JOURNAL OF MANAGEMENT INFORMATION SYSTEMS
2020, VOL. 37, NO. 3, 668–693
https://doi.org/10.1080/07421222.2020.1790185

Understanding Security Vulnerability Awareness, Firm Incentives, and ICT Development in Pan-Asia

Yunhui Zhuang [a], Yunsik Choi[b], Shu He [c], Alvin Chung Man Leung [a], Gene Moo Lee [d], and Andrew Whinston [e]

[a]Department of Information Systems, College of Business, City University of Hong Kong, Kowloon, Hong Kong; [b]AITRICS, Seoul, Republic of Korea; [c]School of Business, University of Connecticut, Connecticut, USA; [d]Sauder School of Business, University of British Columbia, Vancouver, British Columbia, Canada; [e]McCombs School of Business, University of Texas at Austin, Austin, Texas, USA

ABSTRACT

This paper investigates how the awareness of a security vulnerability index affects firms' security protection strategy and how the information awareness effect interacts with firm incentives and country-wide information technology (IT) development level. The security index is constructed based on outgoing spams and phishing website hosting, which may serve as an indicator of a firm's security controls. To study whether security vulnerability awareness causes firms to improve their security, we conducted a randomized field experiment on 1,262 firms in six Pan-Asian countries and regions. Among 631 randomly selected treated firms, we alerted them of their security vulnerability index and their relative rankings compared to their peers via advisory emails and websites. Difference-in-differences analyses show that compared with the controls, the treated firms improve their security over time, with a statistically significant reduction of outgoing spam volume according to one of the data sources but not phishing website hosting. However, a statistically significant reduction in phishing website hosting was observed among non-web hosting firms, suggesting that firms' underlying incentives play an important role in the treatment effect. Lastly, exploiting the multi-country nature of the data, we found that firms in countries with high information and communications technology (ICT) development are more responsive to our intervention because they have higher IT capabilities and more resources to resolve security issues. Our study provides cybersecurity policymakers with useful insights on how firm incentives and ICT environments play roles in firms' security measure adoption.

KEYWORDS

cybersecurity; information security index; randomized field experiment; security awareness; firm incentives; ICT development; Pan-Asia

Introduction

Cyberattacks impose serious threats to individuals, firms, and our society at large. Even with technological advances in security software and hardware, we are still experiencing an ever-increasing number of cyberattacks and associated costs [46, 51, 59]. Studies on the economics of cybersecurity argue that economic factors are as important as technical aspects in information security solutions and that information asymmetry, misaligned incentives, and negative externalities can be the root causes of security underinvestment [5, 9, 37]. Additionally, country-wide information and communications technology (ICT)

CONTACT Gene Moo Lee gene.lee@sauder.ubc.ca Sauder School of Business, University of British Columbia, 2053 Main Mall, Vancouver, British Columbia, CanadaV6T 1Z2.

Supplemental data for this article can be accessed on the publisher's website.

development may restrain the technical resources available to firms and limit their capabilities to curb security threats [12, 26, 29, 42].

Information asymmetry can exist among firms and between firms and the general public, hindering security vulnerability awareness. As firms' information technology (IT) capabilities vary, some firms may not be fully aware of the underlying risks of their IT systems [14, 18, 29]. Even when firms are aware of cybersecurity issues, they may be reluctant to disclose such knowledge to the public due to the potential loss of financials and customers [21, 43], which creates an information asymmetry between firms and the public [3, 15, 23].

Economic incentives must be aligned for firms to invest in security. Because of the intertwined nature of IT systems, a firm's benefit from security investment can only be realized when a minimum number of firms adopt security technologies.[1] In addition, due to the quality uncertainty of security technologies[2] and misaligned incentives of for-profit firms,[3] firms may deprioritize security issues when related security problems are less likely to *directly* harm themselves, even though the issues create *negative externalities* to other firms and the general public [9, 19, 48]. These factors can drive IT managers to underinvest in information security protection, which may lead to ubiquitous security breaches [7, 22].

Apart from security information asymmetry and economic incentives issues, firms should have sufficient IT capabilities and resources to properly implement security measures [11, 29]. Prior studies showed that the ICT development environment affects the adoption of security-related IT capabilities [14] and that country-level cybersecurity policies can change the attack landscape faced by firms [26, 28, 42].

In this study, we seek to investigate potential ways to increase firms' cyber risk awareness and incentivize firms to develop more secure cyber environments. This study echoes the origin[4] responsibility principle of the research framework of the Bright ICT initiative [33, 34] by proposing a new security vulnerability index to incentivize firms to prevent the widespread use of cyberattacks (e.g., spam and phishing) [57]. Similar to the idea of Moody's and Standard and Poor's credit ratings, our proposed security vulnerability index reflects a firm's vulnerabilities to cybercrime and its adequacy to prevent the spread of unsolicited online content. The index is constructed by processing large-scale cyber incident data feeds on spam emission[5] (Composite Blocking List (CBL) and Passive Spam Block List (PSBL)) and phishing website hosting[6] (Anti-Phishing Working Group (APWG) and OpenPhish). We chose spam and phishing as our data sources because (i) they are the most commonly seen cyber threats and (ii) they can be externally observed without internal system investigations. A firm's computers with inadequate preventive security measures may be easily compromised by adversaries via bots to send spams or host phishing websites [39]. Thus, outgoing spam and phishing websites hosting activities can be indicators of a firm's security vulnerabilities.

We seek to investigate whether informing and publicizing individual firms of their security vulnerability indexes can motivate them to adopt better security measures over time. To examine the information awareness effect of our proposed security index, we conducted a large-scale randomized field experiment (RFE) on 1,262 firms in six Pan-Asian countries and regions. Among 631 randomly selected treated firms, we alerted them about their security vulnerability indexes and their relative rankings compared to their peers via advisory emails and website.

Our research draws on two closely related studies [24, 53] that examine security information awareness effects on spam reduction, where the former is based on a U.S. RFE, and the latter has adopted a quasi-experiment setting. Addressing major limitations of the previous studies, this paper extends the literature in terms of research context, experimental design, and empirical findings. To our best knowledge, this research is among the first to conduct a cybersecurity RFE in multiple countries to study firms' behavior on spam and phishing. The benefit to include firms in different jurisdictions, comparing to a single country setting in He et al. [24], is that such diversification allows us to obtain more robust conclusions and to investigate how country-wide ICT development environment interacts with firms' reaction to the intervention [16, 17]. Furthermore, as phishing is more technically sophisticated than spam to detect and tackle [12], our study can facilitate us to understand why and how firms react differently to the two types of cybersecurity attacks. (Supplemental Online Appendix 1 describes diverse spam and phishing related laws in Pan-Asian countries and the region.)

This study also makes significant improvements in the experimental design and empirical findings. Our security index is based on two distinct types of cyberattacks, outbound spam and phishing website hosting, with which firms have different incentive structures. This allows us to empirically study the impact of firm incentives in the experiment. Different from our study, He et al. [24] and Tang and Whinston [53] only considered one cyberattack type, spam. In addition, our study has more treatments over a longer period (six months in ours vs. two months in He et al. [24]; Tang and Whinston [53] did not have any email treatments), which allows us to estimate short- and long-term treatment effects. Finally, our study adopts sophisticated tracking tools to track whether focal firms have received and opened the advisory emails as well as visited our advisory websites. These tracking measures address potential compliance issues in the two prior studies.

Our empirical results show that the treatments (i.e., receiving and opening advisory emails) induce a significant reduction on outbound spam volume according to the CBL data, but not on phishing website hosting. Our dynamic analysis further shows that there is a significant decline in CBL spam volume after the first two batches of treatment emails, but not after the third batch. Additionally, an extended analysis shows that non-web hosting firms have a significantly reduction in phishing website hosting after receiving our treatments, which was not observed among hosting firms. Furthermore, when we compared firms from countries with low ICT development level with those from highly developed countries, we found that the latter ones are more responsive to our treatment in terms of reduction in both spam volume and phishing websites. These empirical findings suggest that the lack of incentives and IT capabilities may be two potential reasons for the non-significant average treatment effects on phishing website hosting. Finally, we analyzed overall security performance by composite Borda counts, which aggregate spam and phishing volumes from four different sources. The results show that the treatments can lower the treated firm's country-level security vulnerability ranking, which suggests improved performance compared with the peers in the same country.

This study contributes to the cybersecurity economics literature in multiple ways. First, we developed a robust security vulnerability index based on multiple cyberattack types: outgoing spam and phishing website hosting. Second, we showed the effectiveness of disclosing the index with a multi-national RFE. Third, we found empirical evidence that a firm's underlying incentives and IT environment play important roles in its security investment strategies. These findings provide useful insights to cybersecurity policymakers. In addition to using penalties to enforce firm compliance, one may publicize security information to incentivize firms to adopt better preventive measures. The findings also suggest that cybersecurity policies should be aligned with national ICT development strategies. Our study also responds to the call of the Bright ICT Initiative by developing a security index to promote origin responsibilities [33, 34].

Theoretical background

Security researchers and practitioners are exerting enormous efforts into finding efficient and effective solutions to contain widespread cybersecurity threats [32, 47, 55]. Studies in the economics of cybersecurity literature suggest that economic factors are as important as technical aspects in information security solutions [5, 9, 37]. We argue that firms go through three steps in the implementation of security protection measures. First, firms should have an *awareness* of security threats and an objective assessment of the associated risk. Second, they should have proper *economic incentives* to address security issues with the consideration of associated costs and benefits. Lastly, firms should have sufficient IT *capabilities* to implement proper security measures. In this section, we present the theoretical foundations of the interdisciplinary cybersecurity economics field that investigates how information asymmetry, economic incentives, and IT capabilities play roles in firms' cybersecurity strategies.

Security vulnerability awareness

The first step in adopting proper security protection measures is the awareness of cyber threats and the associated risk levels. Prior studies identify two possible causes of information asymmetry that can hinder security vulnerability awareness. First, some firms may not have sufficient IT capabilities to measure the underlying risk of their IT systems [14, 18, 29]. This can create information asymmetry across firms with different levels of IT resources. Second, even for firms with a good understanding of IT risk, they may be reluctant to disclose such knowledge to the public due to the potential loss of financials and customers [21, 43]. In addition, full disclosure may accelerate the diffusion of attacks and increase the risk of penetration probability [36]. This creates an information asymmetry between firms and the general public [3, 15, 23].

Prior studies showed that information disclosure is an effective approach to alleviate such information asymmetry issues [24, 38]. From an information sharing perspective, one can inform firms of their security vulnerabilities in the form of security advisory reports [24, 43]. This can allow firms to better understand their security weaknesses [24] and to prepare against future cybercrimes [38]. In addition, public disclosure of firms' security vulnerabilities can create publicity effect for the firms, which motivates them to take proactive security actions to salvage their public reputation [43]. Moreover, public disclosure can create a social comparison that may further incentivize firms to adopt better cyberattack countermeasures [21, 24, 53]. In Tang and Whinston [53], the authors used ASN level spam data to show that publicizing top spammers' security data would significantly reduce the outbound spam volume of ASNs in the same country compared with that of the synthetic control ASNs.

In our experiment, we sent security advisory emails to the treated firms to inform them of the security risk and publicize such information on a public advisory website to create publicity effect. Compared with the previous study using the country-level analysis [53], our firm-level treatment enabled detailed estimation, and the experimental design with tracking capabilities can effectively address the potential compliance issue. We expect that the empirical analysis of the experimental data can help us identify the causal effect of security vulnerability information awareness through the way of information asymmetry reduction.

Misaligned incentives and negative externalities

Even with the awareness of the underlying security issues, firms will respond to them only if they have the proper economic incentives to address such issues. Studies in the cybersecurity economics literature showed that economic incentives play important roles in the adoption of information security solutions [5, 9, 37]. In addition, different models and factors have been investigated to understand how to effectively motivate users to protect information systems [35].

The cybersecurity issue is intrinsically difficult to tackle because of the intertwined nature of the underlying networks. Kunreuther and Heal [31] demonstrated that the security of a group of people often leans on each of its members. As a user in the system takes less precaution to protect her computer, the more likely the others in the same group will be infected or intruded upon. Therefore, in the absence of an appropriate incentive mechanism, individuals may not exhibit proper security behavior. In our research context, firms may deprioritize IT security problems when the expected harm caused by their insecure system is smaller than the cost to implement proper security measures, even though the insecurity can create negative impacts on external entities [9]. This phenomenon refers to *negative externalities*, in which one's action negatively affects other related parties in a networked environment [9, 26, 28, 42].

IT managers are willing to invest in protective security measures that can safeguard their internal corporate assets from cyberattacks because these attacks can directly harm their systems. For example, given that most spam emails are sent from compromised computers, firms are willing to fix the issues of spam and compromised computers when they become aware of them [24]. In contrast, their incentives to invest in security can deteriorate when the underlying technologies are to protect the assets of external entities [9]. For instance, in the case of a phishing website, web hosting providers may have few incentives to take down malicious websites when "legitimate" customers are operating the sites. This can be the case even when the phishing websites negatively affect external entities (e.g., phishing website visitors). Furthermore, in some jurisdictions, web hosting providers may not have the authority to take down such malicious websites. Unless the security investment is aligned with firm incentives, it is difficult to motivate firms to act to curb such cybersecurity problems. In our field experiment, we examine the moderating effect of firm incentives on our information awareness treatment.

IT capabilities and country-wide ICT development

Once firms are aware of the security issues and have economic incentives to address them, the last important requirement is whether the firms have proper IT capabilities and resources to implement security defense measures. Prior studies showed that IT capabilities depend on the country-wide environment, for example, IT infrastructure, technology readiness, and availability of human resources [11, 29,60-62]. The technology-organization -environment (TOE) framework also highlights the importance of the external environment (e.g., access to resources) in technology adoption [8, 30]. A stream of security research has shown evidence that external environmental factors such as ICT development and regulatory environments are essential in security-related IT capabilities [13, 14, 42]. Bose and Leung [14] showed that the ICT development level has a moderating effect on the positive impact of security defense measure adoption on the firm values. From the cyber attacker's perspective, it was shown that country-level law enforcement can significantly change the attacker's strategies, selecting target computers in countries with weaker security enforcement [26, 28, 42].

All in all, holding security vulnerability awareness and economic incentives constant, we expect that the firms with strong IT capabilities in high ICT development environments are more likely to respond to our information awareness treatment. Though we cannot directly measure an individual firm's security-related capabilities, we can measure the ICT development in the environment exposed by the firms and infer their IT capabilities and resources to handle security-related issues. Following Bose and Leung [14], we use the network readiness index (NRI) that measures country-wide ICT development level with the consideration of environmental factors (i.e., political, regulatory), IT readiness (i.e., infrastructure, affordability, and skills), and IT usage (i.e., individual, business, government) and investigate how firms in countries with different NRI levels respond to the treatment.

Experimental Design and System Implementation

Security vulnerability index development

A firm's information security condition is a latent variable that cannot be directly measured. However, one way to estimate it is by the use of perceptible data. Security attacks originating from a corporate network may be a good indicator of its weak security infrastructure. According to Symantec's MessageLabs, over 50% of spams are sent by botnets [50]. These infected computers and servers may be used by adversaries as vehicles for even more serious cyberattacks such as distributed denial of service (DDoS) attacks, identity thefts, hacking, data breaches, and cyber vandalism. In this research, we use (i) outbound spam volume generated from a corporate network and (ii) the number of phishing websites hosted in the network to construct a comprehensive security vulnerability index.[7] For the outbound spam volume, we collected two independent and representative spam feeds: Spamhaus's CBL[8] and Spamikaze's PSBL.[9] For the phishing websites, we adopted two of the largest phishing data feeds: APWG[10] and OpenPhish.[11] We note that these data feeds are widely used in the security literature [45, 52, 54, 58]. Firms may have different incentive structures with respect to the two cyberattack types. Thus, the use of two different cyberattack types enabled us to study the role of incentives on the effects of security index awareness.

We used the Borda count to construct a composite ranking based on four constituent rankings of each data source (e.g., CBL, PSBL, APWG, and OpenPhish). The Borda count is a voting system that combines multiple orders of preference into a single composite metric [2]. First, we extracted the ranking from each of the four data sources in each industry sector defined by Hong Kong Standard Industry Classification (HSIC) code, with worse performance being ranked higher in terms of spam or phishing volume. Next, we constructed the composite Borda ranking by taking firm *j*'s rank *k* for a given ranking *d* and grant firm *j* a score $(n_d + 1 - k_d)$ for that ranking, where *n* is the total number of firms in ranking *d*. Finally, we summed these points from the individual rankings to produce the composite Borda count (e.g., *score(j)*) for each firm, as shown in Equation (1).

$$score(j) = \sum_d (n_d + 1 - k_{jd}) \tag{1}$$

Firms with higher Borda counts get higher composite Borda ranks, which indicate worse performance. Firms with the best security level (e.g., no spam and phishing volume) are ranked equally the lowest. (Supplemental Online Appendix 2 provides an example of how the composite Borda count was constructed based on the four security data sources.)

Information system implementation

We developed an information system that collected data on a daily basis from four sources: (i) CBL and PSBL for spam data and (ii) APWG and OpenPhish for phishing data. The spam data feeds provide daily reports on the total spam volume associated with a complete list of IP addresses which were sending out spam emails. The data cover more than eight million IP addresses, over 190,000 netblocks, and approximately 21,000 ASNs for 200 countries around the world. PBSL has a relatively smaller daily volume compared to that of CBL, but it provides full email information, including raw email header, body, and attachments.

APWG provides phishing intelligence feeds via a phishing data repository by the eCrime Exchange Service. The data repository of OpenPhish includes phishing URLs, targeted brands, IP addresses, country codes, ASN information, top-level domains, and the time of discovery. Besides, firm-level data must be constructed in order to evaluate a firm's security conditions using raw IP-level data. Thus, there are three levels of mapping: from IP to netblock, from netblock to ASN, and, finally, from ASN to firm.[12] With this mapping, it is possible to trace the host organizations of a spam email and a phishing website. Figure 1 illustrates the architecture of the entire experimental system. Two authors' research centers concurrently hosted the system during the experiment.

Large-scale randomized field experiment

To causally test whether security information awareness improves their security over time, we employed an RFE along with econometric analyses as the main evaluation methodology. An RFE, also referred to as a randomized controlled trial, is a well-established

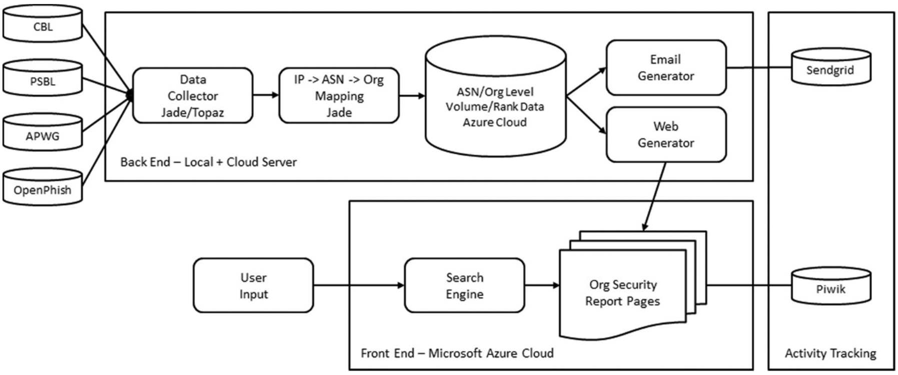
CBL
PSBL
APWG
OpenPhish
Data Collector Jade/Topaz
IP -> ASN -> Org Mapping Jade
ASN/Org Level Volume/Rank Data Azure Cloud
Email Generator
Web Generator
Sendgrid
Back End – Local + Cloud Server
User Input
Search Engine
Org Security Report Pages
Piwik
Front End – Microsoft Azure Cloud
Activity Tracking

Figure 1. Experiment system architecture.

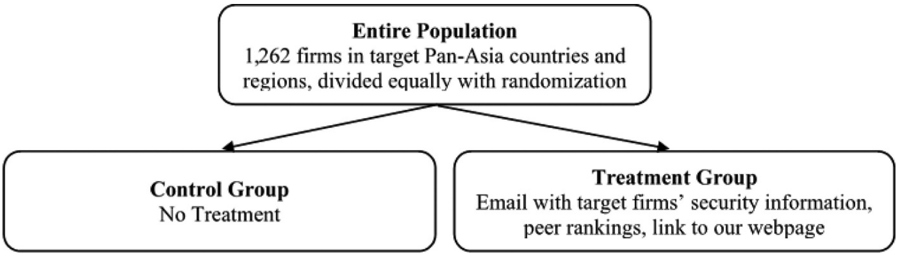
Entire Population
1,262 firms in target Pan-Asia countries and regions, divided equally with randomization
Control Group
No Treatment
Treatment Group
Email with target firms' security information, peer rankings, link to our webpage

Figure 2. Design of the randomized field experiment.

methodology in social science for policy intervention evaluation [25]. The main advantage of this methodology is its capability of identifying a causal effect in a naturally occurring environment.

The firms in this experiment were split into two equally sized, statistically homogeneous groups by stratified and matched-pair randomization [40]. The grouping is summarized in Figure 2. The control group received no treatment. For the treatment group, advisory emails with security evaluation reports were sent to relevant contacts in IT departments within each firm at the beginning of July, September, and November 2017. Each treatment email included (i) the firm's spam and phishing data, such as a total number of spam emails and phishing website counts, (ii) peer rankings in the industry sector or region, and (iii) a hyperlink to a designated advisory webpage for the treated firm. The webpage supported a search function to explore security vulnerability reports on other firms in the treatment group. (Supplemental Online Appendix 3 describes the website's core functions and a sample firm's security vulnerability index. Supplemental Online Appendix 4 shows a sample treatment email.)

Firm data

From the WHOIS database,[13] we collected a full list of 1,930 registered ASNs' information from six Pan-Asian countries and regions: Hong Kong, Macao, Mainland China, Malaysia, Singapore, and Taiwan. After mapping the ASNs to registered firm names, we created a list of 1,293 firms that operate at least one ASN. Lastly, we manually collected and validated corporate email addresses from those firms and finalized a list of 1,262 firms. (We provide the number of sample firms in each industry sector based on the Hong Kong Standard Industrial Classification (HSIC) in Supplemental Online Appendix 5.)

We note that our field experiment was conducted with all the firms that meet two conditions: (i) owning at least one ASN in six Pan-Asian countries and regions and (ii) having a valid email address. We sent out a set of invitation emails to all firms in the treatment group to introduce our project before actual treatment emails were sent. (Supplemental Online Appendix 6 presents an example of our invitation emails.) We used Sendgrid[14] to track all outgoing treatment emails in each of three batches. Overall, 565 out of 631 treated firms successfully received at least one treatment email. As a result, we used the data from these 565 compliant firms and their corresponding control firms as our empirical analysis data set, for a total of 1,130 firms. Table 1 shows the number of firms in each country.

Empirical analysis

Before the experiment, we received approval from the human research ethics committees of the authors' universities to conduct this research and inform the treated firms of their security vulnerabilities. In addition, we contacted the firms in the treatment group to provide them with an opportunity to opt out of the experiment. Starting in July 2017, we sent out security advisory emails to firms in the treatment group every two months, for a total of three batches over a six-month period. Table 2 shows summary statistics for the main variables in our empirical analysis.

To measure the average treatment effect, we compared the treated firms' outbound spam and phishing volume before and after our experimental intervention with those from the control firms. As we sent out the first batch of emails in July 2017, we used six-month average spam and phishing volume from January 2017 to June 2017 as firms' pre-experiment security measures. To check the internal validity of our experiment, we used *t*-tests and Kolmogorov–Smirnov tests to examine whether firms in the treatment group were statistically equivalent to those in the control group. The results in Table 3 show that the differences of the average numbers and the distributions for those characteristics

Table 1. Number of firms for each country and region.

Countries and Regions	# of firms	Treatment Group	Control Group
Hong Kong	309	148	153
Mainland China	309	129	122
Singapore	264	124	127
Malaysia	171	76	84
Taiwan	138	57	57
Macao	4	2	2
Others*	67	29	20
Total	1262	565	565

Note: * IP addresses located in the target countries, but owned by global companies. In these cases, country codes follow the parent companies. Examples: Yahoo, Inc. owns 8 million IP addresses in Pan-Asian countries.

Table 2. Summary statistics.

Variable	Variable Description	Mean	SD	Max	Min
ln(CV)	Natural log-transformed CBL volume	2.099	3.667	18.420	0
ln(PV)	Natural log-transformed PSBL volume	0.393	1.339	11.969	0
ln(AV)	Natural log-transformed APWG volume	0.0340	0.275	6.125	0
ln(OV)	Natural log-transformed OpenPhish volume	0.0678	0.388	4.663	0
# of IP addresses	Total number of IP addresses owned by each firm	352038.3	3,936,268	141 million	0
HSIC	Hong Kong Standard Industrial Classification Code			960,299	50,000
email_treat	If a firm received a treatment email in this month	0.5	0.5	1	0
email_open	If a firm has opened a treatment email on or before this month	0.2062	0.4048	1	0
*if_host**	Whether a firm provides hosting services	0.5196	0.4998	1	0
high_NRI	Whether a firm's average NRI is higher than 5	0.6292	0.4830	1	0
Spam_PCA	PCA score combining *ln(CV)* and *ln(PV)*	6.86e-09	1.3035	8.5141	-0.6123
Phishing_PCA	PCA score combining *ln(AV)* and *ln(OV)*	3.10e-09	1.2671	24.0447	-0.2111

Note: * *if_host* information is only available to firms with at least one phishing website hosting.

Table 3. Baseline comparison for internal validity.

Variable	Mean Difference	*t*-statistic	K-S prob (*p*-value)
ln(CV)	-0.059860	-0.2962	0.909
ln(PV)	-0.038170	-0.5162	1.000
ln(OV)	-0.021080	-1.0929	1.000
ln(AV)	-0.001803	-0.2708	1.000
ln(# of IP addresses)	0.167300	0.7346	0.751
# of IP addresses	101837.100000	0.3094	0.751

between the treatment and control groups are marginal, and none of them are statistically significant. Therefore, our randomization satisfies the assumption of exogeneity.

Difference-in-differences (DID) analysis

Because some firms might not receive or check the treatment emails, we faced a non-compliance issue and therefore started with an intention-to-treat (ITT) analysis. We used a firm's spam volume and phishing website count from July 2017 to December 2017 as its security performance (i.e., dependent variable) after our experimental intervention. If a firm's security condition had improved, we expected a reduction of its spam and phishing activities compared with those of control firms after our treatment. Using the panel data of firms' spam and phishing information from January 2017 to December 2017, we applied a DID model to estimate the average treatment effect of our email notification. In particular, the email treatment dummy variable, $email\_treat_{\mathrm{it}}$, equals 1 if a firm i is in the treatment group and successfully received the treatment email in month t. Specifically, the ordinary least squares (OLS) regression function is as follows:

$$y_{it} = \alpha_0 + \alpha_1 email\_treat_{it} + \theta_i + \sigma_t + \varepsilon_{it}, \qquad (2)$$

where y_{it} is attack intensity according to one of the four cyberattack data sources (CBL, PSBL, APWG, OpenPhish). As shown in Table 2, the distributions of all main variables were highly skewed, thus we used log-transformed spam or phishing volume as our dependent variables.[15] In Equation (2), α_1 is our main variable of interest. If α_1 is negative and statistically significant, then compared with firms in the control group, the security performance of those in the treatment group improved after our intervention. To control for a firm's time-invariant unobservable characteristics and temporal variation, we also included firm-specific (θ_i) and month (σ_t) fixed effects in our regression.

The main results in Table 4 show that among different security performance measures, our information awareness intervention only significantly influenced firms' outbound spam volume measured by CBL. The estimated treatment effect for PSBL volume was negative but not statistically significant. We think that the different results across two data sources are probably due to the different data collection processes regarding open proxy servers.[16] Furthermore, from phishing website data, there was no evidence showing that our intervention motivated firms to reduce their phishing website hosting behavior. As the measurements for spam samples (*ln(CV)* and *ln(PV)*) and phishing samples (*ln(AV)* and *ln(OV)*) were quite different from each other, we used principal component analysis (PCA) to combine them into one score for spam (*Spam_PCA*) and phishing (*Phish_PCA*), respectively. PCA is a dimensional reduction technique that performs a linear mapping of data to a lower-dimensional space such that the variance of data in the lower dimensional representation is maximized [27]. This has been adopted in IS research [10, 56]. The analyses using PCA scores as the dependent variables are reported in Columns (3) and (6) of Table 4. When we used the spam (phishing) PCA as the dependent variable, the estimated coefficient of the *email_treat* dummy was negative (positive), though not statistically significant. It seems that our treatment has some effect to reduce spam but was not that effective in curbing phishing.

An important assumption of the DID model is the parallel trend assumption, which means that in the absence of the treatment, the difference between the control and treatment groups is constant over time [1, 4]. Violation of this assumption can lead to biased estimates. Thus, we included the leads and lags of the actual email treatment time [6]. Specifically, we added interactions between the treatment dummy and the monthly dummies and used the interaction with June (the month immediately before the first batch of treatment emails) as the baseline. Figure 3 illustrates the estimated coefficients of these interactions. It is clear that none of the pre-treatment interactions was significant, which is consistent with the parallel trend assumption, and that there was a significant post-treatment effect.

As we sent out three batches of emails, we could evaluate how the treatment effects evolve over time from the first batch to the third one. If firms put persistent emphasis on security issues,

Table 4. Difference-in-differences analysis on monthly security measures.

	ln(CV)	*ln(PV)*	*Spam_PCA*	*ln(AV)*	*ln(OV)*	*Phish_PCA*
	(1)	(2)	(3)	(4)	(5)	(6)
email_treat	-0.135**	-0.000842	-0.0265	0.00974	-0.00766	0.0111
	(0.0682)	(0.0338)	(0.0252)	(0.0114)	(0.0121)	(0.0390)
Firm fixed effects	yes	yes	yes	yes	yes	yes
Month fixed effects	yes	yes	yes	yes	yes	yes
Constant	1.893***	0.287***	-0.0958	0.0417***	0.0779***	0.0382*
	(0.0341)	(0.0166)	(0.0123)	(0.00522)	(0.00698)	(0.0205)
# of observations	13,560	13,560	13,560	13,560	13,560	13,560
# of firms	1,130	1,130	1,130	1,130	1,130	1,130
R^2	0.014	0.053	0.039	0.012	0.004	0.007

Note: Clustered standard errors in brackets.
***$p < 0.01$. **$p < 0.05$. *$p < 0.1$.

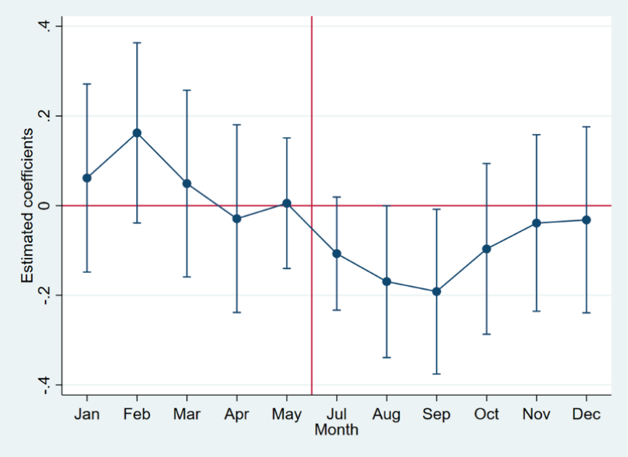

Figure 3. Monthly interaction coefficients for the difference-in-differences parallel trend test on CBL volume.

they would have responded to our emails consistently over time. Otherwise, they would have ignored the advisory emails after a few months. To empirically test this, we included three interactions representing each round of emails separately, instead of having one treatment after interaction (*email_treat*). The results in Table 5 show that the first two email batches significantly reduced firms' outbound spam volumes measured in CBL, while the last one's impact was not significant. Considering the potential lagged effects of firms' security protection measures, the significant effect in the second round might be partially due to the influence of the first email batch. This may suggest that firms may not have had enough motivation to resolve their security problems, as they stopped responding to our treatments after a few months.

Firm incentives on phishing site hosting

As shown in Tables 4 and 5, we did not observe any significant treatment effects on the reduction of phishing website hosting. We want to further understand the observed

Table 5. Different treatment effects of three batches of emails.

	ln(CV)	*ln(PV)*	*Spam_PCA*	*ln(AV)*	*ln(OV)*	*Phish_PCA*
	(1)	(2)	(3)	(4)	(5)	(6)
email_interaction1	-0.157**	0.0230	-0.0180	0.00287	-0.0105	-0.0117
	(0.0788)	(0.0485)	(0.0279)	(0.00810)	(0.0126)	(0.0356)
email_interaction2	-0.179**	-0.00936	-0.0396	0.0252	-0.000239	0.0644
	(0.0801)	(0.0340)	(0.0270)	(0.0155)	(0.0156)	(0.0552)
email_interaction3	-0.0676	0.0145	-0.00536	0.00182	-0.00525	-0.00486
	(0.0833)	(0.0441)	(0.0324)	(0.0175)	(0.0154)	(0.0559)
Firm fixed effects	yes	yes	yes	yes	yes	yes
Month fixed effects	yes	yes	yes	yes	yes	yes
Constant	1.893***	0.287***	-0.0958***	0.0417***	0.0779***	0.0382*
	(0.0341)	(0.0166)	(0.0123)	(0.00522)	(0.00698)	(0.0205)
# of observations	13,560	13,560	13,560	13,560	13,560	13,560
# of firms	1,130	1,130	1,130	1,130	1,130	1,130
R^2	0.014	0.053	0.039	0.012	0.004	0.008

Note: Clustered standard errors in brackets.
***p < 0.01. **p < 0.05. *p < 0.1.

different behaviors in terms of spam and phishing. One of our theoretical predictions is that firms may have different incentives with respect to outbound spam and phishing website hosting. While firms care about their internal security issues (i.e., their own computers being compromised), they are more reluctant to address issues that may bring a negative impact on the rest of the world (i.e., hosting phishing websites). More specifically, the phishing measure evaluates the number of phishing websites which were targeting *external* entities, not the hosted firms. In that sense, there may be an externality issue as the associated security problem does not directly harm the hosted firms. For the hosting service providers, phishing website owners could be considered as "legitimate" customers, although the hosted contents are questionable. As a result, web hosting firms may not have a strong incentive or authority to take down the websites in question owned by their customers (i.e., phishing website operators).[17]

To empirically test this conjecture, we divided firms into two groups: Group 1 (hosting firms) consists of web hosting service providers, with the rest being regarded as Group 2 (non-hosting firms). There are 51 firms in the treatment group with at least one phishing website count in any particular month. We have included these 51 firms and their corresponding 51 control firm in our analysis. For a total of 102 firms, 53 are in Group 1 and 49 firms are in Group 2. We investigated whether the firms in Group 1 responded to our treatment differently compared with those in Group 2 in terms of phishing website hosting behavior.

We created a dummy *if_host* indicating whether a firm was in Group 1 and added an interaction between the *if_host* dummy and the *email_treat* dummy. Since we did not have many observations with positive phishing website counts in either phishing measure, we used the phishing PCA (*Phish_PCA*) measure as the dependent variable. The regression results in Table 6 show that our treatment had a negative and significant effect on the firms in Group 2. In addition, compared with firms in Group 2, those in Group 1 were less responsive to our treatment as the estimated coefficient of the interaction term (*email_treat* × *if_host*) is positive and significant.[18]

IT capabilities and ICT development

As discussed earlier, IT capabilities and ICT development environment may be important factors in firms' reactions to our treatment. Compared to spam, phishing related issues are

Table 6. Heterogeneous treatment effects among hosting and non-hosting firms.

	Phish_PCA
email_treat	-0.330**
	(0.152)
email_treat × *if_host*	0.615**
	(0.287)
Firm fixed effects	Yes
Month fixed effects	Yes
Constant	0.0162
	(0.0752)
# of observations	1,224
# of firms	102
R^2	0.029

Note: Clustered standard errors in brackets.
***p < 0.01. **p < 0.05. *p < 0.1.

more difficult to resolve because more technical expertise is required to detect possible phishing activities (e.g., transaction log monitoring, traffic flow monitoring, and proactive web scanning) and close interaction with external organizations to take down phishing websites (e.g., web hosting service providers, ISPs, and legal authorities) [12]. Therefore, even when firms are aware of the phishing issues and are motivated to mitigate them, they may not have the technical expertise and resources to curb the detected phishing problem.

One unique aspect of our field experiment is that the treated firms are in different countries and regions with different ICT development levels, which can be measured by the World Economic Forum's Network Readiness Index (NRI) that ranges from 1 (lowest) to 7 (highest). Firms from high NRI countries may have more IT resources and capabilities to secure their network when a security issue has been identified. Following Bose and Leung [14], we used the latest released version of NRI prior to our experiment (year 2016) and considered a country to be in a high ICT development phase if the NRI was above 5. To explore if firms from high NRI countries and regions (e.g., Hong Kong, Macao, Singapore, and Taiwan) behaved differently when compared with those in their low NRI counterparts (e.g., Mainland China and Malaysia), we created a dummy *high_NRI* to indicate if the focal firm was in a country with a high NRI. Then we added an interaction between *email_treat* and *high_NRI* in the main analysis.

The results are reported in Table 7. Generally, we found that compared with firms in low NRI countries or regions, those in the high NRI counterparts tended to be more responsive to our treatment, as all the estimated coefficients of the interaction terms (*email_treat* × *high_NRI*) were negative. More importantly, in addition to the significant estimators when we used the CBL spam volume and the spam PCA component as the dependent variables, we found a statistically significant estimator when we used the phishing PCA component of firms as the dependent variable ($p < 0.05$).

Furthermore, we explored how firms' responses evolved over time by adding interactions between each email batch dummy and the *high_NRI* dummy. We show the results in Table 8. As in Table 7, we still found that the spam volume and the phishing website hosting of companies in countries with high NRI decreased more when compared with those in low NRI countries, as all estimated coefficients of the interactions were negative and most of them were statistically significant.

Table 7. Heterogeneous analysis on monthly security measures based on network readiness index.

	ln(CV)	*ln(PV)*	*Spam_PCA*	*ln(AV)*	*ln(OV)*	*Phish_PCA*
	(1)	(2)	(3)	(4)	(5)	(6)
email_treat	0.0673	0.0180	0.0225	0.0369*	0.00616	0.106
	(0.0895)	(0.0476)	(0.0354)	(0.0224)	(0.0180)	(0.0703)
email_treat × *high_NRI*	-0.322***	-0.0299	-0.0780**	-0.0432*	-0.0220	-0.151**
	(0.107)	(0.0499)	(0.0396)	(0.0224)	(0.0219)	(0.0733)
Firm Fixed Effects	yes	yes	yes	yes	yes	yes
Month Fixed Effects	yes	yes	yes	yes	yes	yes
Constant	1.893***	0.287***	-0.0958***	0.0417***	0.0779***	0.0382*
	(0.0339)	(0.0166)	(0.0123)	(0.00522)	(0.00698)	(0.0205)
# of Observations	13,560	13,560	13,560	13,560	13,560	13,560
# of Firms	1,130	1,130	1,130	1,130	1,130	1,130
R^2	0.016	0.053	0.040	0.013	0.004	0.009

Note: Clustered standard errors in brackets.
***$p < 0.01$. **$p < 0.05$. *$p < 0.1$.

Table 8. Heterogeneous analysis on three batches of emails based on network readiness index.

	ln(CV)	*ln(PV)*	*Spam_PCA*	*ln(AV)*	*ln(OV)*	*Phish_PCA*
	(1)	(2)	(3)	(4)	(5)	(6)
email_interaction1	0.0407	-0.0383	-0.0124	0.0183	0.00117	0.0493
	(0.102)	(0.0702)	(0.0387)	(0.0126)	(0.0201)	(0.0559)
email_interaction1× high_NRI	-0.316***	0.0997	-0.00834	-0.0245*	-0.0186	-0.0970
	(0.118)	(0.0753)	(0.0436)	(0.0131)	(0.0221)	(0.0611)
email_interaction2	0.0887	0.00874	0.0217	0.0615*	0.0194	0.194*
	(0.106)	(0.0461)	(0.0367)	(0.0313)	(0.0222)	(0.101)
email_interaction2× high_NRI	-0.424***	-0.0274	-0.0963**	-0.0572*	-0.0310	-0.204*
	(0.122)	(0.0509)	(0.0417)	(0.0324)	(0.0267)	(0.107)
email_interaction3	0.0976	0.131*	0.0878*	0.0490	0.0133	0.150
	(0.111)	(0.0728)	(0.0515)	(0.0330)	(0.0231)	(0.0932)
email_interaction3× high_NRI	-0.261**	-0.178**	-0.145***	-0.0735**	-0.0290	-0.242**
	(0.127)	(0.0713)	(0.0535)	(0.0322)	(0.0277)	(0.0944)
Firm Fixed Effects	yes	yes	yes	yes	yes	yes
Month Fixed Effects	yes	yes	yes	yes	yes	yes
Constant	1.893***	0.287***	-0.0958***	0.0417***	0.0779***	0.0382*
	(0.0339)	(0.0166)	(0.0123)	(0.00522)	(0.00698)	(0.0205)
# of Observations	13,560	13,560	13,560	13,560	13,560	13,560
# of Firms	1,130	1,130	1,130	1,130	1,130	1,130
R^2	0.017	0.054	0.041	0.015	0.005	0.010

Note: Clustered standard errors in brackets.
****p* < 0.01. ***p* < 0.05. **p* < 0.1.

Treatment effect of opening emails

Our experiment may face the compliance issue as some firms might ignore our advisory emails. As a result, we explored the treatment effects for the firms which *opened* the advisory emails based on our tracking tools. Table 9 shows the firms' responses to our treatments, which were followed by email tracking (SendGrid) and web analytics (Piwik) tools. For the table, the treatment group was divided into two subgroups based on spam and phishing records in 2017. Among 565 firms that received the advisory emails, 260 (46.0%) opened the emails. Furthermore, the firms without prior security issues were more likely to open the treatment email. This result may indicate that firms that had better protection cared more about security-related news (*Z*-score = 1.4011, *p*-value = 0.0808, one-tailed). However, once the email was opened, website visit rates and multiple visit rates were nearly identical within the minimal error rate between the two groups.

One econometric challenge of estimating the treatment effects of opening advisory emails is that such actions were *endogenously* determined by the treated firms. Thus, directly estimating the regressions with corresponding dummy variables may lead to biased estimators.[19] We tried to deal with this issue in two ways. In the first analysis,

Table 9. Email open/website visit counts among 565 firms that received our treatment email.

	# of Firms in the Treatment Group			
Volume from All Data Sources	Total	Opened Email (per Total)	Visited Website (per Opened Email)	Multiple Visits (per Visited Website)
Firms with No Spam and Phishing	308	150 (48.7%)	44 (29.3%)	33 (75.0%)
Firms with 1+ Spam or Phishing	257	110 (42.8%)	32 (29.0%)	25 (78.1%)
Total	565	260 (46.0%)	76 (29.2%)	58 (76.3%)

we used the dummy variable, *email_treat*, indicating whether the security measure was from a treated firm after July 2017 as an instrumental variable (IV) for a firm's decision to open an email, taking advantage of the randomization design.[20] In the second analysis, we conducted a subsample assessment and only used the data from firms that opened at least one email and their corresponding control firms.

Because only firms in the treatment groups could receive the advisory emails, the monotonicity condition of IV was satisfied in this case. Then, we applied two-stage least squares (2SLS) to estimate the average causal effect of treatment (ATET) on opening our email [44, 49]. The regression functions of our 2SLS approach are as follows:

$$D_{it}^{*} = \gamma_0 + \gamma_1 * email\_treat_{it} + \epsilon_{it}, \tag{3}$$

with the observed email opening indicator, $email\_open_{it}$, related to the unobserved latent index, D_{it}^{*}, by

$$email\_open_{it} = \begin{cases} 1, & D_{it}^{*} > 0 \\ 0, & D_{it}^{*} \leq 0. \end{cases} \tag{4}$$

Furthermore, the dependent variable y_{it} is related to the treatment by Equation (5):

$$y_{it} = \beta_0 + \beta_1 * email\_open_{it} + \mu_{it} \tag{5}$$

The results for the local average treatment effect (LATE) of opening an email are reported in Table 10. All the standard deviations were robust and clustered at the firm level. Similar to the results in Table 4, only the coefficient of firms' spam volume based on CBL was negative and significant. However, the magnitude of the coefficient was much larger (-0.427 vs. -0.135), indicating that firms that opened the emails tended to be more responsive to our treatment. More specifically, outbound spam volume from the firms that opened our emails decreased by 34.8%. There are two potential reasons that can explain this result: (i) the advisory emails may have provided useful security-related information to the treated firms, leading to enhanced security performance; and (ii) firms which chose to open our emails were those that were more vigilant about potential security threats. Therefore, they were more likely to improve their security safety measures after receiving our treatment emails.

Table 10. Two-stage least squares analysis for heterogeneous treatment effects on opening treatment emails.

	ln(CV)	*ln(PV)*	*Spam_PCA*	*ln(AV)*	*ln(OV)*	*Phish_PCA*
	(1)	(2)	(3)	(4)	(5)	(6)
email_open	-0.427**	-0.0292	-0.0978	0.0239	-0.0271	0.0120
	(0.208)	(0.0972)	(0.0752)	(0.0341)	(0.0356)	(0.116)
Constant	1.893***	0.287***	-0.0958***	0.0417***	0.0779***	0.0382*
	(0.0340)	(0.0166)	(0.0123)	(0.00522)	(0.00698)	(0.0205)
Firm Fixed Effects	yes	yes	yes	yes	yes	yes
Month Fixed Effects	yes	yes	yes	yes	yes	yes
# of Observations	13,560	13,560	13,560	13,560	13,560	13,560
# of Firms	1,130	1,130	1,130	1,130	1,130	1,130

Note: Clustered standard errors in brackets.
***p < 0.01. **p < 0.05. *p < 0.1.

In the second analysis, we applied a DID model on data from a subset of firms in our experiment. The caveat of this method is that compliance was self-selected, and the remaining subsample was not representative of all firms in our study. As we randomly assigned the remained firms in the treatment or control group, we can compare the security measures of firms that opened treatment emails with those of control firms to estimate the treatment effects of opening emails. The results are reported in Table 11. Consistently, we found significant treatment effects for treated firms in terms of spam volume. And the treatment effect for CBL spam was larger compared with it using all firms' data in Table 4 (-0.218 vs. -0.135), as expected.

Overall security performance

Thus far, we have investigated how firms' security protection evolved after our treatments based on individual security measures (i.e., spam volume and phishing website count). Another important question to explore is how the treated firms' *overall* security conditions changed after our interventions. We utilized the ranking data based on the Borda count, which we reported both in the advisory emails and websites, allowing us to combine four different measures.

After we created the Borda count for each firm-month observation, we ranked all firms based on the value by country and industry. Then, we used the ranking information as the dependent variable and repeated the DID analysis. The results are reported in Table 12. The results show that after our experiment, the treated firms' country-level security ranking significantly improved (lower ranking means better security performance). However, for the industry-level ranking, the results were not statistically significant. In addition, based on the results of monthly interactions in Figure 4, we observed a significant treatment effect only for the first email batch, not the second and third ones. This echoes the results in the main analysis that our treatment effects were short term.

Discussion

In our experiment, we used outbound spam emails and phishing websites as two distinct perceptible cyberattack data sources to measure firms' pre- and post-experimental security vulnerability levels. From a series of regression analyses, we found evidence that the security vulnerability awareness has a statistically significant effect on reducing spam

Table 11. Treatment effects on opening treatment emails based on a subset of firms.

	ln(CV)	*ln(PV)*	*Spam_PCA*	*ln(AV)*	*ln(OV)*	*Phish_PCA*
	(1)	(2)	(3)	(4)	(5)	(6)
email_open	-0.218**	-0.00706	-0.0533*	0.0193	-0.00822	0.0415
	(0.0881)	(0.0348)	(0.0316)	(0.0149)	(0.0153)	(0.0609)
Constant	1.499***	0.183***	-0.0909***	0.0287***	0.0625***	0.0374
	(0.0480)	(0.0227)	(0.0201)	(0.00622)	(0.0108)	(0.0343)
Firm Fixed Effects	yes	yes	yes	yes	yes	yes
Month Fixed Effects	yes	yes	yes	yes	yes	yes
# of Observations	5,280	5,280	5,280	5,280	5,280	5,280
# of Firms	440	440	440	440	440	440

Note: Clustered standard errors in brackets.
***p < 0.01. **p < 0.05. *p < 0.1.

Table 12. Analysis on firms' security rankings.

	Full Sample		Positive Security Measures	
	Country Rank	Industry Rank	Country Rank	Industry Rank
	(1)	(2)	(3)	(4)
email_treat	0.563**	0.177	1.304**	0.447
	(0.276)	(0.231)	(0.532)	(0.459)
Firm Fixed Effects	yes	yes	yes	yes
Month Fixed Effects	yes	yes	yes	yes
Constant	35.44***	22.59***	33.74***	22.68***
	(0.181)	(0.144)	(0.313)	(0.255)
# of Observations	13,560	13,560	5,472	5,472
# of Firms	1,130	1,130	456	456
R^2	0.261	0.135	0.153	0.071

Note: Clustered standard errors in brackets.
***p < 0.01. **p < 0.05. *p < 0.1.

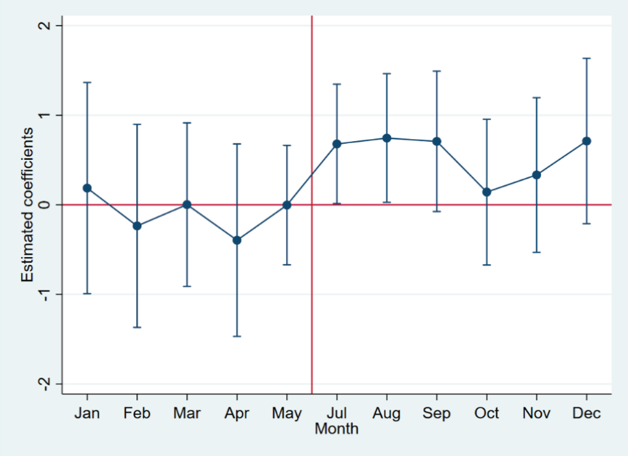

Figure 4. Monthly interaction coefficients for the difference-in-differences parallel trend test on country level ranking.

volume associated to open proxy behavior, but not on decreasing phishing website hosting. The results also show that the magnitude of the treatment effects with respect to CBL spam volume increased from receiving emails (-0.135 in the DID results from Table 4) to opening emails (-0.427 in the 2SLS results from Table 10). The non-significant results in PSBL may be due to the fact that the data source does not flag IP addresses with open proxy server issues, which are considered to be an easy-to-fix spam issue. With the awareness of open proxy issues, IT staff can easily block such spamming behavior with appropriate firewall setups. Putting things together, the empirical results show that publicized security information may have compelled firms to adopt better preventive measures against spam emission. Interestingly, we did not find a statistically significant effect on reducing phishing website hosting behavior. Additional analyses show that the potential reasons for the limited treatment effects are firms' lack of economic incentives and IT capabilities to address security issues.

Web hosting firms do not have economic incentives to eliminate phishing websites because they are operated by legitimate customers of the hosting services. As a result, they let phishing websites exist and pose threats to the unvigilant general public. This can be considered as a negative externality issue. Second, due to a lack of phishing-related laws and policies, web hosting companies face fewer liability risks for the phishing attacks and the resulting damages. Following this line, web hosting service providers may pass the responsibilities onto their customers. Third, web hosting companies may need to adhere to the non-self-censorship principle, and they do not filter the content of web materials uploaded by their customers, allowing phishers to abuse the firms' web hosting services due to their malicious phishing activities. In addition, we found some evidence that security information awareness may induce positive changes: among the 46 treated firms who hosted phishing websites according to OpenPhish data, six of them actually eliminated all phishing websites within one or two months after their first response (opened an email and/or visited the website) to our treatment. Based on the other phishing data source (APWG), among 31 firms who hosted phishing websites, four fully addressed the issues. This result may suggest that firms' incentives play an important role in their security defense strategy.

Another potential reason for the non-significant treatment effect on phishing in our main analysis is that some firms may not have sufficient IT capabilities or resources to resolve the phishing problems. Although we did not observe significant average treatment effects for phishing on average for all firms, we did observe that firms in countries with high NRI were more responsive to our treatment compared with those in low NRI countries. As firms rely on technical expertise and resources to curb phishing, if they operate in an environment with high ICT development, they may be more capable of handling the phishing problems. In contrast, even though firms are aware of the issue, some in the low ICT development countries may not be able to fix it due to a lack of IT capabilities.

For the results, we would like to highlight the findings and differentiate our study from He et al. [24] and Tang and Whinston [53] in the following ways. First, our DID analysis shows that the treated firms which received our three batches of treatment emails improve their security over time when compared with the controlled ones. In particular, the effect was statistically significant in the reduction of CBL spams but not in that of phishing website hosting. Such findings were not observed in the two prior studies. Second, our finding on the non-significant effect on phishing site hosting behavior is quite new. We believe that the non-significant effect may be due to misaligned incentives of companies (e.g., web hosting firms) and insufficient IT capabilities at the country level. This result may offer new insights to understand firm behaviors in different business sectors and countries, which were not documented in the two studies. Finally, it is worth noting that it was difficult to directly compare the differences across the countries in Pan-Asia in the sense that some countries had a relatively small number of samples. Such an imbalanced data sample, however, may have resulted in low statistical power to produce significant estimators. To solve the issue of imbalanced data, previous research used NRI to divide the firms into high NRI and low NRI groups [14]. Our study followed this line of work to observe the differences between the low and high NRI groups, as previously discussed.

To summarize, our empirical results show that (i) the security vulnerability awareness can be effective in reducing outgoing spam associated to open proxy behavior and that (ii) firms have different incentives and IT environments in terms of managing phishing websites. These findings may have important policy implications in that stronger regulations may be required to internalize the negative externalities in information security. Our analysis also shows that publicize information security performance may be an alternative approach to legal enforcements to encourage firms to invest in security improvement and to adopt better security measures. Finally, the findings suggest that cybersecurity policies should be aligned with national ICT development strategies.

Conclusion

The U.S. Department of State and European Commission advocates the use of the 3Ps, namely, prevention, protection, and prosecution, to combat crime (e.g., human trafficking and domestic violence).[21] Despite the wisdom contained in the idiom "prevention is better than cure," prevention is still the weakest link in combating the widespread cybercrime. Due to negative externalities and misaligned incentives, firms may simply choose to adopt insufficient preventive solutions. To some extent, this is very similar to air pollution as people who connect insecure computers to the network do not bear the full consequences of their actions [5, 9]. In this research, we showed that publicizing a vulnerability index may alleviate such misaligned incentives. To some extent, such an approach may achieve similar results to other measures such as legislation [18], subsidies for self-protection [41], and penalties/taxes for non-compliance [33] to heighten public awareness to related cybercrime. Moreover, our proposed approach requires lower processing costs (e.g., time and effort to collect evidence for prosecution) and may incentivize firms to uphold their origin responsibility, which is one of the five principles of the Bright ICT Initiatives [33, 34].

Although our study is based on a large-scale field experiment with a robust security index, it is not without limitations. One limitation is that the treatment communication channel to subjects was only through emails. The message could only be received by IT staff, rather than customers or investors of focal firms. As a result, the publicity effect may be limited. To enhance the communication channels, future studies can use social media platforms (e.g., Twitter, Facebook, LinkedIn, Weibo, and WeChat) so that social media followers (e.g., customers and strategic partners) will be informed of treated firms' security evaluation reports. Thus, information disclosure on social media may lead to more pronounced treatment effects.

Another limitation of our study is that we only focused on firms in six Pan-Asian countries and regions. A possible extension is to expand the scope of the experiment to firms in other countries. Because our data sources include phishing and spam data from more than 200 countries worldwide, the framework used to construct the security index can be generalized to other regions. With a larger sample size, we may be able to test the efficacy of different treatment group. In other words, advisory emails on spam and phishing issues may make firms aware of other cybercrimes and improve their overall security levels.

Notes

1. An analogy to adoption of security technology is vaccinating children against a contagious disease. A parent may choose not to vaccinate their children and freeride on others in the same community who have already done so.
2. Such uncertainty may lead to the problem of "market for lemons" or information asymmetry [3].

3. An example is that a consumer is more willing to spend $20 to buy anti-virus software to prevent virus from contaminating his/her own hard disk rather than spending the same amount of money to prevent virus attacks on someone else.
4. Origin refers to firms whose servers may be compromised to send undesired content to the Internet and the firm owners may or may not be aware of such a problem and have control of it [33].
5. Note that the term "spam mail" in this paper includes advertisement, phishing mail, and malware attached email.
6. Note that phishing, in this paper, exclusively refers to website-related incidents, and we only focus on the firms who are actually hosting the phishing websites on their own server. All email-related attacks including phishing emails are included in our spam data.
7. We acknowledge that other cyberattacks (e.g., DDoS and identity thefts) can also serve the purpose if the related data sources are publicly available.
8. https://www.abuseat.org/
9. https://psbl.org/
10. https://apwg.org/
11. https://openphish.com/
12. We recognize that some IP prefixes are geographically located in countries that are different from the ASN's countries. To address this possible country mismatch issue, we used Team Cymru data that provides IP prefix level country code (https://www.team-cymru.com/IP-ASN-mapping.html).
13. WHOIS is a database system to which maintains who is responsible for a domain name or an IP address. The website is: https://whois.icann.org/en
14. Sendgrid: https://sendgrid.com/
15. Specifically, using CBL spam volume as an example, the dependent variable used in the analysis is $ln(CV) = log(CV + 1)$.
16. The different result across CBL and PSBL is probably due to the different data collection processes. CBL lists IP addresses "exhibiting characteristics which are specific to open proxies of various sorts (https://www.abuseat.org)", while Spamikaze (the system that PSBL is using) "does not tests for open proxy or open relay vulnerabilities (https://spamikaze.org/AboutSpamikaze)." An open proxy is "a non-email server that can be tricked into sending emails to third parties" (https://www.abuseat.org/faq.html).
17. One may argue that outbound spam data may have similar firm incentive issues if the email senders are deliberately sending massive emails. However, CBL and PSBL pay special attention not to flag any legitimate email sending servers. Below are quotes from the data sources: "virtually all listees are the victims of a virus or other compromise, not deliberately spamming (https://www.abuseat.org)" and "an IP address gets added to the PSBL when it sends email to a spamtrap, that email is not identified as non-spam and the IP address is not a known mail server (https://psbl.org)."
18. Because of the small sample size, we also used bootstrap method to calculate the standard deviation, which does not require distributional assumption and can provide more accurate inferences when the sample size is small [20]. The result is consistent.
19. In our 2SLS analysis, we have adopted a Wu-Hausman test and the Hansen J statistic for the CBL as the dependent variable is 6.434 (Chi-sq p-value is 0.0112). The results support that the variable *email_open* is not exogenous.
20. As we are using an RFE to find the treatment effects, being in the treatment group for a firm is exogenous to a firm's security conditions, which are the dependent variables. Besides, a firm can only open an email if it is in the treatment group, which makes the treatment dummy a valid IV for the analysis.
21. See https://www.state.gov/3ps-prosecution-protection-and-prevention/ and https://ec.europa.eu/justice/grants/results/daphne-toolkit/content/3ps-prevention-protection-prosecution_en for details.

Acknowledgements

The authors are grateful to the guest editors, Robert J. Kauffman and Thomas A. Weber, and three anonymous reviewers for their excellent comments and suggestions. They are indebted to Anandhi Bharadwaj, Arun Rai, H. R. Rao, Raghu Santanam, and the participants at the WITS 2017, IS OneWorld and Annual Security Conference 2017, WEIS 2018, BIGS 2018, CityU IS Summer Workshop 2018, and HICSS 2020 for their valuable suggestions to improve the working paper. The authors thank Mark Varga, Markus Iivonon, Jessie Ma, and Ishwara Manjunath Hegde for their excellent research assistance. The authors are solely responsible for the content and any issues that may arise from the article.

Funding

The work was fully supported by grants from the US National Science Foundation (NSF Award Number: 1718360), HK Public Policy Research Funding Scheme (Project Number: 2015.A1.030.16A) from the Policy Innovation and Coordination Office of the Hong Kong Special Administrative Region Government, and CityU Digital Innovation Laboratory.

ORCID

Yunhui Zhuang http://orcid.org/0000-0003-4950-8481
Shu He http://orcid.org/0000-0001-5899-5299
Alvin Chung Man Leung http://orcid.org/0000-0001-8961-8357
Gene Moo Lee http://orcid.org/0000-0003-0657-6898
Andrew Whinston http://orcid.org/0000-0002-7371-8991

References

1. Abadie, A. Semiparametric difference-in-differences estimators. *The Review of Economic Studies 72*, 1 (2005), 1–19.
2. Adelsman, R.M.; and Whinston, A.B. Sophisticated voting with information for two voting functions. *Journal of Economic Theory 15*, 1 (1977), 145–159.
3. Akerlof, G.A. The market for “lemons”: Quality uncertainty and the market mechanism. *The Quarterly Journal of Economics 84*, 3 (1970), 488–500.
4. Angrist, J.D.; and Pischke, J.S. *Mostly Harmless Econometrics: An Empiricist’s Companion*. Princeton, NJ: Princeton University Press, 2008.
5. August, T.; August, R.; and Shin, H. Designing user incentives for cybersecurity. *Communications of the ACM 57*, 11 (2014), 43–46.
6. Autor, D.H. Outsourcing at will: The contribution of unjust dismissal doctrine to the growth of employment outsourcing. *Journal of Labor Economics 21*, 1 (2003), 1–42.
7. Ba, S.; Whinston, A.B.; and Zhang, H. The dynamics of the electronic market: An evolutionary game approach. *Information Systems Frontiers 2*, 1 (2000), 31–40.
8. Baker, J. The technology–organization–environment framework. In, Dwivedi, Y.K., Wade, M. R., and Schneberger, S.L., (eds.), *Information Systems Theory: Explaining and Predicting Our Digital Society*, Vol. 1, New York, NY: Springer New York, 2012, pp. 231–245.
9. Bauer, J.M.; and van Eeten, M.J.G. Cybersecurity: Stakeholder incentives, externalities, and policy options. *Telecommunications Policy 33*, 10 (2009), 706–719.
10. Bergeron, F.; Rivard, S.; and de Serre, L. Investigating the support role of the information center. *MIS Quarterly 14*, 3 (1990), 247–260.
11. Bhatt, G.D.; and Grover, V. Types of information technology capabilities and their role in competitive advantage: An empirical study. *Journal of Management Information Systems 22*, 2 (2005), 253–277.

12. Bose, I.; and Leung, A.C.M. Unveiling the mask of phishing: Threats, preventive measures, and responsibilities. *Communications of the Association for Information Systems 19* (2007), 24.
13. Bose, I.; and Leung, A.C.M. Do phishing alerts impact global corporations? A firm value analysis. *Decision Support Systems 64* (2014), 67–78.
14. Bose, I.; and Leung, A.C.M. Adoption of identity theft countermeasures and its short- and long-term impact on firm value. *MIS Quarterly 43*, 1 (2019), 313–327.
15. Brown, S.; and Hillegeist, S.A. How disclosure quality affects the level of information asymmetry. *Review of Accounting Studies 12*, 2 (2007), 443–477.
16. Chatterjee, S.; Sarker, S.; and Valacich, J.S. The behavioral roots of information systems security: Exploring key factors related to unethical IT use. *Journal of Management Information Systems 31*, 4 (2015), 49–87.
17. Chen, Y.; and Zahedi, F. Individuals' internet security perceptions and behaviors: Polycontextual contrasts between the United States and China. *MIS Quarterly 40*, 1 (2016), 205.
18. D'Arcy, J.; Hovav, A.; and Galletta, D. User awareness of security countermeasures and its impact on information systems misuse: A deterrence approach. *Information Systems Research 20*, 1 (2009), 79–98.
19. Eeten, M.; and Bauer, J. Economics of malware: Security decisions, incentives and externalities. OECD Science, Technology and Industry Working Papers, Directorate for Science, Technology and Industry, OECD, Paris, France, 2008.
20. Efron, B. *An Introduction to the Bootstrap*. New York: Chapman & Hall, 1993.
21. Gal-Or, E.; and Ghose, A. The economic incentives for sharing security information. *Information Systems Research 16*, 2 (2005), 186–208.
22. Gordon, L.A.; Loeb, M.P.; and Lucyshyn, W. Information security expenditures and real options: A wait-and-see approach. *Computer Security Journal 19*, 2 (2003), 1–7.
23. Gordon, L.A.; Loeb, M.P.; and Sohail, T. Market value of voluntary disclosures concerning information security. *MIS Quarterly 34*, 3 (2010), 567–594.
24. He, S.; Lee, G.M.; Han, S.; and Whinston, A.B. How would information disclosure influence organizations' outbound spam volume? Evidence from a field experiment. *Journal of Cybersecurity 2*, 1 (2016), 99–118.
25. Heckman, J.J.; and Smith, J.A. Assessing the case for social experiments. *The Journal of Economic Perspectives 9*, 2 (1995), 85–110.
26. Hui, K.-L.; Kim, S.; and Wang, Q.-H. Cybercrime deterrence and international legislation: Evidence from distributed denial of service attacks. *MIS Quarterly 41*, 2 (2017), 497.
27. Jolliffe, I.T. *Principal Component Analysis*. New York: Springer-Verlag, 2002.
28. Kim, S.; Wang, Q.-H.; and Ullrich, J. A comparative study of cyberattacks. *Communications of the ACM 55*, 3 (2012), 66–73.
29. Kim, S.H.; and Kim, B.C. Differential effects of prior experience on the malware resolution process. *MIS Quarterly 38*, 3 (2014), 655–678.
30. Kuan, K.K.Y.; and Chau, P.Y.K. A perception-based model for EDI adoption in small businesses using a technology–organization–environment framework. *Information & Management 38*, 8 (2001), 507–521.
31. Kunreuther, H.; and Heal, G. Interdependent security. *Journal of Risk and Uncertainty 26*, 2 (2003), 231–249.
32. Kwon, J.; and Johnson, E.M. Meaningful healthcare security: Does meaningful-use attestation improve information security performance? *MIS Quarterly 42*, 4 (2018), 1043–1067.
33. Lee, J.K. Research framework for AIS grand vision of the Bright ICT initiative. *MIS Quarterly 39*, 2 (2015), iii–xii.
34. Lee, J.K.; Cho, D.; and Lim, G.G. Design and validation of the Bright Internet. *Journal of the Association for Information Systems 19*, 2 (2018), 63–85.
35. Menard, P.; Bott, G.J.; and Crossler, R.E. User motivations in protecting information security: Protection motivation theory versus self-determination theory. *Journal of Management Information Systems 34*, 4 (2017), 1203–1230.

36. Mitra, S.; and Ransbotham, S. Information disclosure and the diffusion of information security attacks. *Information Systems Research 26*, 3 (2015), 565–584.
37. Moore, T. The economics of cybersecurity: Principles and policy options. *International Journal of Critical Infrastructure Protection 3*, 3 (2010), 103–117.
38. Moore, T.; and Clayton, R. The impact of public information on phishing attack and defense. *Communications & Strategies 1*, 81 (2011), 45–68.
39. Moore, T.; Clayton, R.; and Anderson, R. The economics of online crime. *Journal of Economic Perspectives 23*, 3 (2009), 3–20.
40. Morgan, K.L.; and Rubin, D.B. Rerandomization to improve covariate balance in experiments. *The Annals of Statistics 40*, 2 (2012), 1263–1282.
41. Öğüt, H.; Raghunathan, S.; and Menon, N. Cyber security risk management: Public policy implications of correlated risk, imperfect ability to prove loss, and observability of self-protection. *Risk Analysis 31*, 3 (2011), 497–512.
42. Png, I.P.L.; Wang, C.-Y.; and Wang, Q.-H. The deterrent and displacement effects of information security enforcement: International evidence. *Journal of Management Information Systems 25*, 2 (2008), 125–144.
43. Quarterman, J.S.; Linden, L.L.; Tang, Q.; Lee, G.M.; and Whinston, A.B. Spam and botnet reputation randomized control trials and policy. The 41st Research Conference on Communication, Information and Internet Policy, George Mason University, Arlington, VA, 2013.
44. Rubin, D.B. Basic concepts of statistical inference for causal effects in experiments and observational studies. Cambridge, MA: Harvard University, 2004, pp. 1–140.
45. Sanchez, F.; Duan, Z.; and Dong, Y. Blocking spam by separating end-user machines from legitimate mail server machines. *Security and Communication Networks 9*, 4 (2016), 316–326.
46. Santanam, R.; Sethumadhavan, M.; and Virendra, M. *Cyber Security, Cyber Crime and Cyber Forensics: Applications and Perspectives*. Hershey, United States: IGI Global, 2010.
47. Sen, R.; and Borle, S. Estimating the contextual risk of data breach: An empirical approach. *Journal of Management Information Systems 32*, 2 (2015), 314–341.
48. Shetty, N.; Schwartz, G.; and Walrand, J. Can competitive insurers improve network security? In, Acquisti, A., Smith, S.W., and Sadeghi, A.-R., (eds.), *Trust and Trustworthy Computing*, Berlin, Heidelberg: Springer Berlin Heidelberg, 2010, pp. 308–322.
49. Sommer, A.; and Zeger, S.L. On estimating efficacy from clinical trials. *Statistics in Medicine 10*, 1 (1991), 45–52.
50. Symantec. Internet security threat report 2016. Mountain View, CA, 2016.
51. Symantec. Internet security threat report 2017. Mountain View, CA, 2017.
52. Tan, C.L.; Chiew, K.L.; Wong, K.; and Sze, S.N. Phishwho: Phishing webpage detection via identity keywords extraction and target domain name finder. *Decision Support Systems 88* (2016), 18–27.
53. Tang, Q.; and Whinston, A.B. Do reputational sanctions deter negligence in information security management? A field quasi-experiment. *Production and Operations Management 29*, 2 (2020), 410–427.
54. van Wanrooij, W.; and Pras, A. Filtering spam from bad neighborhoods. *International Journal of Network Management 20*, 6 (2010), 433–444.
55. Wang, J.; Xiao, N.; and Rao, H.R. Research note—an exploration of risk characteristics of information security threats and related public information search behavior. *Information Systems Research 26*, 3 (2015), 619–633.
56. Weill, P. The relationship between investment in information technology and firm performance: A study of the valve manufacturing sector. *Information Systems Research 3*, 4 (1992), 307–333.
57. Wright, R.T.; Jensen, M.L.; Thatcher, J.B.; Dinger, M.; and Marett, K. Influence techniques in phishing attacks: An examination of vulnerability and resistance. *Information Systems Research 25*, 2 (2014), 385–400.

58. Zeng, V.; Baki, S.; Aassal, A.E.; Verma, R.; Moraes, L.F.T.D.; and Das, A. Diverse datasets and a customizable benchmarking framework for phishing. In *Proceedings of the Sixth International Workshop on Security and Privacy Analytics*, New York: ACM Press, 2020.
59. Zhou, W.; and Piramuthu, S. IoT security perspective of a flexible healthcare supply chain. *Information Technology and Management 19*, 3 (2018), 141–153.
60. Zhu, K.; and Kraemer, K.L. Post-adoption variations in usage and value of e-business by organizations: Cross-country evidence from the retail industry. *Information Systems Research 16*, 1 (2005), 61–84.
61. Zhu, K.; Kraemer, K.; and Xu, S. Electronic business adoption by European firms: A cross-country assessment of the facilitators and inhibitors. *European Journal of Information Systems 12*, 4 (2003), 251–268.
62. Zhu, K.; Kraemer, K.L.; and Dedrick, J. Information technology payoff in e-business environments: An international perspective on value creation of e-business in the financial services industry. *Journal of Management Information Systems 21*, 1 (2004), 17–54.

About the Authors

Yunhui Zhuang (yhzhuang2-c@my.cityu.edu.hk) is a Postdoctoral Fellow in the Department of Information Systems at College of Business, City University of Hong Kong. He received his Ph.D. in Computer Science from that university. Dr. Zhuang’s research interests lie at the intersection of economics and information security. In particular, he is interested in applied cryptography, security and privacy of mobile payments, financial technology, business analytics, applied econometrics, and e-learning.

Yunsik Choi (yun@aitrics.com) is the Head of Technical Sales and Research Scientist at AITRICS. He received his Ph.D. in Computer Science from the University of Texas at Austin. His research interests include artificial intelligence and security. Dr. Choi provides deep-learning and machine-learning solutions and consulting services to companies that need to implement AI technologies for their products.

Shu He (shu.he@uconn.edu) is an Assistant Professor at the Department of Operations and Information Management, School of Business, University of Connecticut. She earned her Ph.D. in Economics from the University of Texas at Austin. Dr. He’s research interests include social media, platform, online advertising, and cybersecurity. Her work has appeared in *Information Systems Research, MIS Quarterly*, and *Journal of Cybersecurity*. She has received a National Science Foundation grant to support her research.

Alvin Chung Man Leung (acmleung@cityu.edu.hk) is an Associate Professor at the Department of Information Systems, College of Business, City University of Hong Kong. He received his Ph.D. in Information, Risk, and Operations Management from McCombs School of Business, the University of Texas at Austin. His research interests include IT business value, information security, and FinTech. His work has appeared in *Management Science, Information Systems Research, MIS Quarterly*, and *Decision Support Systems.*

Gene Moo Lee (gene.lee@sauder.ubc.ca; corresponding author) is an Assistant Professor of Information Systems at the Sauder School of Business, University of British Columbia, Canada. He received his Ph.D. in Computer Science from the University of Texas at Austin. Dr. Lee’s research program takes big data analytics approaches to study online platforms, tech ecosystems, and unintended consequences of technology. His works have appeared in *Information Systems Research, Journal of Management Information Systems, MIS Quarterly*, and *Journal of Business Ethics*. He has industry experiences at Samsung, AT&T, Intel, and Goldman Sachs, and holds 11 patents in mobile technology.

Andrew B. Whinston (abw@uts.cc.utexas.edu) is the Hugh Cullen Chair Professor in the Department of Information, Risk, and Operation Management at the McCombs School of

Business at the University of Texas at Austin. He is also Director at the Center for Research in Electronic Commerce. Dr. Whinston has published over 300 papers in major economic and management journals and has co-authored 27 books. His Erdös number is 2.