HKUST
BUSINESS SCHOOL
香港科大商學院
WORLD CLASS IN ASIA

Cybersecurity: Challenges and Recent Developments

Prof. Kai-Lung Hui (許佳龍)
Department of ISOM, HKUST Business School

for

SAS ESSEC Cyber Risk Conference, Singapore

Recent Incidents (1)

HKUST BUSINESS SCHOOL 香港科大商學院
WORLD CLASS IN ASIA

Biggest attack vector in finance: SWIFT

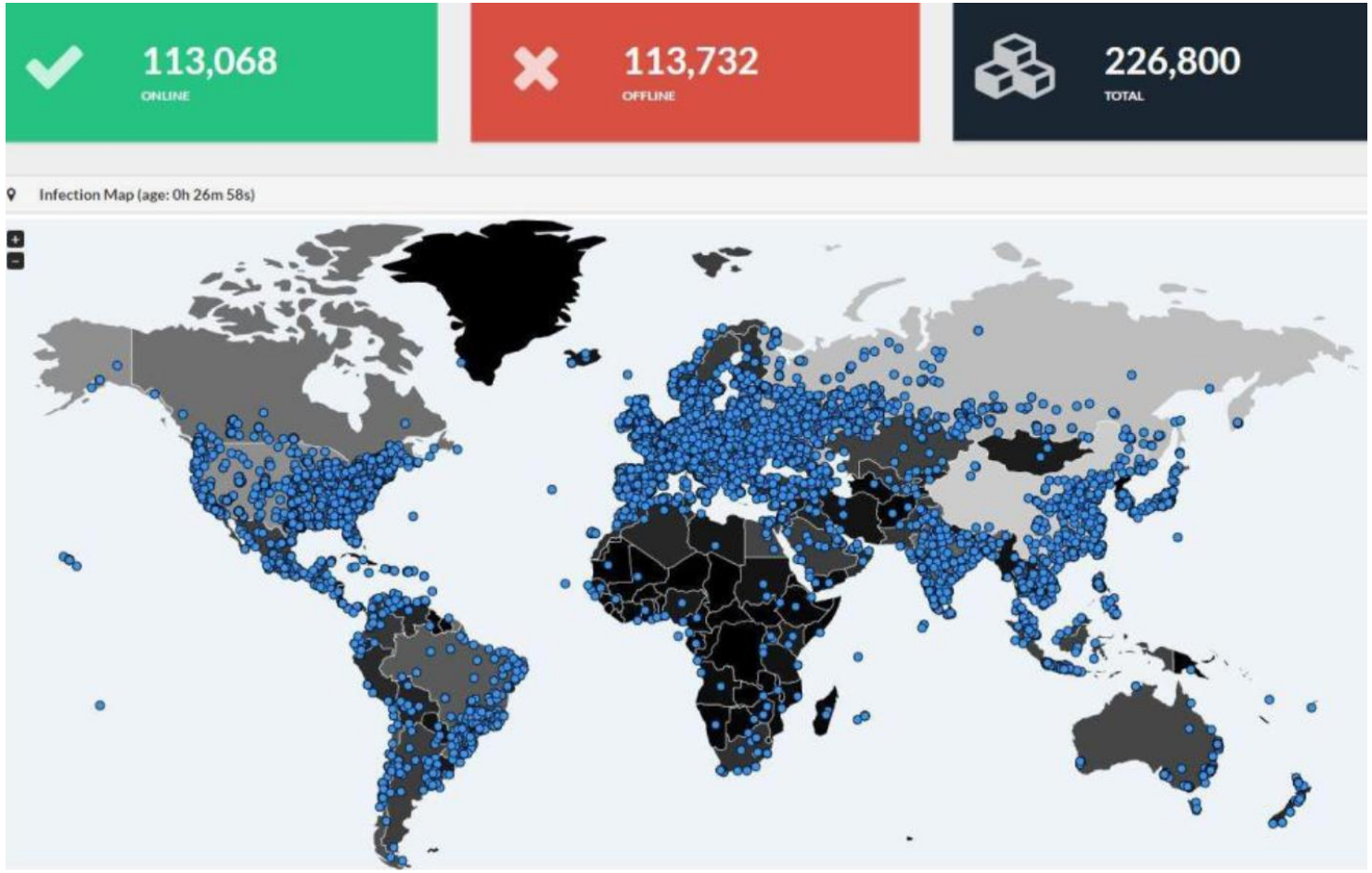
The Society for Worldwide Interbank Financial Telecommunication (SWIFT) is a global transaction messaging network used by banks and other financial entities such as foreign exchanges and investment firms. Unfortunately, this year saw attackers targeting SWIFT clients, compromising and manipulating organizations into sending fraudulent money transfer requests. It's unclear how many of these attacks were actually successful, but in June, SWIFT sent its clients a letter warning them about the possible dangers. The organization also urged clients to update their software and tighten their cyber defenses.

Source: Trend Micro

Bangladesh Bank was the highest profile victim of SWIFT fraudsters, but it was also disclosed that Ecuadorean bank Banco del Austro fell victim to a SWIFT attack in 2015.

The bank lost $12 million when hackers gained access to the codes the bank used to move money via SWIFT. The stolen cash was moved to accounts in Hong Kong, Dubai, New York and Los Angeles.

Recent Incidents (2)



- WannaCry attack map after 24 hours
- Demanded US$300 in Bitcoin per computer
- Other famous ransomware in 2017 includes Petya and Bad Rabbit

Image source: The Sun

Biggest Data Breaches

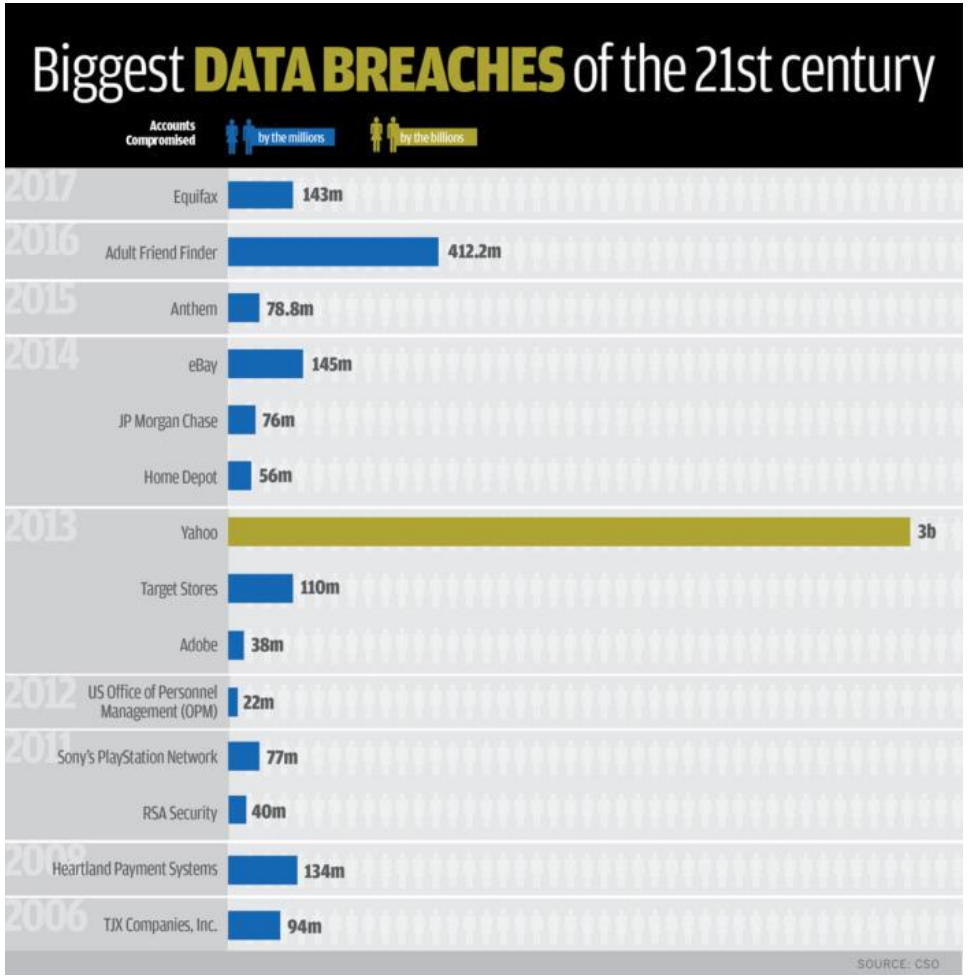


Image source: CSO Online

Equifax's stock has fallen 31% since breach disclosure, erasing $5 billion in market cap

Published: Sept 14, 2017 6:25 a.m. ET

Credit-reporting company's shares rallied Tuesday, but fell 15% Wednesday and are down in premarket action Thursday

Image source: Market Watch

Major Vulnerabilities

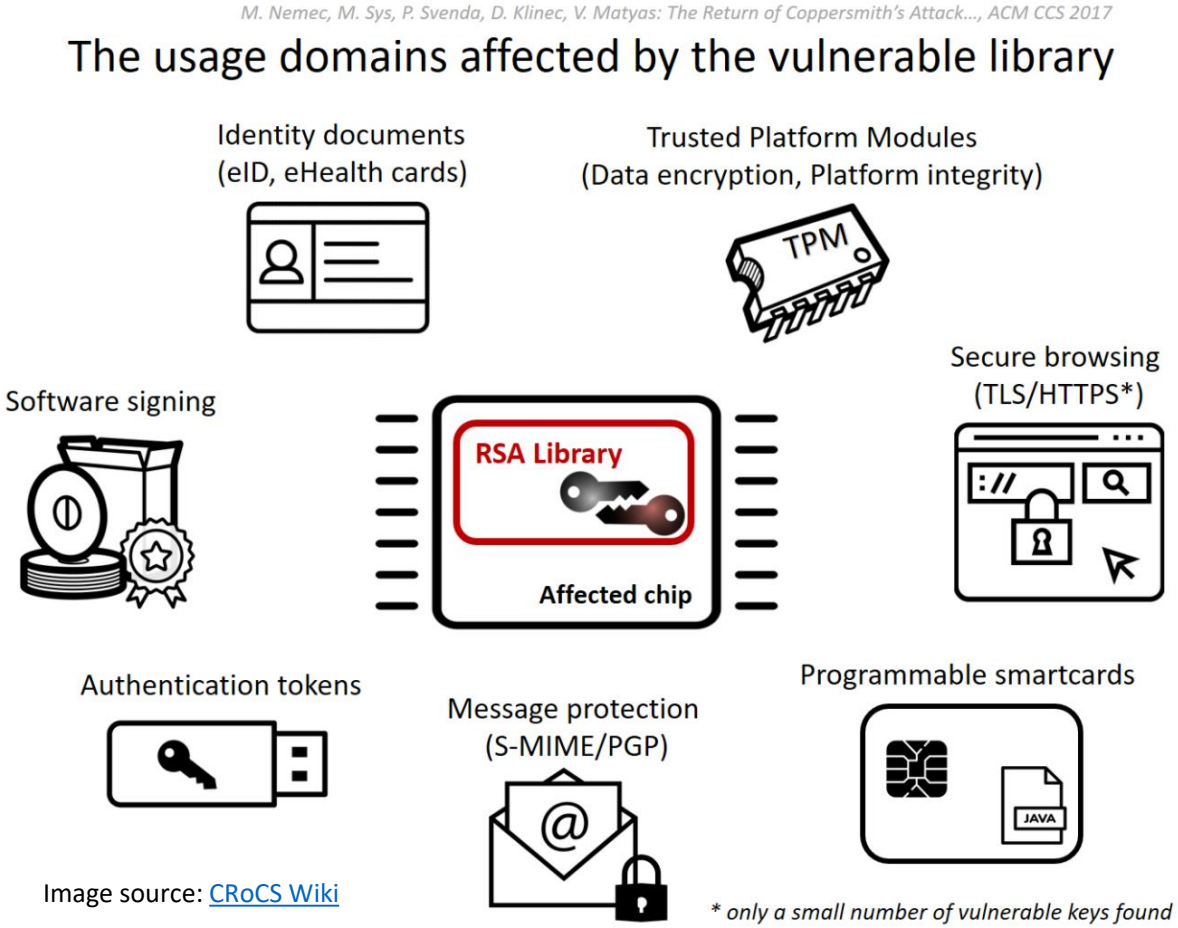


Image source: CRoCS Wiki

- Now, Meltdown and Spectre, which exploit a loophole in CPU design (meant for enhancing execution efficiency)

Nature of the problem

HKUST BUSINESS SCHOOL 香港科大商學院
WORLD CLASS IN ASIA

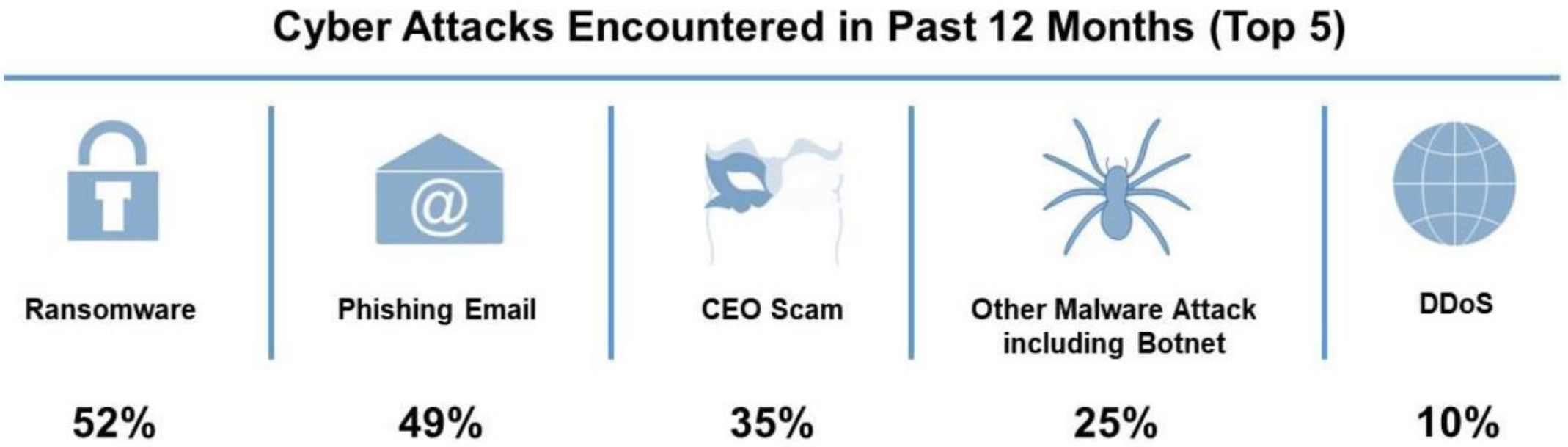
- Technology development
  - High interconnectivity of the Internet
  - Emergence of net-enabled businesses and the so-called “sharing economy”
  - Growing use of sensors and IoT
- People factor
  - More sophisticated attackers
  - Insufficient user-end awareness and precaution
- National policies
  - Update of regulatory frameworks and international collaboration

Global Trends/Predictions

HKUST BUSINESS SCHOOL 香港科大商學院
WORLD CLASS IN ASIA

McAfee Labs	Trend Micro	Kaspersky		ISF	Symantec
Connected home devices and privacy	Internet of Things (IoT)	Mobile malware	IoT hacks: router and modem	Internet of Things (IoT)	File-less or file-light malware
Server-less apps present new vulnerabilities	Enterprise application vulnerabilities	Destructive attacks, wiper ransomware, and cyber warfare	Supply chain attacks	Crime-as-a-service	Security-as-a-service (SaaS) and IaaS security
High-value ransomware targeting	Ransomware and digital extortion	Identity thefts	Cryptographic vulnerabilities	Supply chain risks	Attack on the cryptocurrency ecosystem
Children's privacy	Business email compromise (BEC)	Use of robots in social media	UEFI and BIOS attacks	Regulation	IoT, financial Trojans, and ransomware
Machine learning arms race	Cyber-propaganda and fake news	Profiling of targets to identify vulnerabilities		Unmet board expectation on security return	Supply chain attacks
	Regulation				AI and machine learning attacks
	Machine learning and blockchain				Attacks against automation movements such as DevOps

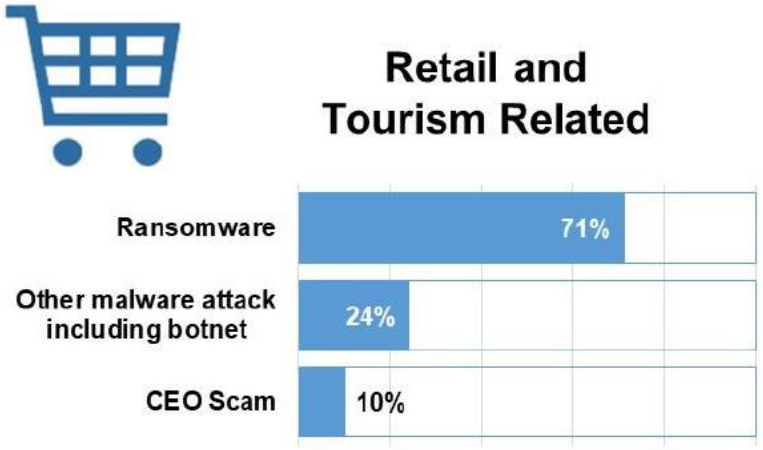
Major Threats: HK Example

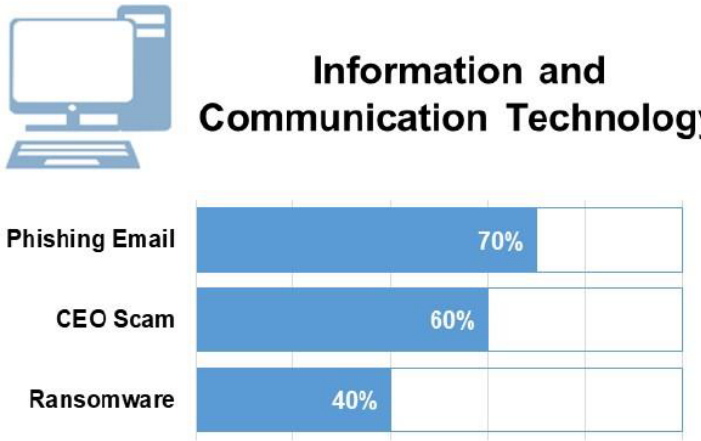


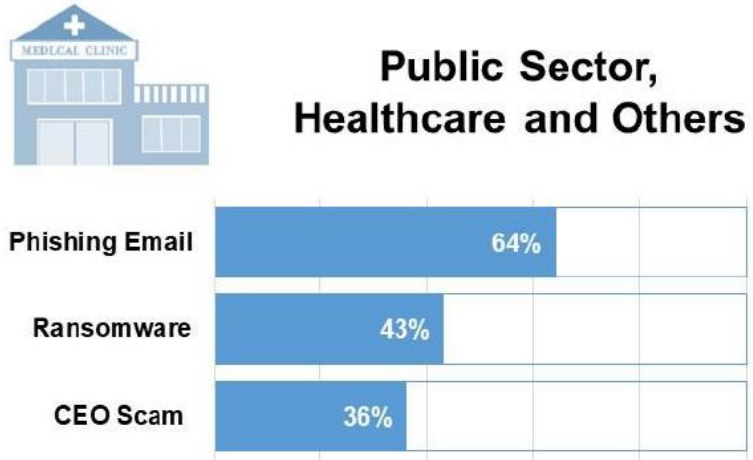
Source: SSH Hong Kong Enterprise Cyber Security Readiness Index 2018 Survey

Major Threats: HK Example

HKUST BUSINESS SCHOOL 香港科大商學院
WORLD CLASS IN ASIA







Source: SSH Hong Kong Enterprise Cyber Security Readiness Index 2018 Survey

Cybersecurity Readiness

HKUST BUSINESS SCHOOL 香港科大商學院
WORLD CLASS IN ASIA

	Average Rating (0-100)						
Indicator	FS	RT	MTL	ICT	PS	PHO	All
1. Security Risk Assessment	64.8	50.5	40.3	60.3	58.8	39.0	49.4
2. Technology Controls - Cyber Threats Detection	52.8	26.8	39.3	37.3	46.3	34.8	36.9
3. Process Control	71.2	54.8	51.9	60.7	62.8	58.8	57.3
3.1 Privileged Access Management	73.5	65.0	58.0	66.3	68.5	65.5	64.1
3.2 Data Backup Management	97.8	86.5	85.3	89.3	92.5	84.0	87.8
3.3 Third Party Risk Management	42.3	13.0	12.3	26.5	27.3	27.0	19.9
4. Human Awareness - Cyber Security Awareness Education	53.3	33.3	36.5	48.5	30.3	49.3	38.8
Sub-index of business category	**60.5**	**41.3**	**41.9**	**51.6**	**49.5**	**45.5**	**45.6**

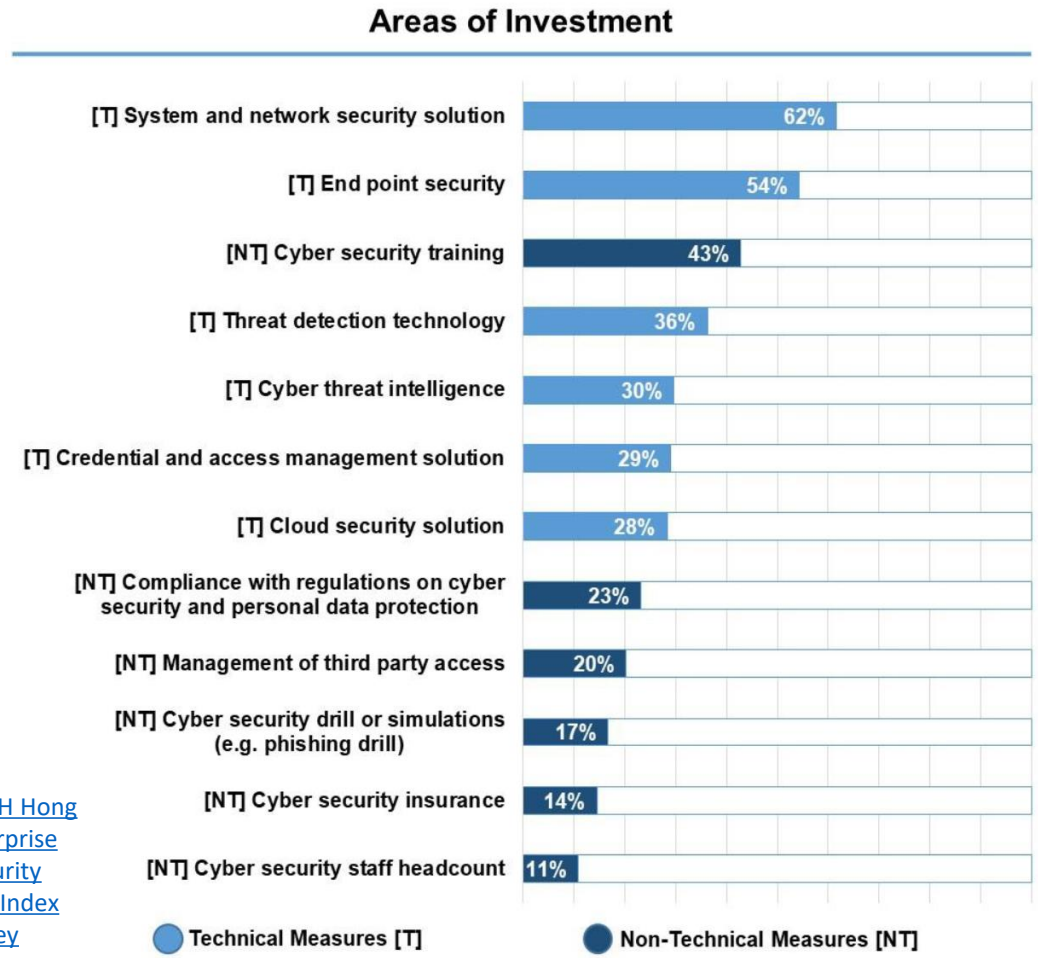
FS: Financial Services **RT:** Retail and Tourism related **MTL:** Manufacturing, Trading and Logistics

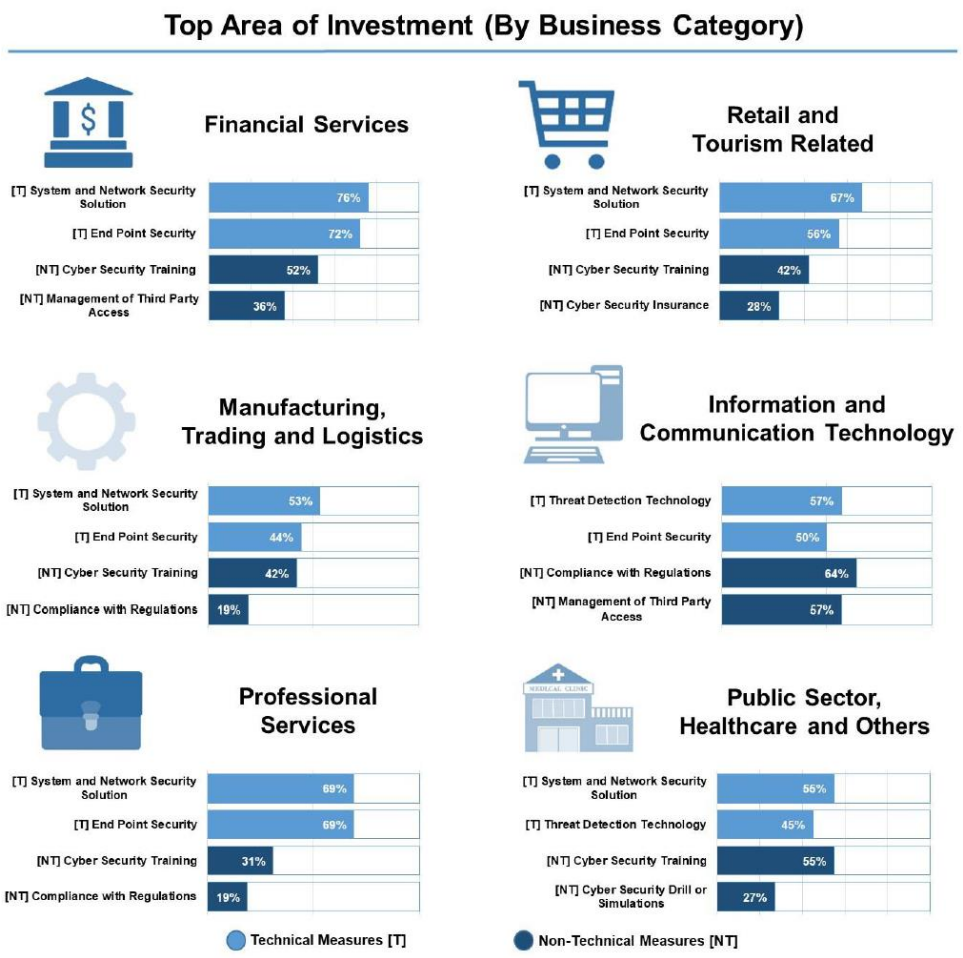
ICT: Information and Communication Technology **PS:** Professional Services **PHO:** Public sector, Healthcare and Others

All: All Business Categories

Source: SSH Hong Kong Enterprise Cyber Security Readiness Index 2018 Survey

Investment Focus

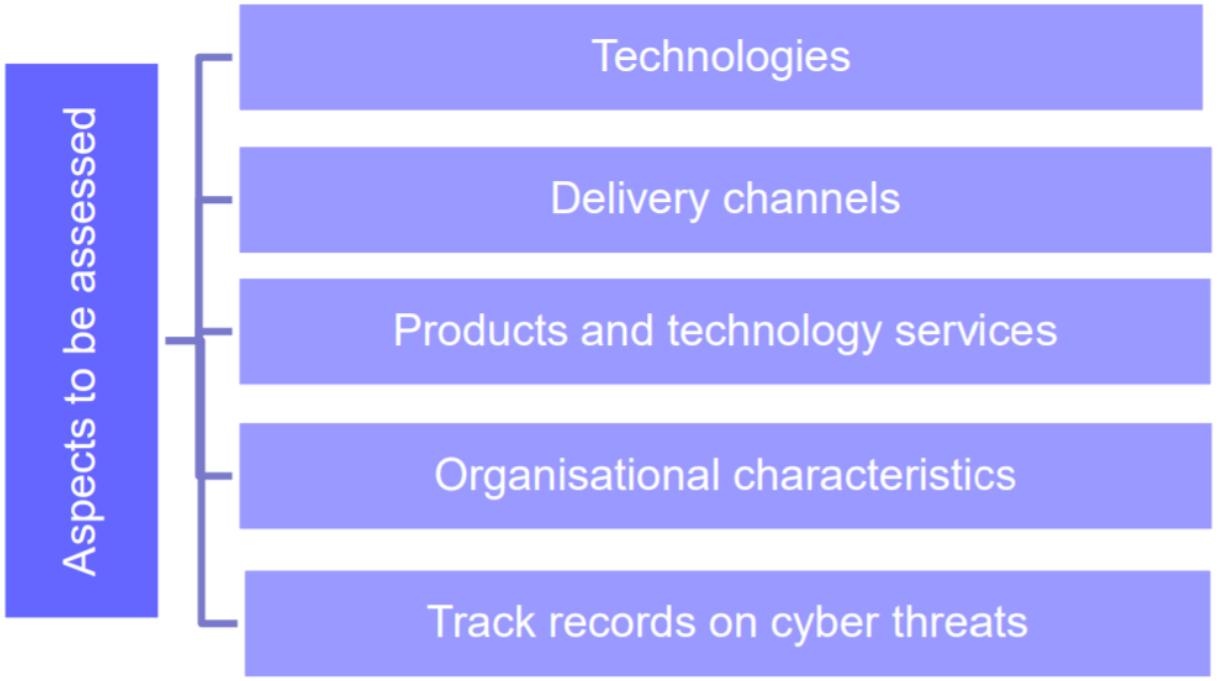




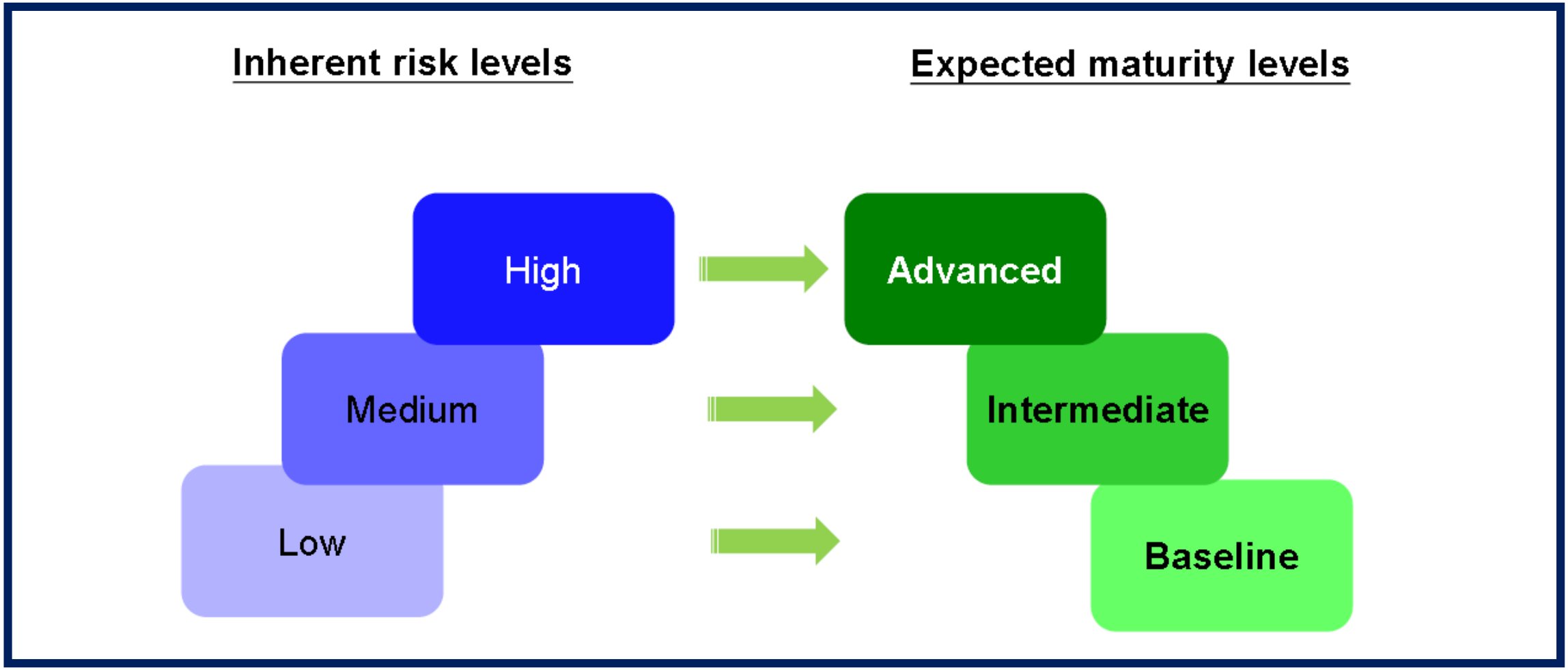
Source: SSH Hong Kong Enterprise Cyber Security Readiness Index 2018 Survey

Regulation: HK Example

- HKMA's Cyber resilience assessment framework (C-RAF)
  - Inherent risk assessment
  - Cyber maturity assessment
  - Roadmap for improvement



HKMA's C-RAF


Inherent risk levels
Expected maturity levels
High
Medium
Low
Advanced
Intermediate
Baseline

Other Developments in the Industry

HKUST BUSINESS SCHOOL 香港科大商學院
WORLD CLASS IN ASIA

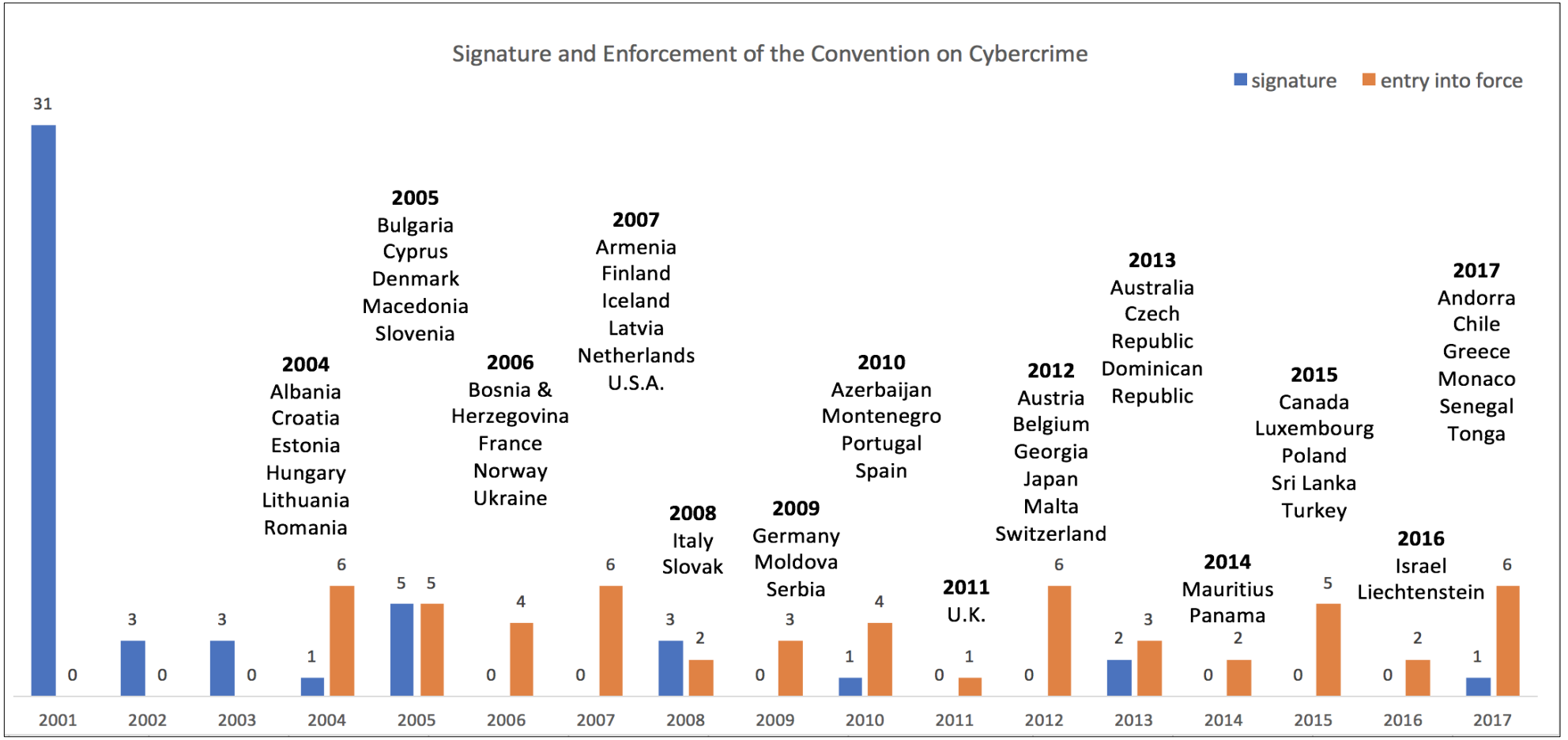
- Security intelligence systems
- Cyber insurance
- AI and machine learning in security detection and protection
  - Obviously, in security attack too!
- Blockchain
  - High data security and usability
  - Collaborative transaction and processing (increase risk or protection?)

Cybersecurity Strategy

HKUST BUSINESS SCHOOL 香港科大商學院
WORLD CLASS IN ASIA

- All of these developments are practically doing (and extending) what we have been doing over time
- They help reduce risks due to cybersecurity, but they will never eliminate all the risks
  - Target, Home Depot, Equifax, and more to come…
- To better protect an organization, we need to go beyond technological solutions and investments
  - What is missing?

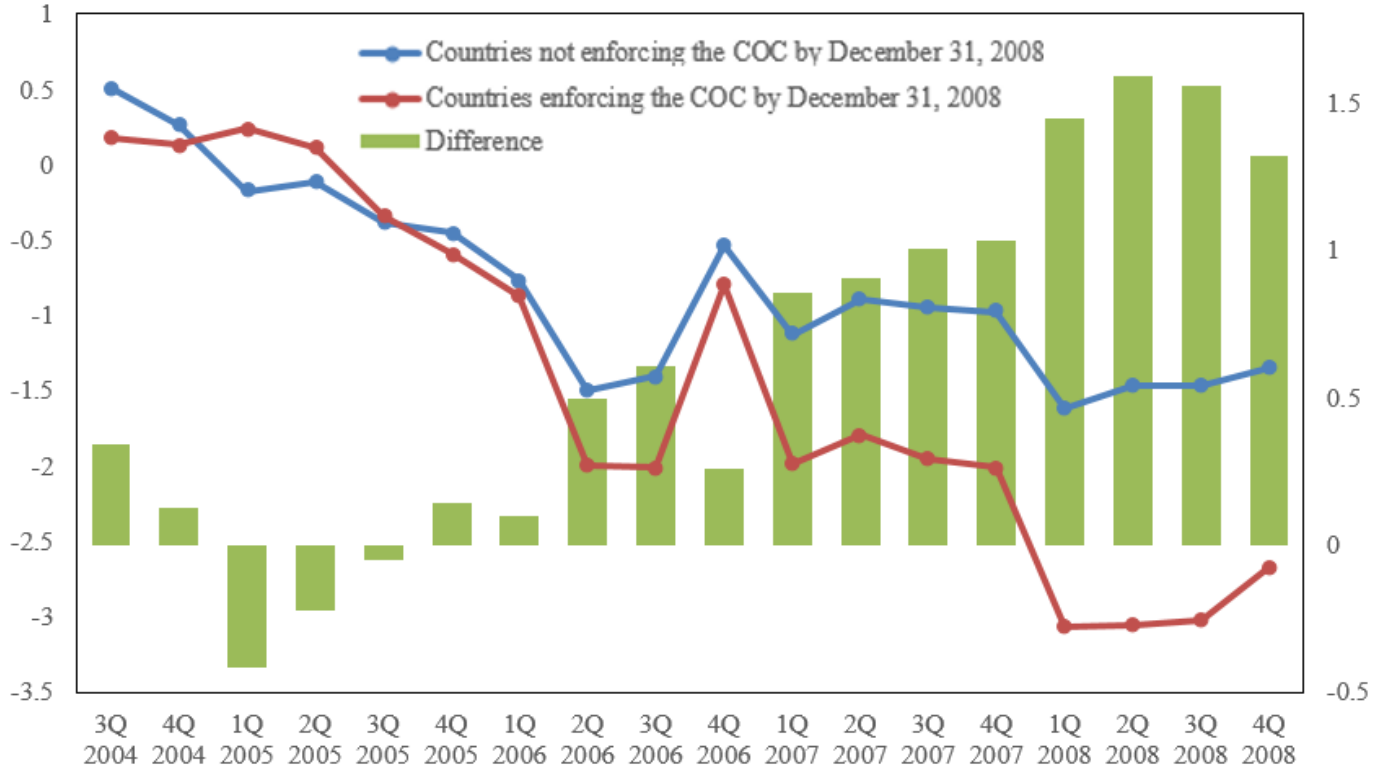
National Policy and Collaboration



National Policy and Collaboration

HKUST BUSINESS SCHOOL 香港科大商學院
WORLD CLASS IN ASIA

- Attackers are economic agents who do cost-benefit analysis



- DDoS attacks decreased in countries enforcing cybercrime laws
- The attacks are shifted to countries not enforcing the laws
- The more countries enforcing the law , the bigger the decrease

National Policy and Collaboration

HKUST BUSINESS SCHOOL 香港科大商學院
WORLD CLASS IN ASIA

VARIABLES	(1) Main estimate (preferred)	(2) Binary domestic legislation	(3) 2SLS: CPHRFF enforcement as instrument	(4) COC signature instead of enforcement	(5) Include responsible authorities and reservations	(6) Separate reservations into four sets	(7) Exclude USA
COC enforcement	-0.125***	-0.133***	-1.160**				
	(0.028)	(0.030)	(0.473)				
COC signature				-0.014			
				(0.070)			
COC enforcement without the responsible authority					-0.131***	-0.142***	-0.137***
					(0.044)	(0.045)	(0.046)
COC enforcement with the responsible authority					-0.160***	-0.185***	-0.181***
					(0.040)	(0.057)	(0.057)
Number of reservations					0.019		
					(0.021)		
Reservations – domestic enforcement						-0.023	-0.021
						(0.043)	(0.043)
Reservations – mutual assistance						0.301***	0.290***
						(0.071)	(0.072)
Reservations – DDOS irrelevant						-0.005	-0.010
						(0.062)	(0.062)
Reservations – federal clause						0.094	
						(0.146)	

Economics of Cybersecurity

HKUST BUSINESS SCHOOL 香港科大商學院
WORLD CLASS IN ASIA

$$Prob(committing\ cybercrime)$$
$$= f(expected\ net\ benefit)$$
$$= g(revenue\ from\ crime) - h(cost\ of\ crime)$$

Why did the criminals attack us?

How to increase this?

How to motivate better protection?

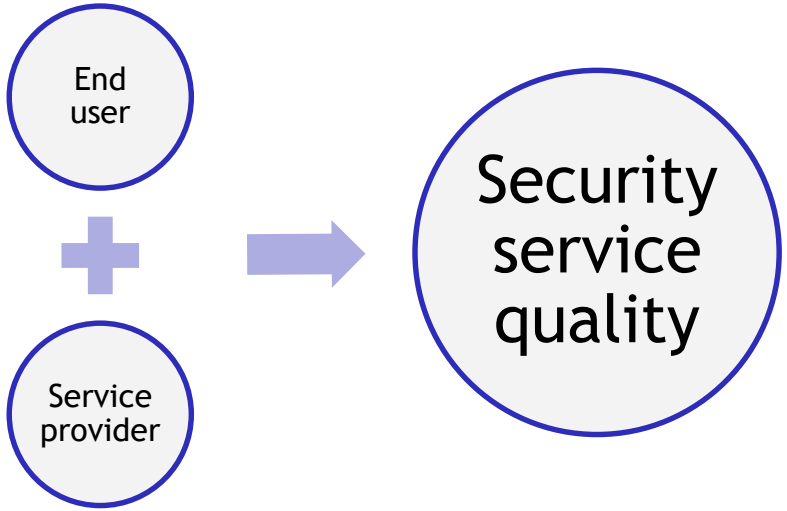
Economics of Cybersecurity

HKUST BUSINESS SCHOOL 香港科大商學院
WORLD CLASS IN ASIA

- Misaligned incentives
  - Quality of security service depends on the effort input by multiple parties – end users, IT staff, service providers
  - This gives rise to the double moral hazard problem

- Not logging off computer accounts when leaving the office
- Use easily memorable passwords such as date of birth
- Not responding to firewall alerts

- Develop sub-standard software or web services
- Not patching software
- Not actively monitor IDS and firewall



Example – The Target Incident

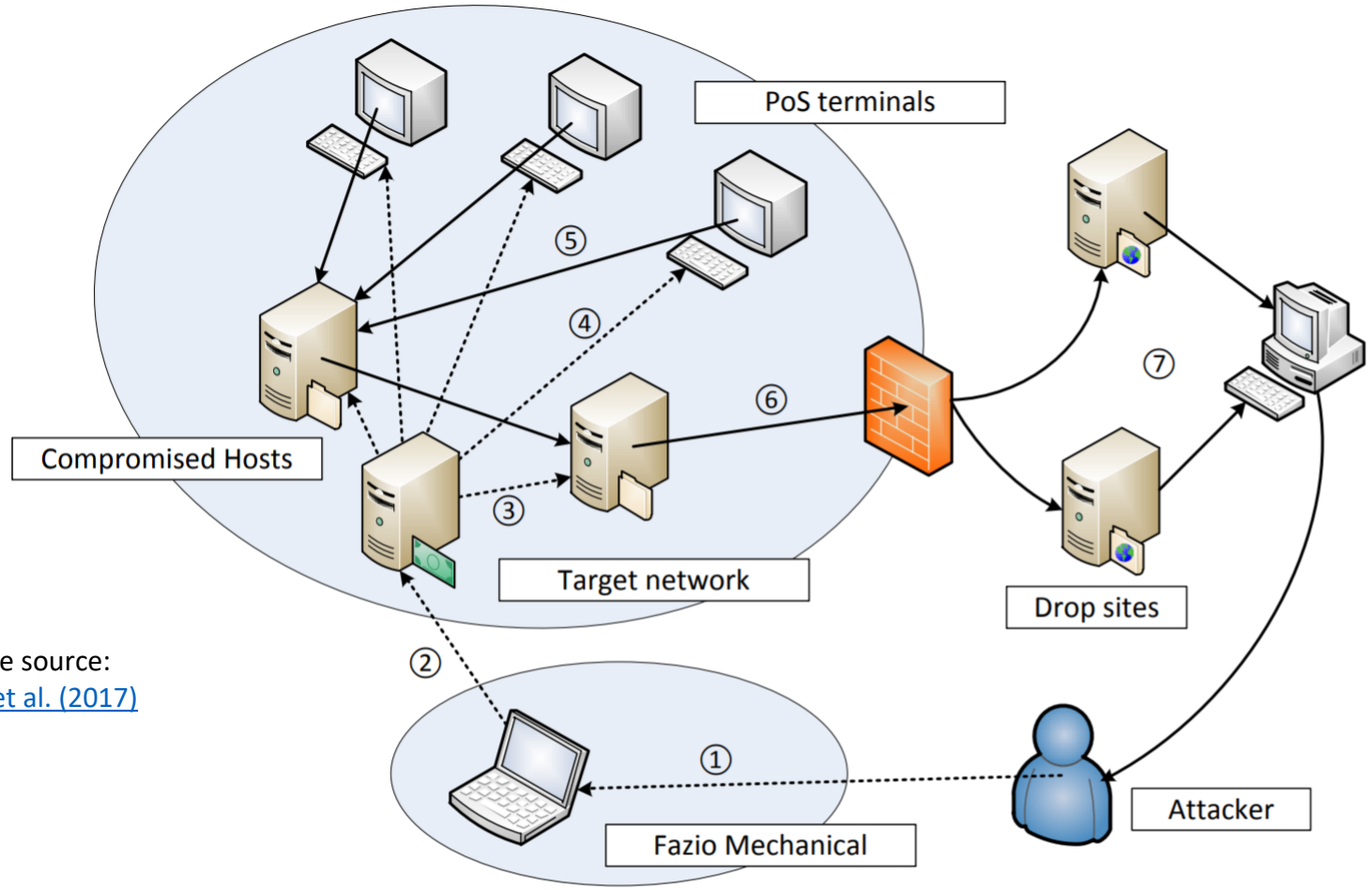


Image source:
Shu et al. (2017)

control path
data flow

1. Phishing attack against Fazio Mechanical Service

2. Accessing the Target network

3. Gaining access to vulnerable machines

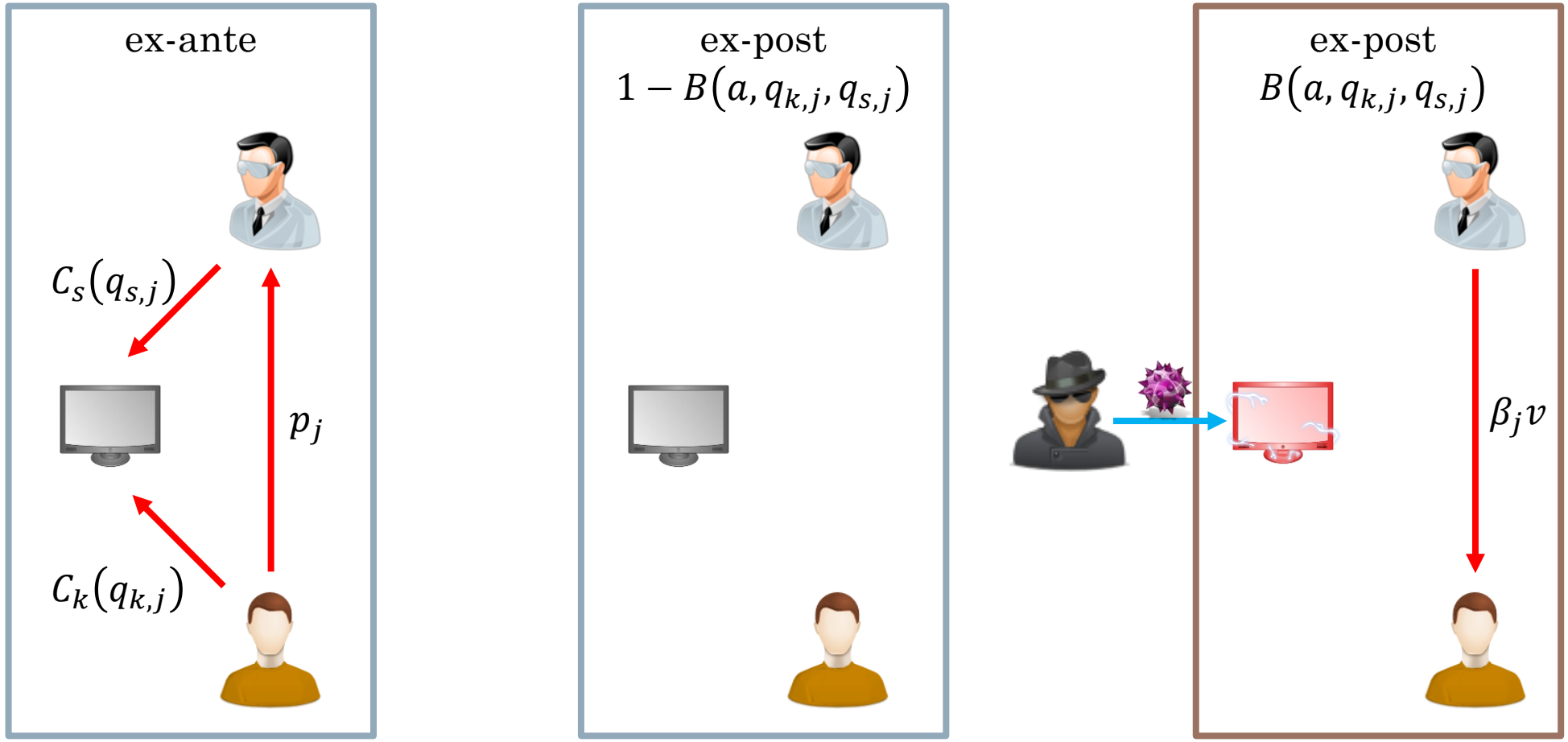
4. Installing malware on PoS terminals

5. Collecting card information from PoS

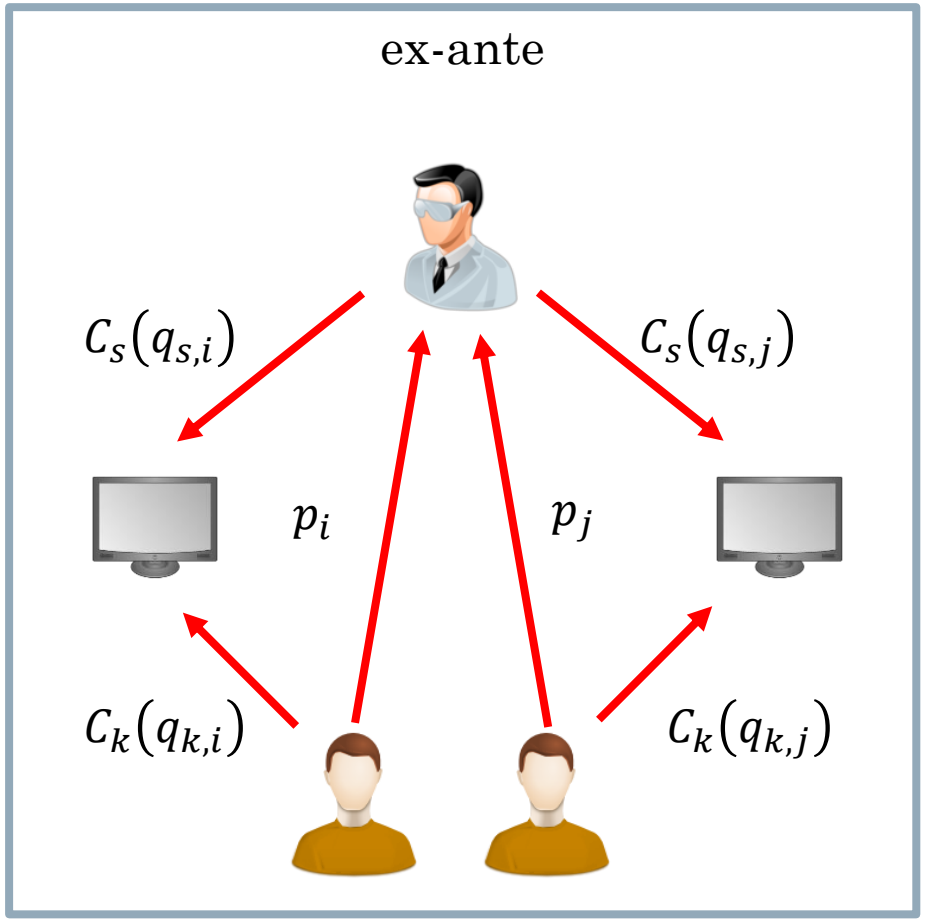
6. Moving data out of the Target network

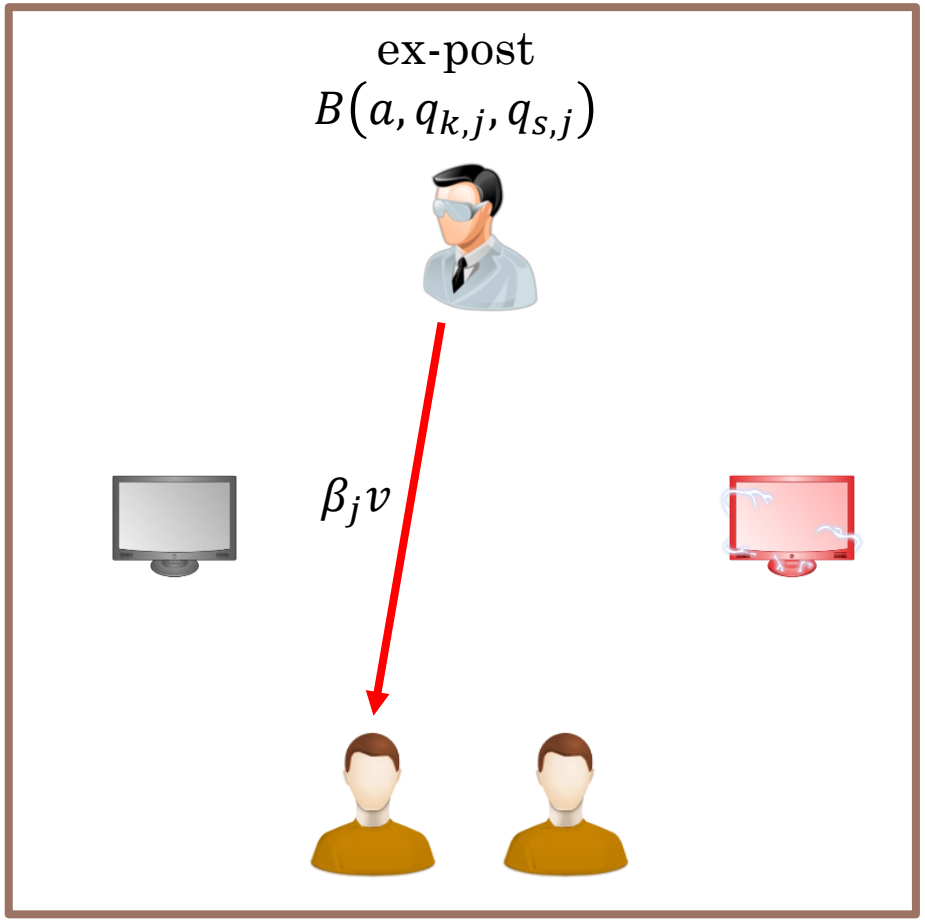
7. Aggregating stolen card and person data

Common Practice: Loss-Based Contract

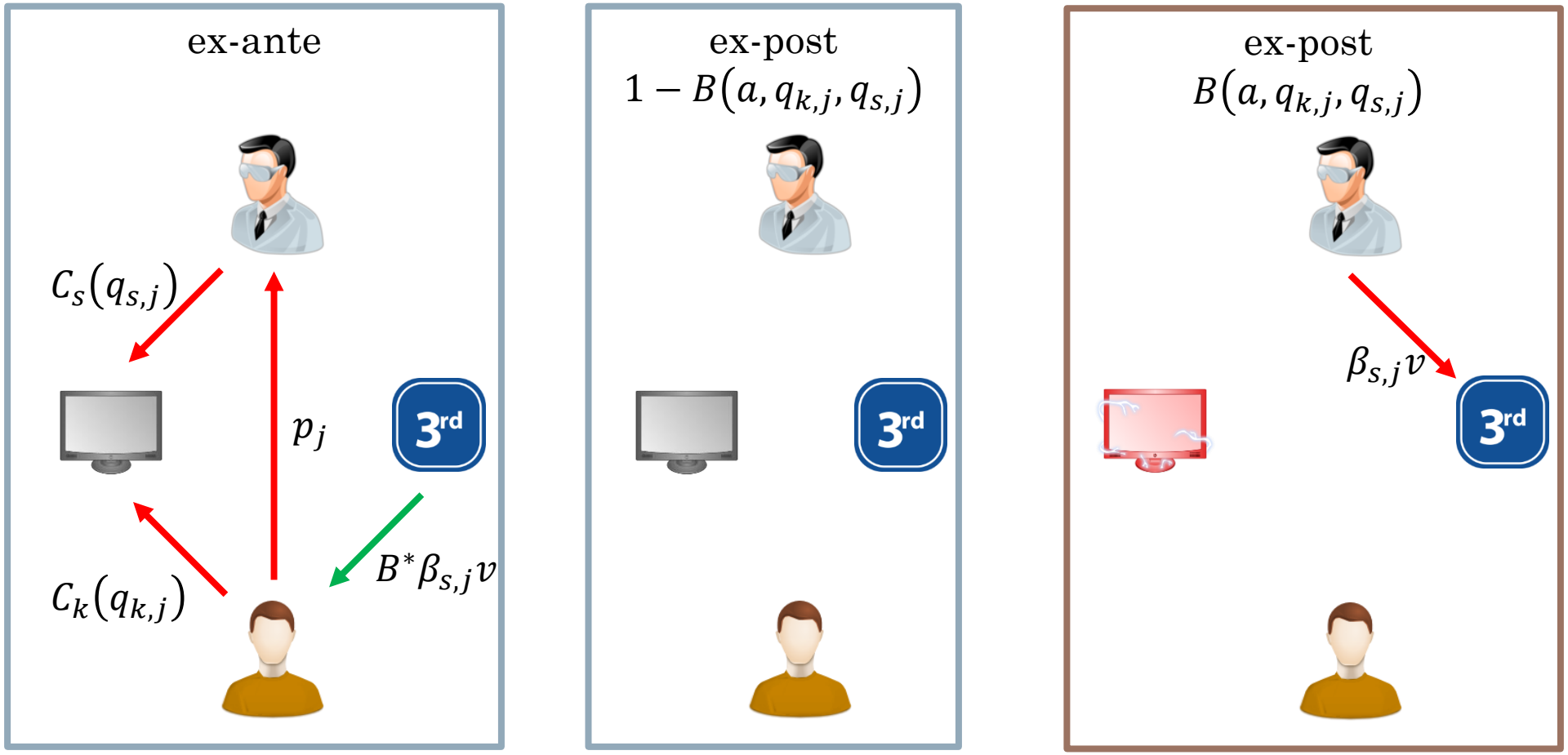


Theoretical Efficient Solution (1) – Multilateral Contract

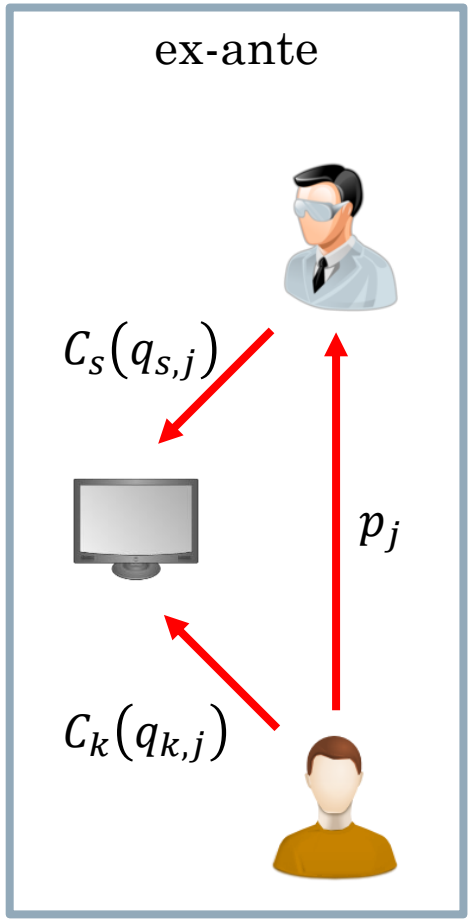


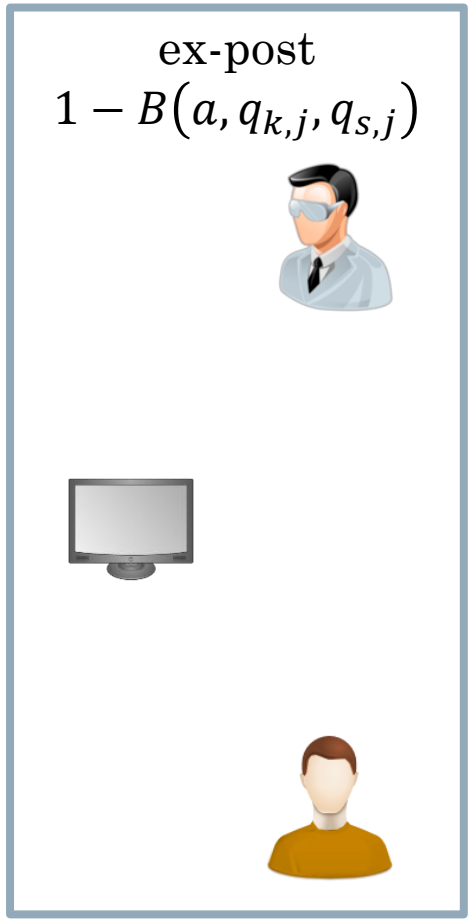


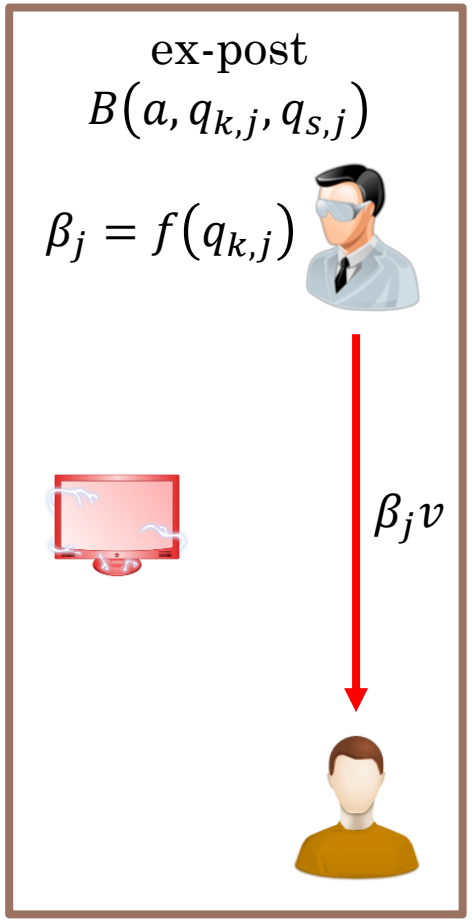
Theoretical Efficient Solution (2) – Reverse Insurance



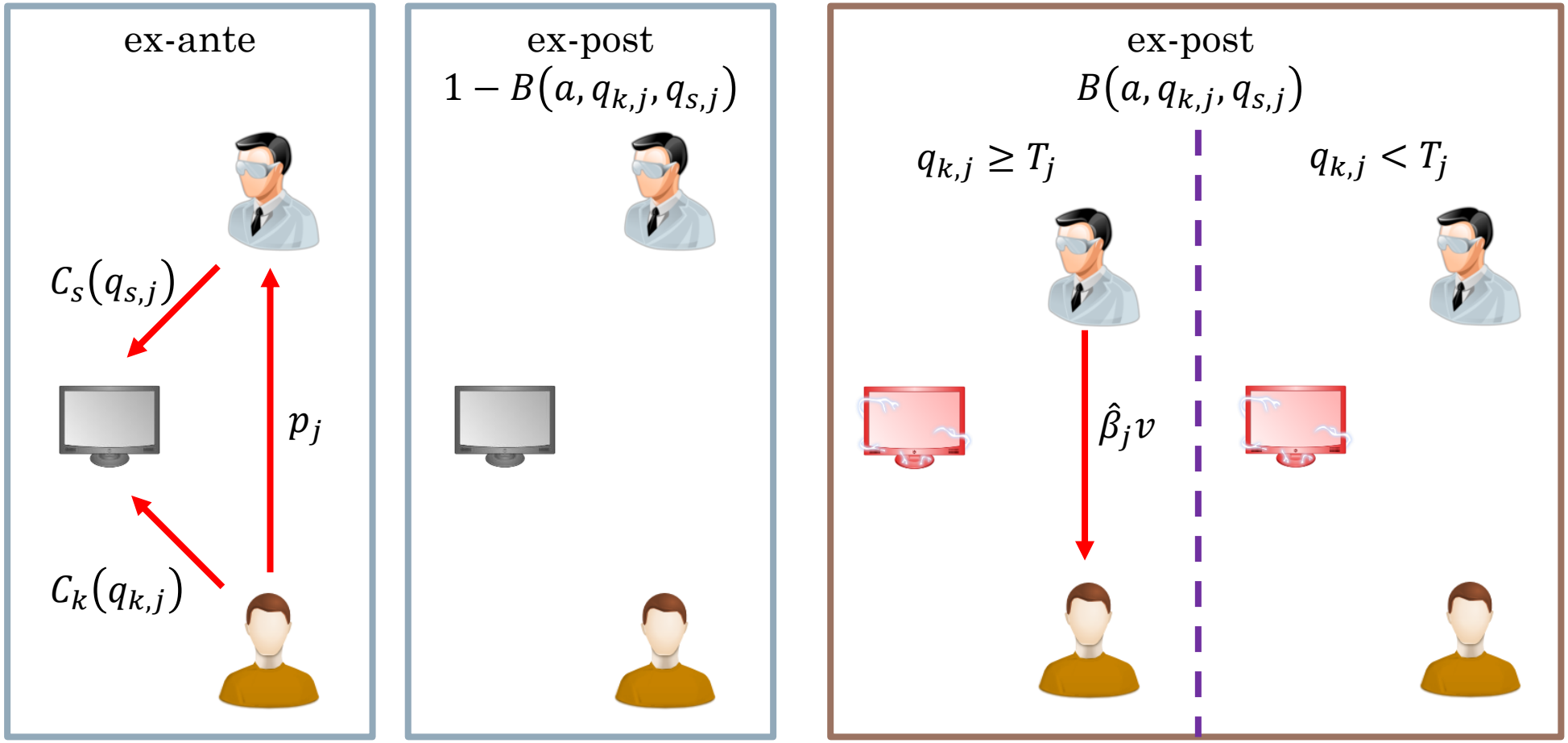
Variable-Liability Contract







Threshold-Based Liability Contract



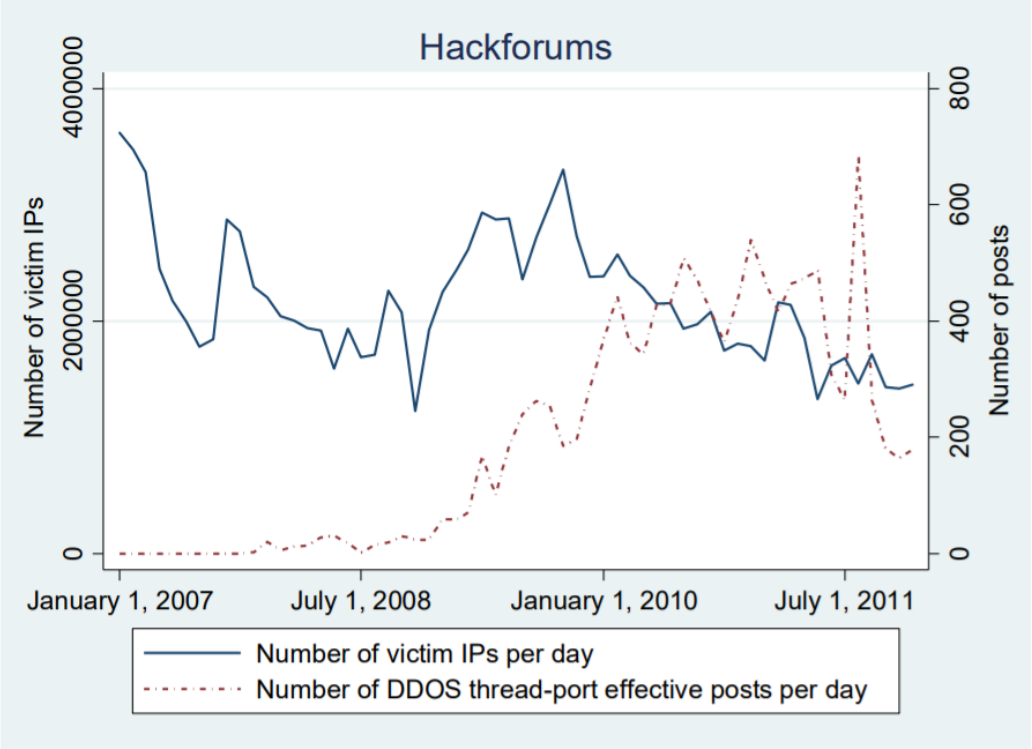
Security Service Contract Design

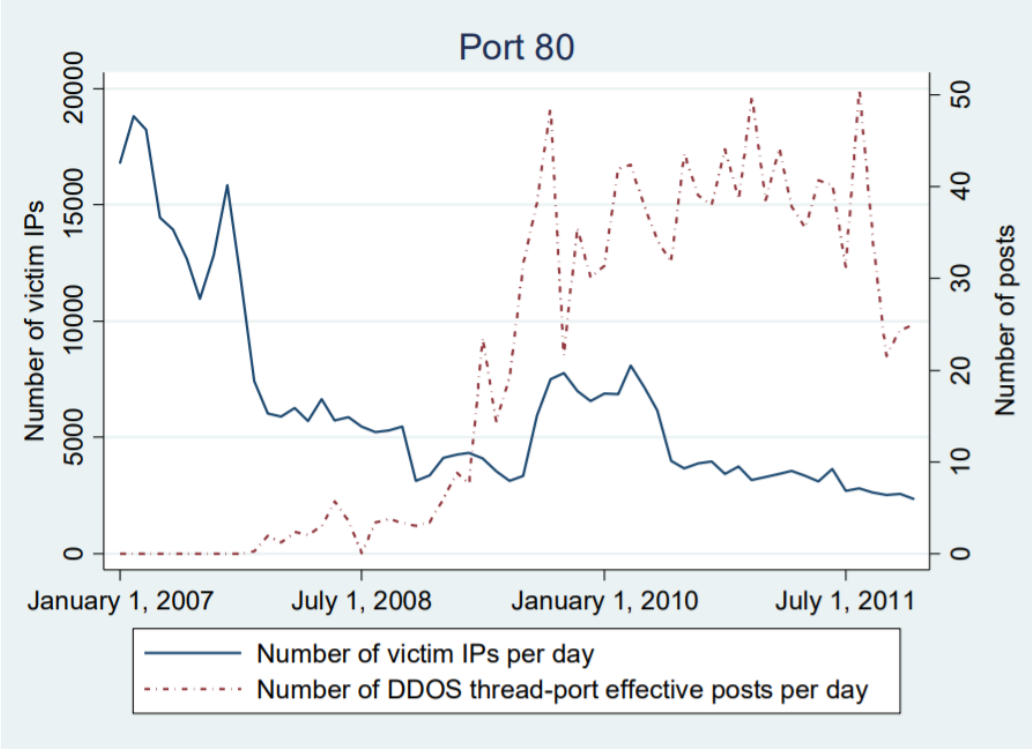
HKUST BUSINESS SCHOOL 香港科大商學院
WORLD CLASS IN ASIA

- Liability needs to be assigned properly to incentivize user protection
  - Typical loss-based liability contracts don't work very well
- With after-event auditing, we can allocate liability to end-users based on actual effort or threshold effort level
  - With limited liability, the threshold-based liability contract produces better protection quality and outcomes than third-party or reverse insurance contracts
  - It is also easier to implement than variable liability contracts and more resilient to auditing errors

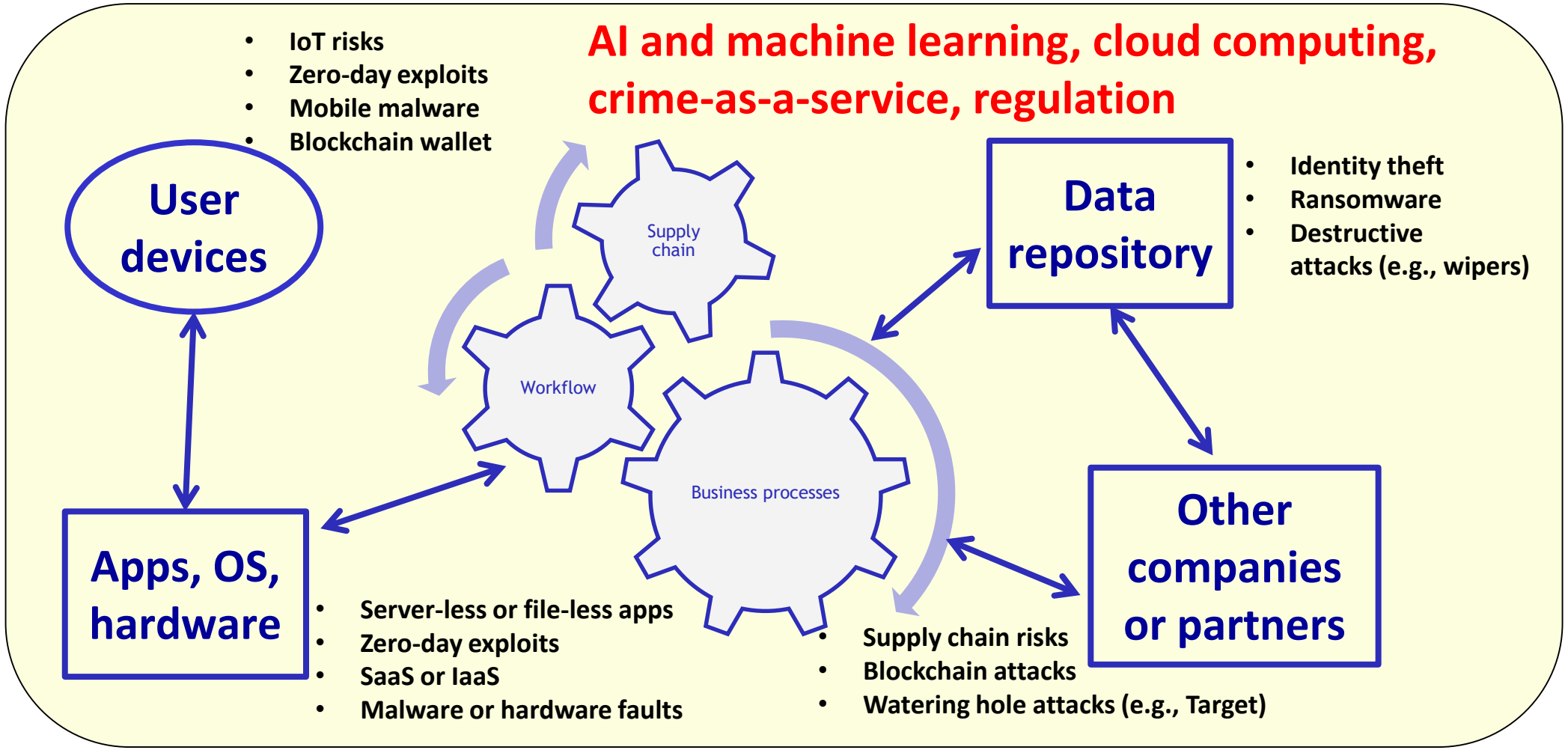
Prevention vs. Education

- Should we ban online discussion of malicious attacks?





Overall: Where is Cybersecurity?



Concluding Remarks

HKUST BUSINESS SCHOOL 香港科大商學院
WORLD CLASS IN ASIA

- We have done a lot in security investment and training
  - They are useful and effective in reducing risks
  - They help ensure a minimal level of resilience and protection
- Latest developments, such as threat intelligence, big data analytics and blockchain, add to our toolbox
- However, a good security plan should include economic and psychological factors
  - It is time for us to formally include user and attacker motivations into the strategic cybersecurity plan

Concluding Remark

HKUST BUSINESS SCHOOL 香港科大商學院
WORLD CLASS IN ASIA

- Protection strategy (what we have been doing)
- Deterrence strategy (how to signal our commitment to would be attackers and heighten their punishment)
- Liability sharing strategy (how to motivate our workers and partners in taking up their share)

The missing components in our security plan and strategy

References

- Hui, K.L., P.F. Ke, Y. Yao, and W.T. Yue "Liability-Based Contracts in Information Security Outsourcing," *Information Systems Research*, forthcoming.
- Yue, W.T., Wang, Q.H., and K.L. Hui "See No Evil, Hear No Evil? Dissecting the Impact of Online Hacker Forums," *MIS Quarterly*, forthcoming.
- Hui, K.L., S.H. Kim, and Q.H. Wang "Cybercrime Deterrence and International Legislation: Evidence from Distributed Denial of Service Attacks," *MIS Quarterly*, vol. 41, no. 2, June 2017, 497-523.

Further Discussion

HKUST BUSINESS SCHOOL 香港科大商學院
WORLD CLASS IN ASIA

- Kai-Lung Hui, PhD
  Deputy Head and Chair Professor
  Department of Information Systems, Business Statistics, and Operations Management
  School of Business and Management
  Co-Director, Dual-Degree Program in Technology and Management
  Hong Kong University of Science and Technology
- Email: klhui@ust.hk