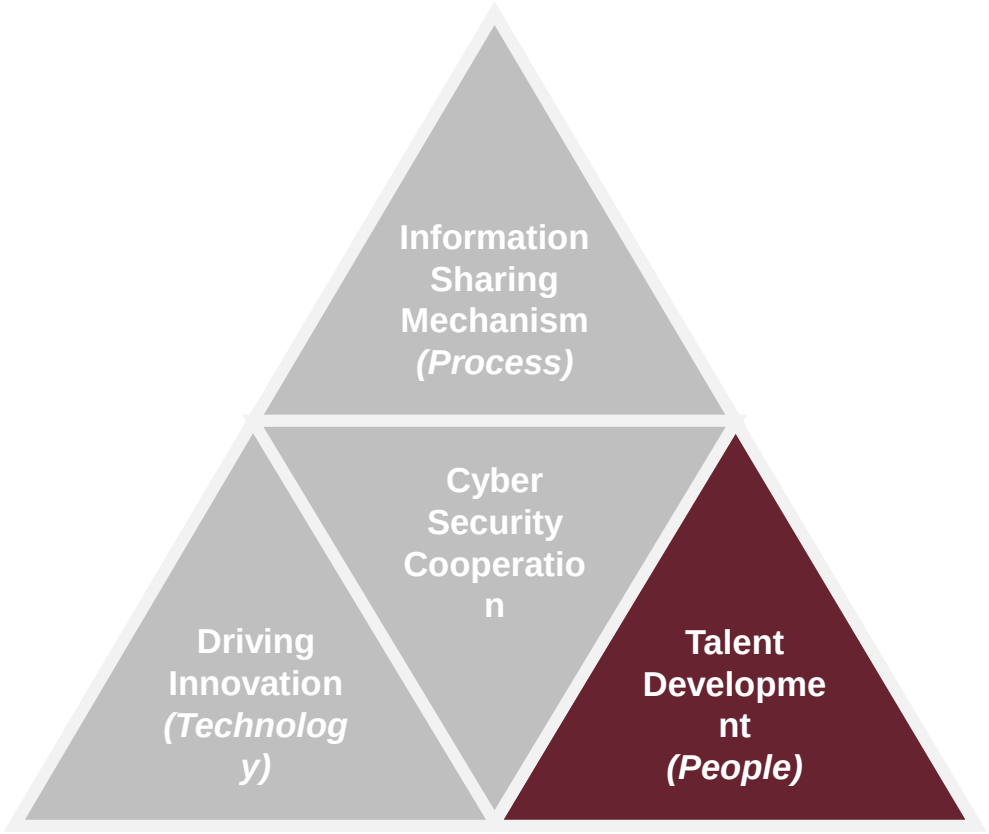


Three Key Pillars of Cyber Security Cooperatio

Three Pillars – Talent Development (People)

"People" is the most important element in bringing a successful cyber security cooperation. A multiparty-driven and industry-wide programme should be implemented to fill up the gap in cyber security talents:

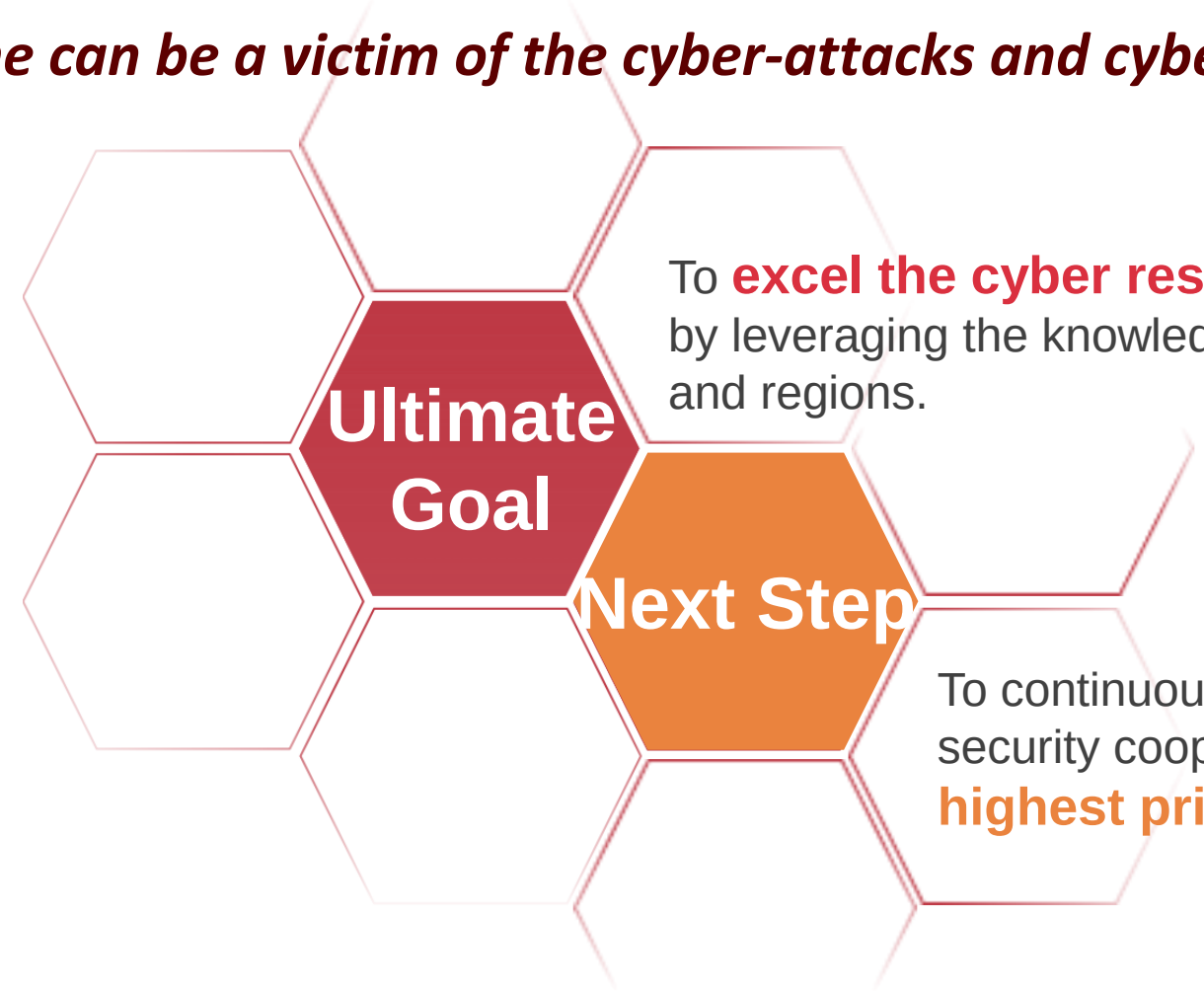
- Uplifting the competency standards
- Enabling effective trainings



Three Key Pillars of Cyber Security Cooperatio

The Road Ahead

Everyone can be a victim of the cyber-attacks and cyber-crime…



To **excel the cyber resilience capabilities** of a single entity by leveraging the knowledge and experiences across industries and regions.

To continuously advance and deepen the cyber security cooperation and putting this as one of the **highest priority** items in the cyber security strategy.

BEA東亞銀行

Thank You!