SWIFT Institute

NANYANG TECHNOLOGICAL UNIVERSITY SINGAPORE

Productivity of Cybersecurity Investment:
A Singapore Framework

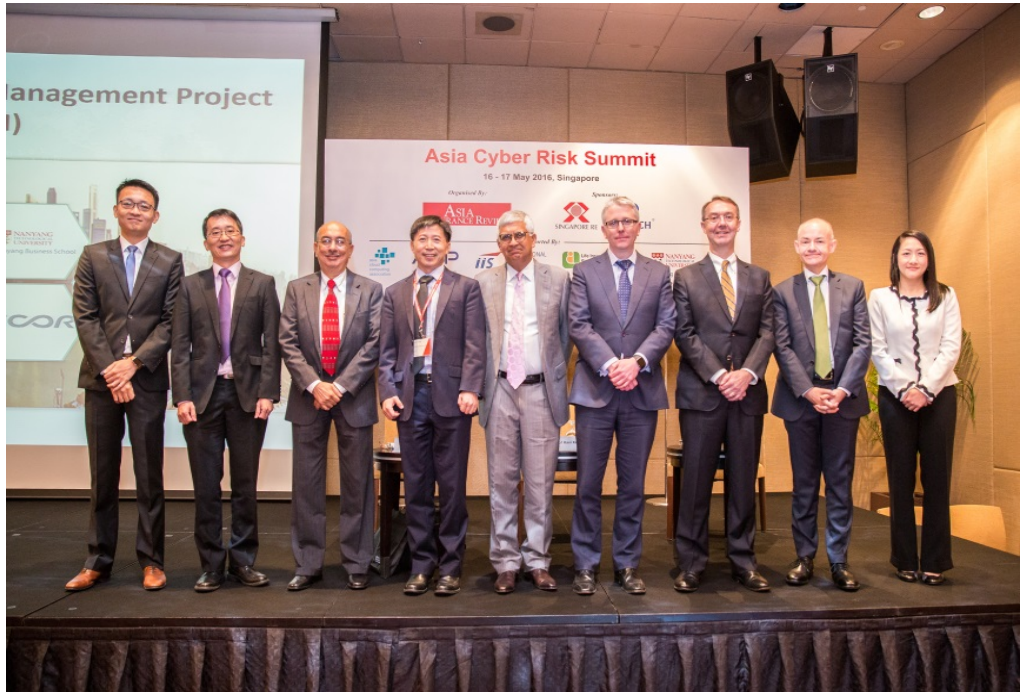
Professor Shaun Wang

Director of the NTU-MAS CyRiM Project

shaun.wang@ntu.edu.sg

NTU-MAS Cyber Risk Management Project (CyRiM)

- Three-year project 2016-19
- **Partners:**
  - Nanyang Technological University (NTU)
  - Monetary Authority of Singapore (MAS)
  - Cyber Security Agency of Singapore (CSA)
  - SCOR, Aon, MSIG, Lloyd's; TransRe
  - Geneva Association; Verizon



Goals of the NTU-MAS CyRiM project

- Marry technology and business approaches
- Develop theoretical framework
  1) guiding cybersecurity investment and cybersecurity assurance product design
  2) making policy recommendation on measures to enhance cyber resilience
- Bridge “Theory” ➔ “Practice” by Database & Analytics
  - ➢ Special focus of the financial sector

Recognize the Multi-facets of Digitization and Cyber Risk

- Project team met various stakeholders: Banking CISOs, InfoSec experts, law-enforcers, Insurance underwriters, Institutes and NGOs
- Some identified challenges

✓ Rapid changing technology: cloud computing, internet of things, encryption, new malware

✓ Language barriers between business people and IT experts

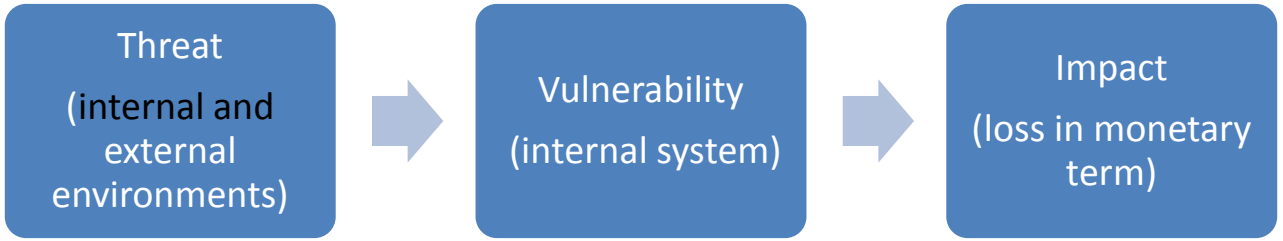
✓ Fragmentation of legal jurisdictions

✓ Difficulty in attribution of responsibility in inter-connected network

Feedbacks from Various Stakeholders

- Executives of the financial sector:
  - Pressure from the digitization trend and disruptive technology (e.g. Blockchain and mobile pay)
  - Increasing cyber threats and compliance requirements (e.g., Singapore new Cybersecurity Bill requires CII owners to conduct audit and risk assessment)
- CISOs: asking for benchmarks for cybersecurity budget and effectiveness of spending
- Interpol: overwhelmed by case load, low enforcement rate, lack of resources
- Lawyers in uncharted territory of digital economy

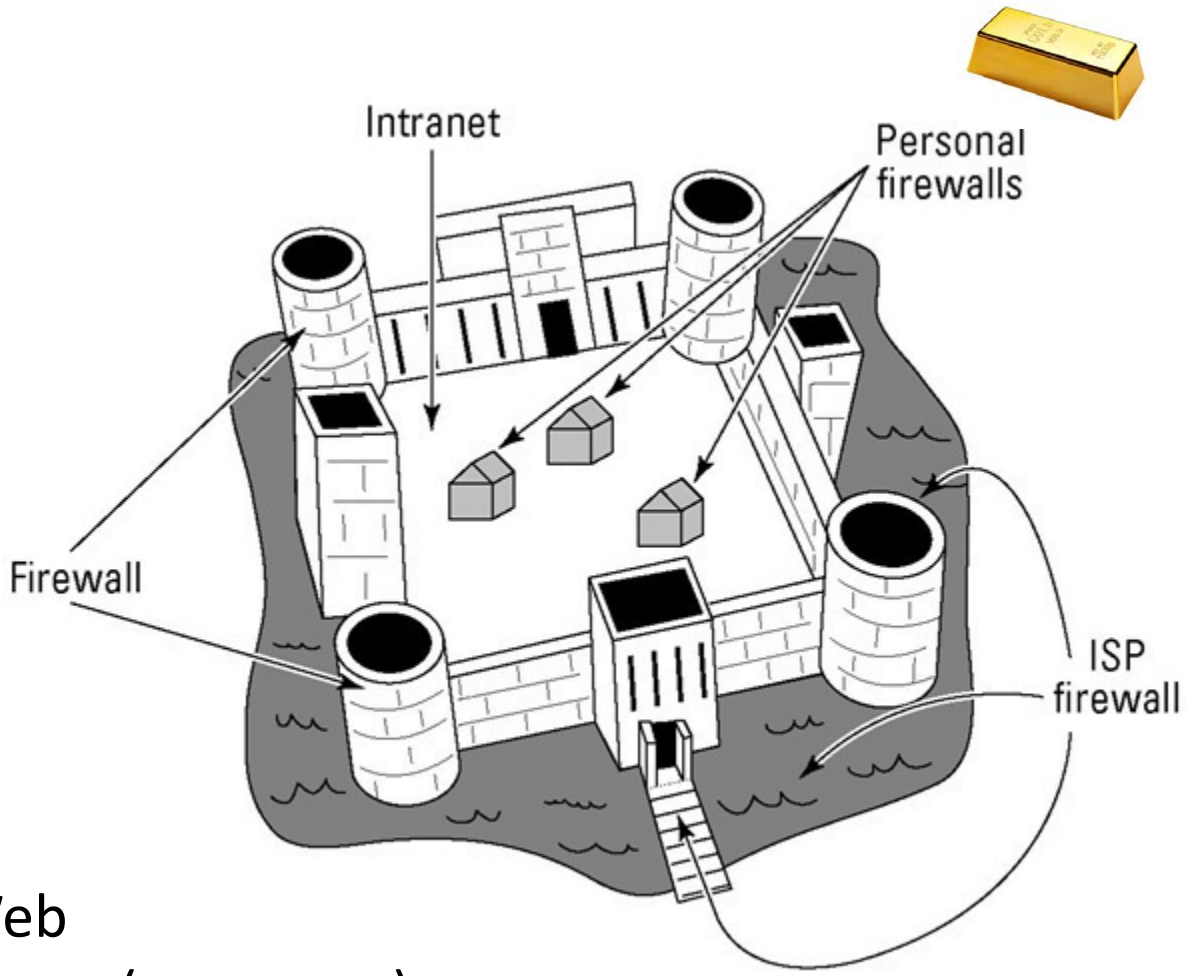
Framework for Quantifying Cyber Risk



- The **threat** or the number of cyber threats *n*.
- The **vulnerability** or probability *v* of a successful data breach arising from a cyber threat.
- The i**mpact** or monetary loss, λ, in the event of an actual data breach occurring.
- The remaining **annual loss expectancy**

$$loss_{firm} = n \cdot v \cdot \lambda$$

Illustration: Threats, Vulnerability and Impact



Fast-growing Dark Web
Malware & Ransomware (arms race)

Dimension 1. Investment to address Vulnerability

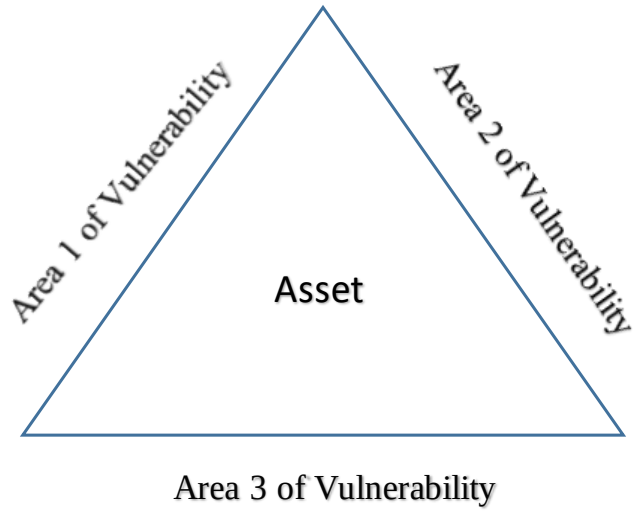
- Choose a benchmark spending *B and* cyber breach probability $v(1)$
- With spending *Y* and spending ratio *y=Y/B*, cyber breach probability $\mathrm{v}(y) = 1 - [1 - v(1)]^{y^{\beta}}$,

  [This is the proportional hazard model: $h(y) = h(1) \cdot y^{\beta}$]

β -- *effectiveness* of spending in reducing vulnerability

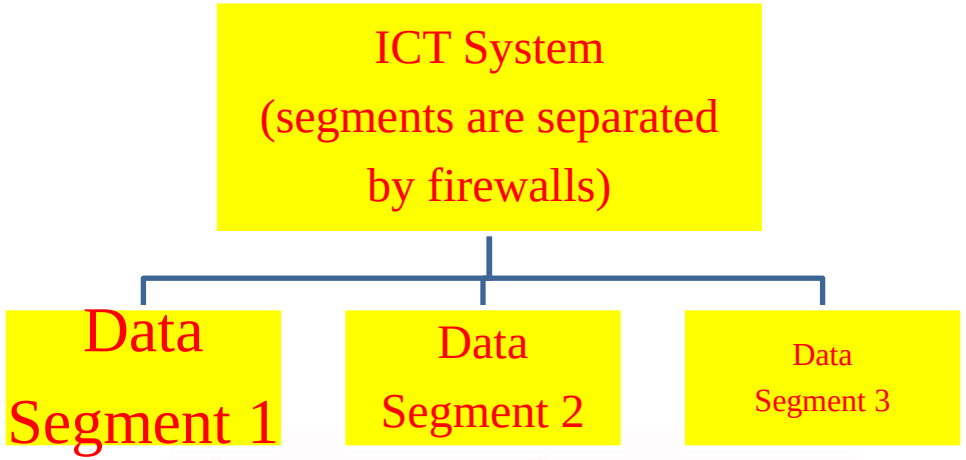
- Increasing spending reduces vulnerability, but at declining rate
- *Examples of effective measures:*
  - *2-factor authentication in online banking;*
  - *timely update of software*
  - *Employee training*

Multiple Areas of Vulnerability: competing hazards model



Model Insight: Important to cover all areas of vulnerability

Prioritise Data Assets



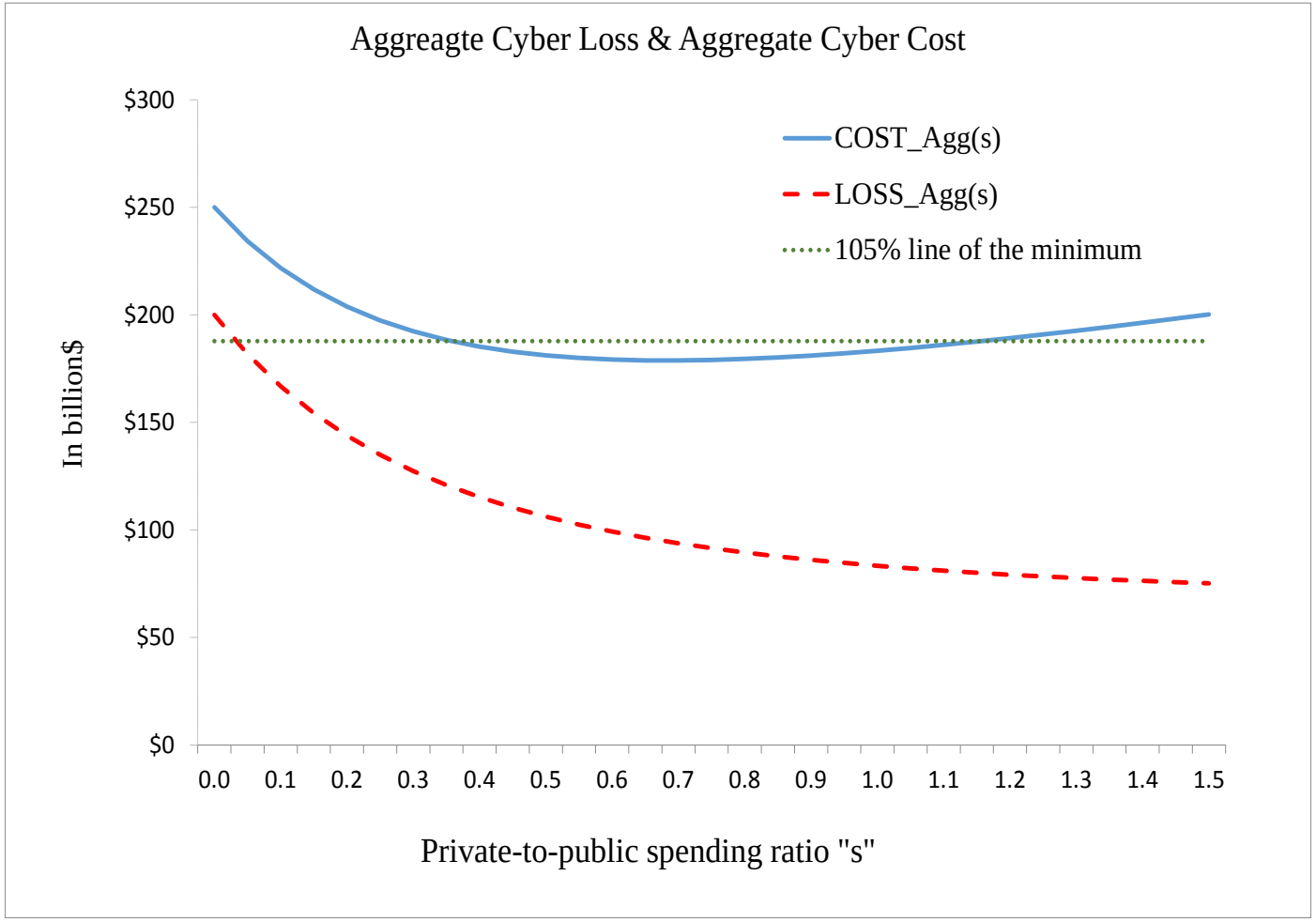
Dimension 2. **Address Threats** through Private-Sector Collective Spending

- 2015 global government spending in addressing threats is *G*=$50 billion, but no private sector *collective* spending, aggregate cyber loss is $LOSS_{Agg}(0)$= $200 billion
- Private sector *collectively* contribute "*S*" to address cyber threats, $s = S/G$ is private-to-public spending ratio.
- With private sector *collective* spends $S = s \cdot G$ to address cyber threats,

$$LOSS_{Agg}(s) = LOSS_{Agg}(0) \cdot (1+s)^{-\alpha}$$

Index α is effectiveness of collective spending (coordination)

Example: Effect of Private-Sector Collective Spending on Aggregate Cyber Cost



Firm level: number of threat is reduced

- If private sector collective spending $S = s \cdot G$, the Firm's contribution to collective spending equals $X = s \cdot A$ with

$$\mathrm{A} = G \cdot \frac{loss_{Firm}(0)}{LOSS_{Agg}(0)}$$

- the Firm faces a number of cyber threats:

$$n(s) = n(0) \cdot (1 + s)^{-\alpha}$$

Dimension 3: Monetary impact of cyber breach

- Post cyber breach, the speed of emergency response affect the loss and expense impact
  - $\lambda(T)$ increases with response time T
- Pre-event segmentation reduces loss
- Pre-event "assurance" coverage can help soften demand surge for investigation and legal services
- Alternative business back-up plan helps reduce business disruption cost

Dimension 4: The Network Effect

- A large portion of cyber threats come from interconnected network (clients and service providers)
  - 2003 Target data breach attributed to a contractor
  - Malware APT on Bangladesh Bank in Feb 2016
- Impose cyber liability insurance can help firms to instill responsibility to others in the network economy
- Well coordinated collective efforts can enhance the security of the whole network

Implications of the 4-dimensional Framework

- A common framework for banks to customize their own calibrations
- Quantifies the benefit of ERM approach, combining technical defense, risk management, corporate governance and employee training
- Calculates the benefit of greater international coordination in countering cyber crime
  - E.g. Private sector collective contribution to resource for engaging law enforcement in pursuing criminals and seek loss recovery, and intelligence sharing
- Economic benefit of prescribing baseline security measures across firms and jurisdictions to optimize network effect

Cyber Assurance Pooling Arrangement

1. Standard “Cyber Assurance” (tailored for the banking sector) to be jointly offered to banks by participating insurers and InfoSec firms
2. Include preventive services to address *vulnerability*
3. Provide post-breach response services
4. *Guaranteed* insurance payment of losses and expenses, assigning the *right* of seeking loss recovery
5. Risk-based pricing incentivizes increased security investment by firms
6. Serve as means to facilitate private sector collective spending to counter cyber crime
7. Cyber Assurance to qualify as cost-effective way of achieving compliance for banks

Further Research needed

1. Quantify the impact of traceability of transactions, usage of BlockChain, multi-factor authentication in reducing threat, vulnerability and impact.
2. The network effect: Incentives, Liability and Markets for cyber breach risk (just like CDS or trade-credit insurance)
3. Use the 4-dimensional framework to identify areas of international coordination that have maximum potential in increasing cybersecurity productivity

Academic References:

- Lawrence A. Gordon and Martin P. Loeb (2002) “The economics of information security investment”, ACM Transactions 5 (4), 438-457
- L. Jean Camp and Catherine D. Wolfram (2004), “Pricing Security: Vulnerabilities as Externalities”, Economics of Information Security.
- Kanta Matsuura (2008), “Productivity Space of Information Security in an extension of the Gordon-Loeb’s Investment Model”, Springer monograph on Managing Information Risk and the Economics of Security, pp 99-119
- Herley, Cormac (2009) “So long, and no thanks for externalities: the rational rejection of security advisors by users”, Association for Computing Machinery
- Shaun Wang (2017), “Integrated Framework for Information Security Investment and Cyber Insurance”, 2017 American Risk and Insurance Association Annual Meeting, Toronto