Managing Cyber Risks as Regulators

15th Annual International Conference on Policy Challenges for the Financial Sector
3-5 June 2015

Ho Hern Shin
Monetary Authority of Singapore
Evolving Cyber Threat Landscape

**FUN**
Technically curious individuals

**FAME**
Technically adept groups leaving their mark on public websites

**FORTUNE**
Cyber criminals, organized gangs stealing money, data ransom schemes and competitive information

**FORCE**
Nation states and non-nation state groups launching targeted attacks for strategic purposes

Year:
- 1988
- 2001
- 2004
- 2010
Evolving Cyber Threat Landscape

117,260 security incidents per day, every day in 2014

Source: Global State of Information Security Survey 2015 (PWC)
Changing Mind-sets

- **Not if, but when**
  - Operational resilience crucial
  - Minimise disruption and impact of successful attack

- **From elementary defences to cyber resilience**
  - Basic ICT controls
  - Multilayered defences
  - Security by design

- **Board and senior management attention**
  - Upskill board and senior management
  - Focused cyber security function
Changing Mind-sets

- The enemy is already within
  - Most intrusions undetected for more than 6 months

- Situational awareness
  - Threat intelligence
  - Predictive analytics

- Beware the weak links
  - 3rd party vendors
  - Staff
  - Smaller institutions

- Collaboration
  - This war cannot be won alone
Supervisory Approach

Three Possible Pillars to Support Effective Supervision

- Policy & Supervision
- Surveillance & Exploration
- Coordination & Collaboration

Cyber Resilient Financial Ecosystem
**Goal:** Influence and shape financial institutions’ cyber security capability from elementary defences to a state of cyber resilience
Surveillance & Exploration

**Goal:** Supervisory policies and approaches keep pace with evolving cyber threat landscape

- Scan horizon for emerging cyber risks
- Explore new security technology and solutions
- Research to understand system and technology vulnerabilities
Coordination & Collaboration

**Goal:** Leverage on collective strength to engender cyber resilience

- Enable cyber intel sharing
- Coordinate response and recovery
- Co-create industry standards
In Summary

- The fight against cyber threat is never ending

- Regulators play an important role
  - Set clear expectations and standards
  - Hold financial institutions accountable
  - Maintain a watchful eye over emerging cyber threats
  - Encourage and facilitate collaboration

- Learn and evolve

- Partnership matters
Thank You