Towards A Better Measure of Cybersecurity Awareness: An Exploratory Study of Online Scams in Pan-Asia (Work-In-Progress)

Yunhui Zhuang[1], Yun-sik Choi[2], Alvin Chung Man Leung[1], Gene Moo Lee[3], Shu He[4] and Andrew B. Whinston[5]

[1] Dept. of Information Systems, City University of Hong Kong
[2] Dept. of Computer Science, UT Austin
[3] Dept. of Information Systems and Operations Management, UT Arlington
[4] Dept. of Operations and Information Management, University of Connecticut
[5] Dept. of Information, Risk, and Operations Management , UT Austin

April 19, 2017

Acknowledgments

This work is fully supported by a research grant (*Project Number: 2015.A1.030.16A*) from the Public Policy Research Funding Scheme of the Central Policy Unit of the Hong Kong Special Administrative Region Government.

Central Policy Unit
The Government of the Hong Kong Special Administrative Region

Outline

- Motivations
- Contributions and Impacts
- Data Collection
- System Design and Implementation
- Peer Ranking Effects
- Information Security Index
- Empirical Analysis
- Future Research
- Concluding Remarks
- Q&A

Motivations

- Cyber insecurity is a serious threat
  - ➢ Hong Kong Stock Exchange was forced to suspend trading of seven companies (e.g., HSBC, Cathay Pacific) due to DDoS attacks, 2011
  - ➢ Alipay, lost over 20 Gigabyte worth of customers' data in a security breach, 2013
    (>15 million people affected).
  - ➢ Hong Kong Computer Emergency Response Team received 3,443 reports of security incidents in 2014, with a sharp increase of 103% over 2013

Motivations

- Cyber insecurity is a serious threat
    - ➢ Online scams in Singapore totaled 1,015 cases, up by almost 62% in 2014, estimated loss at SG $450,000
    - ➢ Personal data breach of Hong Kong Airlines from its Android mobile app leaks hundreds of passengers' mobile boarding pass, including names, passport numbers, DoB, and travel records, 2016
    - ➢ IRS hit by a massive data breach, exposing the information of more than 700,000 individuals, 2016

Why So Many?

- Many developing countries in the region whose country priority is economic development and they lack awareness of cybersecurity.

- Most of the countries neither have a formal information security assessment framework nor well-established cybersecurity infrastructure.

- Unable to help organizations to evaluate current information security performance and to protect themselves against sophisticated cyberattacks.

- Security underinvestment

Motivations – Cont'd

- Government's measures

  United States:

  ✓ Cybersecurity Policy Review, 2009

  ✓ Executive Order 13636 "Improving Critical Infrastructure Cybersecurity", 2013

  ✓ Cybersecurity Enhancement Act, 2014

  ✓ Cybersecurity Information Sharing Act, 2014

  ✓ Federal Cybersecurity Research and Development Strategic Plan, 2016

  European Union:

  ✓ Article 13a, Agency for Network and Information Security, 2015

Motivations – Cont'd

- Government's measures

  Pan-Asia:

  ✓ Cybersecurity Law, China, 2016

  ✓ Cybersecurity Bill, Singapore, 2017

  ✓ Cybersecurity Commission, Thailand, 2016

  ✓ Cybersecurity Basic Act, Japan, 2014

The ever increasing number of cyberattacks over the past decade motivates us to explore a more effective way to enhance the security awareness of the general public.

However, research in Pan-Asia is very limited. We are motivated to conduct an exploratory study to analyze the online scam status in the region.

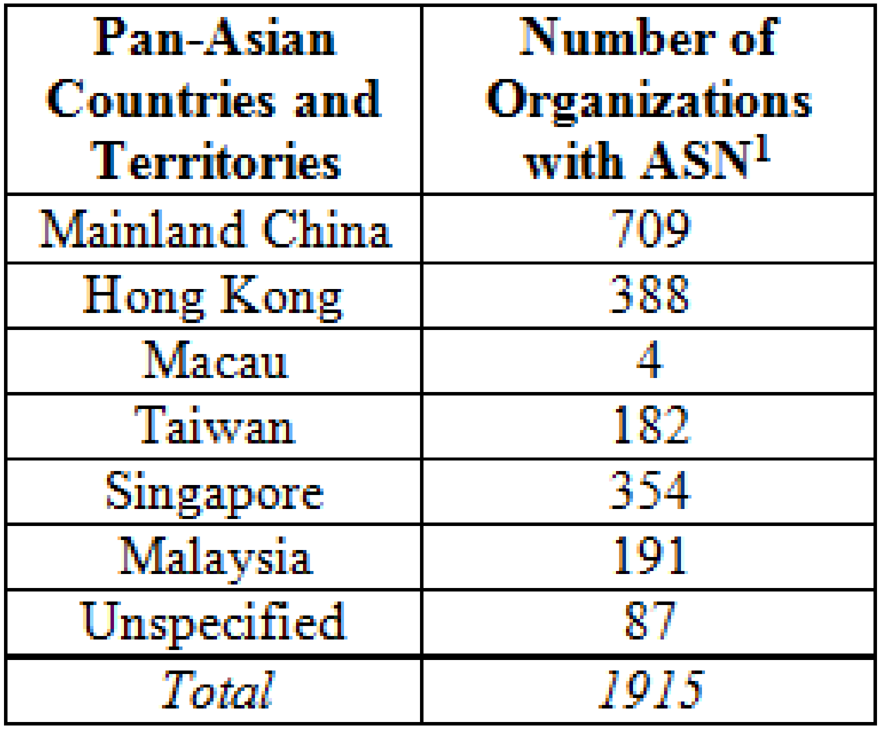
Contributions and Impacts:

- This project plans to design an independent Pan-Asian cybersecurity evaluation institution that
  - (1) monitors and evaluates the security performance of firms in Pan-Asia based on diversified daily reports of malicious cybercrimes, (spam, phishing, and DDoS attacks as originated from firms' registered network).
  - (2) that publishes firms' cybersecurity evaluation reports to the public.

Contributions and Impacts:

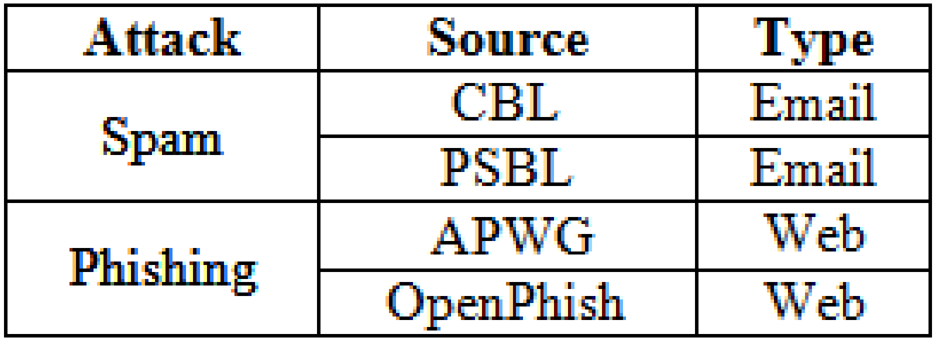
- Develop an automated system that can take in security intelligence feeds from reliable resources.
- Publish the security ranking of companies based on online scam volume.
- Provide free public access to the ranking via our website.
- An information security index is developed to reflect the strength and vulnerabilities of an organization or a country's information security condition.
- The first to propose an online scam ranking system for organizations in Pan-Asia.

Data Collection



Pan-Asian Countries and Territories	Number of Organizations with ASN[1]
Mainland China	709
Hong Kong	388
Macau	4
Taiwan	182
Singapore	354
Malaysia	191
Unspecified	87
Total	*1915*

Table 1. Organizations in Pan-Asia



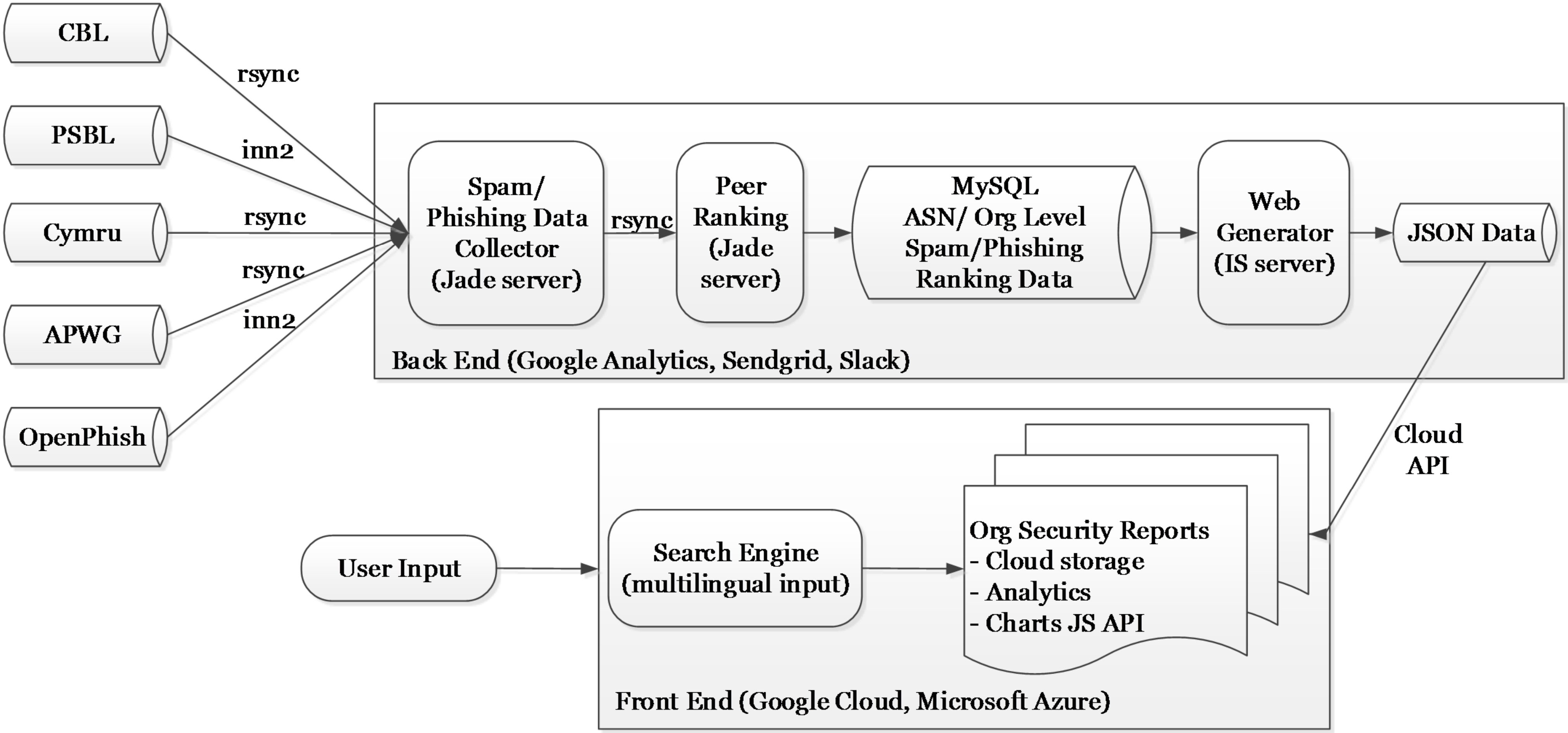
Attack	Source	Type
Spam	CBL	Email
	PSBL	Email
Phishing	APWG	Web
	OpenPhish	Web

Table 2. Data Sources

We receive daily:

- Spam feeds from *Spamhaus' Composite Blocking List (CBL)* and *Spamikaze's Passive Spam Block List (PSBL)*,
- Phishing data feeds from the *Anti-Phishing Working Group (APWG)* and *OpenPhish*.

System Design and Implementation


CBL
PSBL
Cymru
APWG
OpenPhish
rsync
inn2
rsync
rsync
inn2
Spam/ Phishing Data Collector (Jade server)
rsync
Peer Ranking (Jade server)
MySQL ASN/ Org Level Spam/Phishing Ranking Data
Web Generator (IS server)
JSON Data
Back End (Google Analytics, Sendgrid, Slack)
Cloud API
User Input
Search Engine (multilingual input)
Org Security Reports
- Cloud storage
- Analytics
- Charts JS API
Front End (Google Cloud, Microsoft Azure)

Peer Ranking Effects

- Publishes an organization’s security ranking against others – peer ranking.

- Hong Kong Standard Industrial Classification Code (HSIC), e.g.,

org	HSIC	Industry Description
China Telecom (Group)	611000	Telecommunications network operation

- Essentially helps an organization to better evaluate its security performance by “benchmark” their current security status against their peers.

- Promote peer comparison and increase security investment over time.

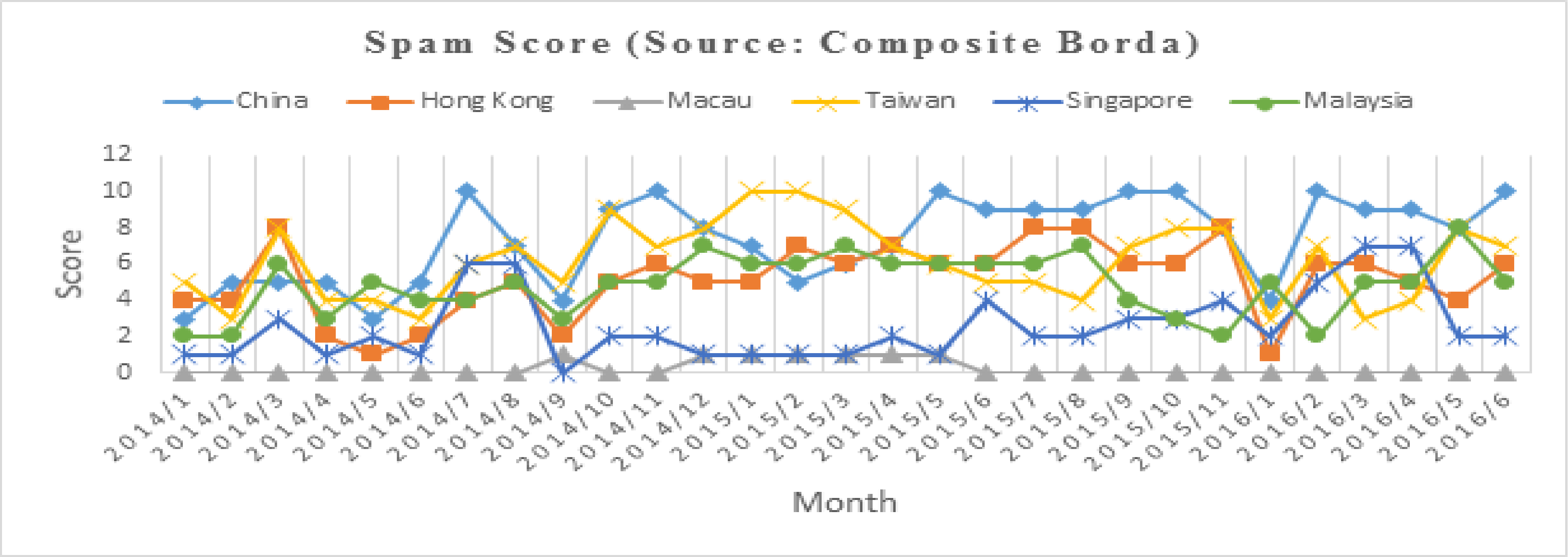
Information Security Index

- Derived from a composite **Borda count** (Adelsman and Whinston 1977) from four constituent rankings with CBL volume, PSBL volume, APWG volume, and OpenPhish volume.
- A Borda count is a voting system that combines multiple orders of preferences into a single composite metric.

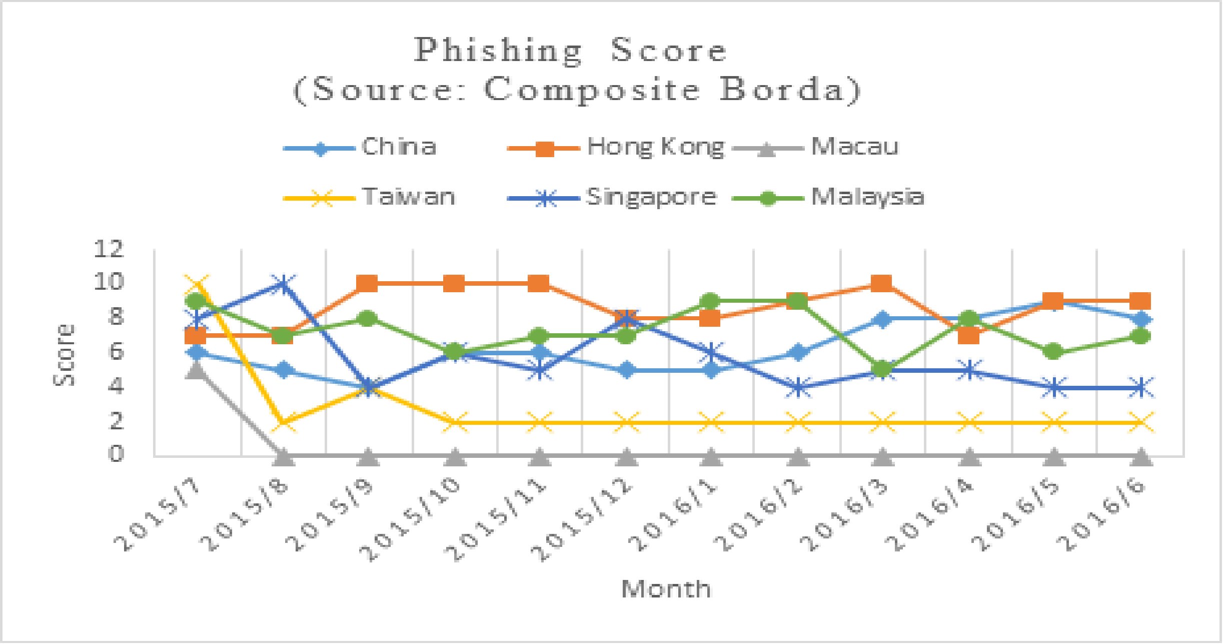
Information Security Index - Cont'd

- For example:
- If an organization is ranked *j*, it gets a point of *n-j*, where *n* is the total number of organizations in the ranking.
- The sum of these points is the Borda count for each organization. Organizations with higher Borda counts are ranked higher which indicate weaker security levels.
- To provide both macroscopic and microscopic views of the rankings, the ranking system calculates *daily* and *monthly* rankings.

Empirical Analysis



Composite Spam Score



Composite Phishing Score

Future Research

- The approaches and early-stage results of current work suggest some future directions:
  - ✓ A large-scale randomized field experiment will be conducted on 1915 Pan-Asian organizations with rigorous randomizations.
  - ✓ Through various treatment channels, such as email, website, and social media.
  - ✓ Information disclosure on social media may lead to a more prompt reaction from the treatment organizations because social media is closely followed by customers and strategic partners.

Future Research

- ✓ The treatment website is constructed on both Google and Azure cloud platforms from which we can benefit for scalability.

- ✓ The findings may be useful to public policy makers to develop new strategies to motivate firms to strengthen their information security infrastructure over time.

Concluding Remarks

- In the long run, a nationwide cybersecurity evaluation agency sponsored by governments can be proposed in relation to the main objectives of this project.
- The root causes of the cyber insecurity are organizations' insufficient security investment and the lack of relevant policies.
- Lack of publicized security information may make company owners and policy makers unaware of the seriousness of security issues.

Concluding Remarks

- Through the project, we hope to investigate whether publicized security information can motivate organizations to invest more in security.

- Provide policy makers with important information on corporate preparedness against cybercrimes so as to help them evaluate existing strategies and develop new ways to promote cybersecurity and strengthen corporate information security infrastructure.

Thank you!

Q&A