Journal of Computer Information Systems

ISSN: 0887-4417 (Print) 2380-2057 (Online) Journal homepage: http://www.tandfonline.com/loi/ucis20

Online Security Performances and Information Security Disclosures

David C. Li

To cite this article: David C. Li (2015) Online Security Performances and Information Security Disclosures, Journal of Computer Information Systems, 55:2, 20-28

To link to this article: http://dx.doi.org/10.1080/08874417.2015.11645753

ONLINE SECURITY PERFORMANCES AND INFORMATION SECURITY DISCLOSURES

DAVID C. LI
The Hong Kong Polytechnic University
Kowloon, Hong Kong

ABSTRACT

This study tests whether the voluntary disclosures in the annual reports concerning information security are credible. It also develops a scale to measure online security performances and identifies influencing factors. Our findings provide insights into the online security performances of financial institutions. Specifically, they manifest the similarity of online security performances within the same business sector and across different markets. Through finding a positive relation between online security performances and information security disclosures, our results confirm the credibility of the latter. Our study also extends the Technology-Organization-Environment framework for explaining online security performances. While the results show all three variables: (1) importance of information security as measured by its disclosures, (2) existence of government regulation, and (3) firm size, have significant and positive effects on online security performances, only the first two variables have such effects on the adoption of two-factor authentication.

Keywords: Online security, authentication, Technology-Organization-Environment framework, voluntary disclosures, information security

INTRODUCTION

Online security, a major component of information security, aims to protect the information-rated assets of users and operator of a Web site in e-commerce transactions through employing technologies, policies and procedures. To achieve this objective, the site operator has to guard against security threats such as hacking, phishing and identity theft. Online security continues to be an important issue because any security breach will damage the reputation of an online business and may cause substantial financial loss due to litigation and disruption of business. A survey of financial institutions (hereafter FIs) has shown an increase in attacks by hackers [34]. To combat the threats, the regulators in the Greater China region, which includes mainland China, Taiwan and Hong Kong, have recommended the banks to strengthen the online security and adopt two-factor authentication (hereafter 2FA) in particular. An authentication factor is a secret piece of information linked to a user's identity like username. There are three common types of authentication factors: knowledge-based (i.e. something a person knows); possession-based (i.e. something a person has); and biometric-based (i.e. something a person is). 2FA requires two different types of factors for logging in an online account.

Despite the regulators' recommendation has been released for several years, the extent of compliance is not known as empirical studies remain lacking. A prior study has indicated that password remains the single factor of authentication for accessing online banking and securities trading accounts in the USA [32]. A question then arises as to whether the FIs in the Greater China region have similar online security performances (hereafter OSPs). OSP reflects the level of online security adopted by a firm engaging in e-commerce. For the purpose of this paper, OSPs are evaluated based on an 18-item scale shown in Table 1. This scale is necessary because management of online security risk, which is one type of operational risk, is increasingly getting important [41]. Prior studies seldom tested a comprehensive list of online security features. Instead, they used a small number of visual security cues to elicit respondents' security perceptions [21]. Such approach is apprehensible as participants of experiments or surveys had limited knowledge about online security and they could seldom determine what online security features were deployed [35]. Consequently, there is a lack of tool for management to assess OSP thoroughly. The evaluation of FIs' OSPs in Greater China region is important because online financial services are increasingly popular. Concurrently, the online security threats are serious in this region [1]. Our findings can potentially help the FIs or the regulators to decide whether further actions are necessary for improving the OSPs.

Another related question is why FIs have different OSPs. Extant research has focused mainly on positive information technologies (IT) which are designed to benefit users in terms of productivity, efficiency, competitiveness or entertainment [8]. This is understandable as their value can be more easily justified. Technology-Organization-Environment (hereafter TOE) framework [39] was often applied to explain the adoption of innovative technologies which are mostly positive IT [24, 29]. In contrast, the TOE framework was rarely applied to study the adoption of protective IT which aim to guard against security threats. Since the benefits of protective IT are less observable and do not emerge until after a security breach has occurred, the applicability of the TOE framework to study their adoption is questionable. This study attempts to extend the applicability of the TOE framework for explaining the OSPs, which involve the adoption of protective IT and associated policies and procedures.

One final question is whether there is a positive relation between OSPs and information security disclosures. The latter refer to voluntary disclosures (i.e. disclosures beyond what are required by regulations) in the annual report concerning information security, and they are based on the disclosure keywords shown in Table 3. Firms choose to disclose information security practices because they want to provide signals to the capital market that they are adopting necessary measures to protect against security breaches. However, whether those disclosures are credible remains unknown. If information security disclosures are credible, this should be reflected by a firm's OSP. Gordon et al. [15] found a significant and positive relation between firm values and information security disclosures. However, when the study tested the relation by industry, it failed to find such a relation in the financial service industry. The exact reason is not known and it may be due to the violation of the study's key assumption that information security disclosures are credible. Without this assumption, the reasoning that information security disclosures contribute to firm values becomes questionable. This study aims to investigate the validity of this assumption because disclosure credibility is a key research issue [33] and other domain such as

environmental accounting has found mixed results [5]. To our knowledge, this is the first paper that investigates this issue.

This study has two primary objectives. It tests (1) whether the TOE framework could be extended to explain OSPs, and (2) the credibility of information security disclosures. Our findings intend to answer three research questions. First, what are the OSPs of FIs? Second, what are the technological, organizational and environmental factors that affect the OSPs? Third, is there a positive relation between OSPs and information security disclosures? The paper proceeds as follows. In the next two sections, we present our literature review and hypotheses development. They are followed by the research methodology. We then discuss the empirical results and their implications.

LITERATURE REVIEW

Information security disclosures credibility

Disclosure credibility arises because investors typically could not appraise the actual reliability of the information disclosed. Prior studies investigated disclosure credibility from three aspects. The first aspect assessed investors' perceptions of the believability of a particular disclosure. Mercer [33] identified four factors that investors evaluated when assessing disclosure credibility: (1) situational incentives at the time of the disclosure, (2) management's credibility, (3) the levels of external and internal assurance, and (4) disclosure characteristics. Holt [18] investigated the effects of internal audit role and reporting relationships on disclosure credibility using experiment and found that the credibility was higher when the Chief Auditor reported functionally to the audit committee and administratively to the Chief Executive Officer. The second aspect evaluated the disclosure credibility indirectly through investors' reactions (e.g. stock price reaction) or events subsequent to the disclosures. For example, Wang et al. [41] showed that the nature of the disclosed information security risk factors was associated with future breach announcement in the media. It also found that the market reaction following the announcement was different depending on the nature of the preceding disclosure. The third aspect, which is relevant to this study, evaluated the relation between the information disclosures and the performance related to those disclosures. For instance, in environmental accounting research, Clarkson et al. [5] examined this aspect due to prior mixed results on the relationship between corporate environmental performance and the discretionary environmental disclosures. The study developed a content analysis index to assess the extent of discretionary disclosures in environmental and social responsibility reports and found a positive relation to relative environmental performance. These studies, however, have neither investigated the credibility of information security disclosures nor tested its relation to OSPs.

Online security performances

Prior research examined OSPs from two different aspects. One aspect assessed the online security features and information through content analyses of Web sites. For instance, Bose and Chung [2] investigated the anti-phishing preparedness of 36 banks operating in Hong Kong and remarked that the banks needed to improve the accessibility of online information relating to anti-phishing measures. Lim et al. [30] analyzed the differences of online security information of 8 banks from a cultural perspective. They found that Australian banks provided more online security information than the Malaysian banks. Another aspect explored the factors affecting the adoption of certain protective IT. For example, Chang et al. [3] studied the e-signature adoption by hospital and identified four significant factors: hospital size, adequate resources, vendor support and government policy. Lee and Larsen [28] showed that threat and coping appraisal, IT budget and vendor support influenced anti-malware adoption. Laux et al. [35] found that the intention to adopt biometric authentication system was driven by competitive factors, financial resources and perceived benefits. Yeh and Chang [42] found perceived security threats, industry type, organizational readiness and security incidents as factors influencing the organizational diffusion of information systems security. While these studies have provided valuable contributions, they have not measured the OSPs and examined the antecedent factors.

Concerning the framework to explain OSPs, an examination of organizational IT adoption studies [3, 4, 20, 24, 29, 38, 44] revealed that TOE framework is appropriate. TOE framework is used to study the factors affecting organizations' adoption of innovative technologies. Swanson [36] classified information systems innovation into three types: Type I innovations confined to the IS task; Type II innovations supporting administration of the business; and Type III innovations imbedded in the core technology of the business. According to this classification, online security technologies should be a combination of Types II and III innovation as they are embedded in the e-commerce system and are also used to support the administration of the online business.

TOE framework identifies three elements: technological, organizational and environmental contexts that can affect a firm's adoption decision. The technological context relates to the existing or new technologies that are available to a firm. It emphasizes on how the nature and characteristics of the technologies can affect a firm's adoption decision. Perceived importance is one of the technological variables in Chau and Tam [4]'s study of open systems. However, the study found an insignificant relation between perceived importance and adoption. Since the benefits of protective IT are less observable, we are uncertain about management's adoption decision even though it attributes importance to the technologies. The organizational context refers to the impact of internal variables, such as firm size, on adoption decision. The environmental context emphasizes the impact of external variables and existence of government regulation is one of those variables. TOE framework has consistent empirical support in explaining the adoption decisions of positive IT, such as electronic data interchange [24], knowledge management systems [27], open systems [4] and e-business [29, 44]. However, prior research has seldom applied the framework to study the factors affecting the adoption of protective IT.

HYPOTHESES DEVELOPMENT

By applying the TOE framework, this study tests the predictions that a FI's OSP is positively associated with (1) the technological factor: importance of information security as measured by information security disclosures; (2) the organizational factor: firm size; and (3) the environmental factor: existence of government regulation.

Technological factor: Importance of information security

Information security refers to activities that are carried out by a firm to protect its information-related assets. For a firm to take action to improve its information security, it entails managerial vigilance, an appropriate level of awareness about the issue, and an economic analysis that addresses the cost-effectiveness of information security investment. The importance that top management attributes to information security could vary among different organizations because of the differences in the characteristics of top management [14, 19], its assessments of the information assets vulnerability [37], and its IT expenditure budget. Since top management's choice to disclose information voluntarily in the annual report will depend on

its importance [7, 17], information security disclosure was used as a proxy measure for importance that top management attributes to information security.

If top management attributes importance to information security, its FI will likely become superior performer in online security. Naturally, it will try to differentiate itself from inferior performers in order to avoid the adverse selection problem and to improve the FI's valuation [9, 40]. One common method is signaling to the public through the annual report that its FI is actively managing the information security risks. However, top management will put its reputation at stake and risk incurring litigation costs when it makes false disclosures. Thus, it is logical to expect top management's voluntary assertions match the FI's OSP and the adoption of 2FA in particular. Therefore, the following hypotheses are proposed:

H1a & b: The importance that top management attributes to information security, as measured by information security disclosures, will be positively associated with the (a) OSP, and the (b) adoption of 2FA.

Organizational factor: Firm size

Large firms tend to possess slack resources that can facilitate technological innovation adoption [39]. Small firms, on the other hand, suffer from resource poverty due to lack of financial resources, professional expertise and a short range management perspective. Consequently, small firms tend to be slower in technological innovation adoption [38]. Moreover, the substantial scale of operation for a large firm can better absorb the additional investment costs resulting from technological innovation adoption and achieve economies of scale quicker than small firms [44].

By that logic, large FIs have more resources to acquire and implement online security technologies. In case customers do not accept the technologies, large FIs are usually more capable of bearing the failure costs. Furthermore, large FIs have stronger incentives to enhance their corporate reputations or images through stronger online security than do small FIs. Previous studies found that firm size was linked to technological innovation adoption [31, 44]. Therefore, the following two hypotheses are proposed:

H2a & b: Firm size will be positively associated with the (a) OSP, and the (b) adoption of 2FA.

Environmental factor: Existence of government regulation

Government regulation in the form of new operational requirements often stimulates the adoption of new technological innovation [39]. In our study, bank customers sometimes have to conduct high risk online transactions such as fund transfer to third parties and thus they face relatively high risks. Hence, the regulatory bodies have recommended the banks to improve OSPs and adopt 2FA in particular. Banks that want to avoid penalty in case their online security measures fail would likely follow the regulatory bodies' recommendation. In contrast, the regulatory bodies of the other business sectors give no specific requirements to their member firms for improving OSPs. Since only banks have to face the government regulation pertaining to online security, the business type of FIs was used as a proxy measure for the existence of government regulation. Chang et al. [3] found that government regulation was positively associated with technological innovation adoption. Therefore, the following two hypotheses are proposed:

H3a & b: Existence of government regulation, as measured by the business type of FIs, will be positively associated with the (a) OSP, and the (b) adoption of 2FA.

RESEARCH METHODOLOGY

Our initial sample of 178 listed FIs in the Greater China region was obtained from the Datastream database. Seven oversea listed FIs that have dedicated Web sites and login screens for their customers in the region were added in order to make our sample more representative. Our final sample of 115 listed FIs was derived after adding the 7 oversea listed FIs, counting 19 dually listed FIs in the region only once, and discarding 46 and 5 FIs with no online accounts and employee numbers respectively.

Content analysis methodology [23] was used to evaluate the OSPs of the FIs' Web sites in November 2012. This methodology is appropriate because of two reasons. First, because it is based on explicit content, it could avoid the problem of self-reporting bias inherited in survey or interview method. If we request managers to assess their own OSPs, they may overstate the strength in order to avoid giving people an impression that their Web sites are insecure. Second, mangers may be reluctant to talk about their OSPs given the issue is highly sensitive and intrusive [22]. By reviewing online security literature and the guidelines issued by the Federal Financial Institutions Examination Council [11, 12], we have constructed an 18-item scale shown in Table 1 to measure the OSPs.

The first two items assess the highest security level of authentication processes used for login and conducting transaction. The authentication processes mostly use either one or two authentication factors. While knowledge-based and possession-based authentication factors were commonly used, biometric-based authentication factor was not used among our FIs. A scoring scheme shown below items A1 and A2 was used. Items A3-A13 and A15-A18 assess the additional online security measures. Item A14 assesses whether a FI has provided its customers a choice to use different authentication processes.

We measured our scale based on the presence or absence of the online security features or information. To further reduce the subjectivity of assessments, all items were rated by two raters. For items A3 to A18, a score of 1 was assigned if the feature or information was present and 0 otherwise. Each of these 16 items has equal weighting because we believe they are of equal importance. For items A1 and A2, a score of 1 (lowest security) to 5 (highest security) was assigned depending on the presence or absence of certain authentication processes. A score of 3 was assigned if the digital certificate was stored in the same computer device used to access the Web site. Such authentication process is considered as less secure than the one that stores digital certificate in a USB drive or smart card because the certificate can be stolen by malicious software installed in the computer device. Authentication processes have scores of 1-2, 3-4 and 5 if they use one-factor, two-factor and three-factor authentication respectively. There is no score of 0 as every Web site in our sample has certain authentication process. Consequently, the minimum score of our scale is 2 rather than 0, and the maximum score is 26.

Explanatory Variables

Three explanatory variables: firm size (SIZE), government regulation (GR) and importance of information security (IOIS) were used in our research models shown in equation (1).

$$\text{OSP or 2FA} = \alpha + \beta_1 \text{SIZE} + \beta_2 \text{GR} + \beta_3 \text{IOIS} + \beta_4 \text{ROE} + \beta_5 \text{GROWTH} + \varepsilon \quad (1)$$

Table 1. The measurement items of Online Security Performances

No.	Item descriptions	% of FIs
A1	Highest security level of authentication used for login. Score of:	
	1: user-generated password	51.3
	2: user-generated password + second user-generated password	0.9
	3: user-generated password + digital certificate in the same device	0.9
	4: user-generated password + digital certificate in USB / smart card or OTP	46.9
	5: user-generated password + digital certificate in USB / smart card + OTP	0.0
A2	Highest security level of authentication used for transaction. Score of:	
	1: user-generated password	27.8
	2: user-generated password + second user-generated password	7.0
	3: user-generated password + digital certificate in the same device	13.0
	4: user-generated password + digital certificate in USB / smart card or OTP	48.7
	5: user-generated password + digital certificate in USB / smart card + OTP	3.5
A3	Does it monitor online activities to detect fraud?	7.0
A4	Does it disable the account access after a number of incorrect login attempts?	55.6
A5	Does it use secure firewall to prevent unauthorized access to its network?	50.4
A6	Does it use SSL 128-bit or 256-bit encryption to secure information transmission?	65.2
A7	Does it use auto-logoff after a period of idle time?	53.0
A8	Does it use reserved verification information for customer to verify that they have logged in the genuine Web site of the FI?	11.3
A9	Does it use secure connection with a valid site certificate displayed on login screen?	86.9
A10	Does it use additional measures (e.g. soft keypad, dynamic code) to secure the login process?	48.7
A11	Does it notify customers through another communication channel after customers execute online transactions?	38.3
A12	Does it have controls over account activities (e.g. transaction value thresholds, number of transactions allowed per day)?	47.8
A13	Does it notify customers through another communication channel over changes to account maintenance activities performed by customers?	0.9
A14	Does it provide customers a choice to use different authentication processes (e.g. 1 or 2-factor)?	44.3
A15	Does it provide an explanation of protections provided, and not provided, to account holders relative to transactions conducted by unauthorized parties?	60.0
A16	Does it explain under what circumstances and through what means the institution may request the customer's provision of login credentials?	39.1
A17	Does it provide institutional contact information in case customers notice suspicious account activities?	58.3
A18	Does it provide security tips that customers may consider implementing to mitigate their own security risks? *	69.6

* Any of the security tips as stated below

- install latest security updates and patches	- always log off when finished
- use a personal firewall	- disable the 'AutoComplete' function
- block phishing / fraudulent e-mails	- empty your browser's cache
- keep password secure	- ensure the website is genuine (e.g. checking padlock)
- avoid accessing bank account with public computers	- check the account and transaction history details
- disable the "File and Printer Sharing" feature	

Table 2 summarizes all the variables used. Since OSP is a metric variable, multiple regression technique was used. When OSP is replaced by a dichotomous dependent variable: 2FA, logistic regression was applied.

IOIS was indirectly measured by information security disclosures in the annual report. This proxy measure is appropriate because if survey or interview methodology were used, some managers might exaggerate their importance attributes to information security. Thus, it is more sensible to assess IOIS from a customer's or an outsider's perspective [26]. The information security disclosures are based on the 26 security keywords adapted from Gordon et al. [15] and are shown in Table 3. Since some annual reports were written in Chinese, these 26 keywords were translated in Chinese and then back translated to ensure both Chinese and English versions were accurate. Using the advanced search features of the Adobe Acrobat software, the annual reports were searched for those keywords. The three paragraphs near each keyword were examined to determine whether or not the keyword was actually related to information security. A score of 1 was assigned to IOIS if there were one or more of the keywords disclosed and 0 otherwise. The number of occurrences for each of these keywords is shown in Table 3.

Control Variables

We control for variables that may provide some explanations of the two dependent variables beyond the three predictive variables that our hypotheses focus. Profitability was included because profitable FIs might have more resources available to invest in security technologies, making them more likely to have stronger OSPs. It was measured using the return on equity (ROE), which is equal to the net income after taxes divided by the book value of equity, expressed as a percentage. Growth prospect was included as fast growing FIs might outgrow their online security requirements and thus needed more time to make new investments in security technologies. Consequently, their OSPs might lag behind slow growing FIs. Similar to Frankel et al. [13], growth prospect (GROWTH) was measured using the ratio of market capitalization to book value of net assets. The 2012 accounting data for SIZE, ROE and GROWTH were obtained from the Datastream database.

RESULTS

Item A2 in Table 1 indicates that 65.2% of the FIs adopt 2FA (i.e. with score 3 and above) for conducting transactions. Item A14 shows that 44.3% of the FIs offer their customers a choice to use different authentication processes. Table 4 shows that the most popular second authentication factor offered by the FIs is digital certificate stored in a smart card or USB drive.

Panel A of Table 5 indicates that 2FA is mostly adopted by the banks (98%) but not by the insurance/finance firms (0%). Only 43% of the securities trading firms have adopted it. Comparisons of the OSP mean values among the three business sectors reveal that the banking sector ranks highest, with the securities trading and insurance / finance sectors rank the second and third respectively.

Table 2. Variable definitions

Variables	Predicted Sign	Definitions
Dependent variables		
OSP		Online security performance - sum of scores for items A1 to A18 shown in Table 1; scores from 2 to 26
2FA		Two-factor authentication - 1 if a FI adopts it, and 0 otherwise
Explanatory variables		
SIZE	+	Total number of employees
GR	+	1 if the FI is a bank, which has to face the government regulation relating to online security, and 0 otherwise
IOIS	+	1 if top management attributes importance to information security (as measured by information security disclosures in the annual report), and 0 otherwise
Control variables		
ROE	+	Net income after taxes divided by the book value of equity (in percentage)
GROWTH	-	Ratio of market capitalization to book value of net assets

Table 3. List of security keywords and number of occurrences in annual reports

Keywords	Occurrences	Keywords	Occurrences
Information security	166	Security breach	4
Business continuity	35	Access control	4
Security management	24	Denial of service	3
Computer virus	20	Online security	2
Authentication	19	Security measure	2
Encryption	16	Security incident	1
Cyber security	15	Internet fraud	1
Information system security	14	Computer system security	0
Network security	13	Computer security	0
Internet crime	12	Security expenditure	0
Cyber attack	10	Security monitoring	0
Hacker	8	Computer Intrusion	0
Disaster recovery	6	Computer Breach	0

Table 4. Second authentication factors used by the FIs [a]

Sector	Banking				Securities Trading			Insurance / Finance			
Market [b]	CN	HK	TW	Oversea	CN	HK	TW	CN	HK	TW	TOTAL
2nd Authentication Factor [c]											
2nd UGP	4	3	9	0	7	7	1	0	0	0	31
Challenge Q&A	4	0	0	0	1	0	0	0	0	0	5
DC (device)	6	1	9	0	3	0	11	0	0	0	30
DC (smart card/USB)	15	4	24	1	1	0	0	0	0	0	45
OTP (SMS)	14	5	9	4	1	0	0	0	0	0	33
OTP (token)	5	3	2	5	8	0	0	0	0	0	23
OTP (code card)	3	0	0	0	0	0	0	0	0	0	3
OTP (smart card)	1	0	4	1	1	0	0	0	0	0	7

a. Each cell contains the number of FIs that adopt the second authentication factor.
b. CN: Mainland China, HK: Hong Kong, TW: Taiwan
c. UGP: User generated password, DC: Digital certificate, OTP: One-time password

Panel B of Table 5 breaks down the OSP mean values by business sectors and by markets. It shows that within the same business sector and across different markets, the OSP mean values are quite similar. Table 6 presents the descriptive statistics for the key variables. The OSP value ranges from 2 to 24, with the mean (median) value equals to 12.7 (13.0).

Instrument Reliability and Validity

Content analysis is a research method for making replicable and valid inferences from texts (or other data) to their context [23, p.24]. To assess the reliability of our OSP scale, the replicability, which is also called inter-rater reliability [23, p.271], was tested. Inter-rater reliability of our two raters was calculated as the percentage of agreement for each of the 18 items. Our result ranges from 70% to 96% (not shown), which indicates a good to excellent level of inter-rater reliability. Coding disagreements were resolved by discussions and through re-examination of the features or information in question. Cronbach's alpha, another measure of reliability which assesses the internal consistency among the items in our scale, was 0.91. This value is well above the minimum threshold of 0.6 for acceptable reliability. Validity of our OSP scale was assessed through face validity, which was commonly used by content analysts [23, p.330]. Face validity was addressed by involving more than one researcher in developing the scale [30].

To assess the multicollinearity problem, Table 7 presents the correlation matrix between the explanatory and control variables. The variables with the highest correlation are GROWTH and ROE (ϱ = -0.586) and none of them exhibit pair-wise correlations over 60 percent. An alternative checking using the variance inflation factor (VIF) indicates that all five variables do not have VIF values exceeding 1.7, which is well below the threshold value of 10. Hence, multicollinearity does not present a serious concern in our regression analyses.

To ensure the adequacy of our sample size, statistical power analysis and ratio of observations to predictive variables tests were conducted. For 5 predictive variables, a power analysis using the software G*Power 3.1 [10] showed that a sample size of 92 is required to detect a medium effect size of 0.15 [6] at a significant level of 0.05 with a power of 0.8. Hence, our sample size of 115 FIs is adequate for detecting a statistically significant R^2. For the ratio of observations to predictive variables, the desired ratio is from 15 to 20 [16]. Our sample size of 115 FIs and five predictive variables result in a ratio of 23, which is better than the desired ratio.

Results of Regression Analyses

As shown in Panel A of Table 8, hypotheses 1a, 2a, and 3a are supported. For the two control variables: ROE and GROWTH, none of them have significant effects on OSPs. The results also indicate that the predictive variables explain a substantial amount of variance in OSPs, with adjusted R^2 equals to 85%. The F-statistic equals to 132.6 and is significant at the 1% level, which indicates that the proposed model has significant predictive capability.

As shown in Panel B, hypotheses 1b and 3b are supported as variables IOIS and GR are significant at the 1% level. Hypothesis 2b is not supported as SIZE is insignificant. Both control

Table 5. Descriptive statistics for OSPs[a]

Panel A: OSPs by business sectors				
	Overall	Banking	Securities Trading	Insurance/Finance
Mean	12.7	19.4	6.8	4.8
Median	13.0	20.0	6.0	4.0
St. Dev.	7.2	2.4	3.4	2.4
Min.	2	12	2	2
Max.	24	24	15	11
N	115	56	46	13
2FA adoption %	65%	98%	43%	0%

Panel B: OSPs by business sectors and by markets

	Banking				Securities Trading			Insurance/ Finance		
	CN	HK	TW	Oversea	CN	HK	TW	CN	HK	TW
Mean	20.6	18.1	18.9	20.1	8.1	5.4	7.0	3.7	5.4	4.3
Median	21.0	20.0	19.0	20.0	8.0	4.0	6.0	4.0	5.0	4.0
SD	3.2	3.3	1.0	1.3	4.2	2.7	2.4	0.6	3.1	0.5
Min.	13	12	17	18	2	2	4	3	2	4
Max.	24	22	21	22	15	11	11	4	11	5
N	16	9	24	7	18	17	11	3	7	3

CN: Mainland China, HK: Hong Kong, TW: Taiwan

Table 6. Descriptive statistics for the key variables [a]

Variables	Mean	Median	Std. Dev.	Min.	Max.
Dependent variables					
OSP	12.7	13.0	7.2	2	24
2FA	0.65	1	0.48	0	1
Explanatory variables					
SIZE	33,890	4,747	82,731	25	461,100
GR	0.49	0	0.50	0	1
IOIS	0.48	0	0.50	0	1
Control variables					
ROE (%)	5.43	6.95	19.58	- 166.56	23.03
GROWTH	1.44	1.09	1.28	0.08	10.55

a. See Table 2 for variable definitions.

Table 7. Correlation matrix for the explanatory and control variables

Variables	Descriptions	1	2	3	4	5
1. SIZE	Firm Size	1.000				
2. GR	Government Regulation	**0.319**	1.000			
3. IOIS	Importance of Info. Security	**0.250**	**0.584**	1.000		
4. ROE	Return on Equity	0.178	**0.330**	**0.266**	1.000	
5. GROWTH	Growth	-0.053	**-0.253**	-0.101	**-0.586**	1.000

The number is Pearson correlation coefficient. Statistically significant correlations are shown in bold.

variables ROE and GROWTH have insignificant effects on 2FA. Nagelkerke R^2 is 64%, which indicates that 64% of the variance in 2FA can be explained by the predictive variables. Nagelkerke R^2 is preferred because it is a modification over the Cox and Snell R^2 and it has a range of 0 to 1 like the R^2 in multiple regression analysis.

Hosmer and Lemeshow test was used to evaluate the overall model fit. An insignificant value of 0.97 indicates the model fit is acceptable as there is insignificant difference between the observed and predicted classifications. The classification accuracy was also examined to evaluate the overall model fit. Among the 115 FIs, there are 75 adopters and 40 non-adopters of 2FA. As Panel B shows, the logistic regression model achieves a classification accuracy of 84.3% ((34+63)/115), which is much better than the accuracy of 65.2% (75/115) when only constant or intercept is included in the logistic regression model.

DISCUSSIONS

Motivated by the need to test (1) whether the TOE framework can be extended to explain OSPs and, (2) the credibility of information security disclosures, this study addresses the following three research questions.

What are the online security performances of FIs?

Our results indicate that 98% of the banks in our sample have adopted 2FA whereas only 43% of the securities trading firms have adopted it. Our findings are quite different from Mao et al. [32]'s claim that password is the single factor of authentication for accessing online accounts. Although the second authentication factor: digital certificate stored in a USB drive or smart card is most common, many of the FIs have also offered alternative authentication factors such as one-time password sent to a mobile phone. This reflects the FIs' effort to meet different customers' preferences for security, usability and convenience. Our findings also show that OSPs are similar within the same business sector and across different markets. This indicates that FIs will make reference to their competitors in determining levels of OSPs.

What are the technological, organizational and environmental factors that affect the online security performances?

The technological variable: IOIS has positive effects on both OSPs and 2FA. This implies that when top management attributes importance to information security, its FI will have strong OSP and adopt 2FA. Our results show that even though the benefits of online security technologies are less observable, top management will still make the investment if it attributes importance to the protective IT.

The significant positive effect of the organizational variable: SIZE on OSPs implies that larger FIs have more resources to acquire security technologies. Also, larger FIs have broader revenue bases to absorb the associated investment costs. Our result supports previous findings [31, 44] that firm size was one of the determinants of technological innovation adoption. However, SIZE has no significant effect on 2FA. One plausible explanation for the insignificant effect might be due to the high adoption rate of 2FA among the FIs in the region. In other words, even small FIs can afford the authentication technology nowadays.

GR, the environmental variable, has positive and significant effects on both OSPs and 2FA. For FIs to avoid penalty if their online security measures fail, they have to comply with the government regulation. Judging from the t and Wald statistics in Table 8, GR is the strongest variable among the three explanatory variables. This implies that government regulation has the strongest influence on OSPs and the adoption of 2FA. Our result is consistent with Chang et al. [3]'s study which found that government policy was positively associated with technological

Table 8. Results of the Regression Analyses

Panel A: Multiple Regression using OSP as the dependent variable

	Predicted Sign	Coefficient	t Statistic	Significance [a]	Hypothesis
Constant		6.090	10.716	0.000***	
IOIS	+	1.904	2.957	0.004***	H1a supported
SIZE	+	0.000	1.834	0.069*	H2a supported
GR	+	11.285	16.818	0.000***	H3a supported
ROE	+	0.021	1.206	0.230	
GROWTH	-	-0.116	-0.456	0.649	
Model Summary:		Adjusted R2:	0.85	F-Statistic:	132.6***

Panel B: Logistic Regression using 2FA as the dependent variable

	Predicted Sign	Coefficient	Wald Statistic	Significance	Hypothesis
Constant		-0.549	1.215	0.241	
IOIS	+	1.700	6.602	0.010***	H1b supported
SIZE	+	0.000	0.202	0.653	H2b not supported
GR	+	3.975	10.546	0.001***	H3b supported
ROE	+	0.007	0.081	0.773	
GROWTH	-	-0.348	1.606	0.270	

Observed	Predicted		% Correct
	Non-Adopter FIs	Adopter FIs	
Non-Adopter	34	6	85.0
Adopter	12	63	84.0
Overall			84.3

Model Summary:
–2 log likelihood (-2LL) = 76.71
Chi-Square test for Δ (-2LL); significant = 0.000
Hosmer and Lemeshow test $\chi 2$=2.37; significant = 0.97
Cox & Snell R2 = 0.47 Nagelkerke R2 = 0.64

a. ***, **, and * indicate significance at the 1%, 5% and 10% levels (2-tailed test) respectively.

innovation adoption.

Is there a positive relation between online security performances and information security disclosures?

Voluntary disclosures of information security were used as a proxy measure for IOIS. Thus, the significant and positive relation between OSPs and IOIS indicates that online security performances and information security disclosures are positively related. This provides support to Gordon et al. [15]'s assumption that information security disclosures are credible, thus precluding the possibility of invalid assumption that caused the insignificant relation between disclosures and firm values among the FIs in their study. The truthful disclosures show that top management is mindful about its reputation and the potential litigations raised by the investors and thus it chooses to be credible in this issue. These findings also support the signaling argument proposed in the voluntary disclosure theory [9, 40], which states that in order to avoid the adverse selection problem and improve company valuation, superior performers want to differentiate themselves from inferior performers via voluntary disclosures in the annual reports.

CONCLUSIONS

This study provides insights into the OSPs of FIs in the Greater China region. Five of the six hypotheses are supported and our research models have substantial predictive capability, with R^2 range from 64% to 85%. Existence of government regulation is the most significant factor. Our results show that the TOE framework could be extended to study the OSPs. And by finding a significant and positive relation between OSPs and information security disclosures, this study shows that voluntary disclosures of information security in the annual reports are credible.

Implications for research

Our study makes three contributions to the literature. First, the 18-item scale serves as a benchmark for the evaluation of OSPs. Unlike prior studies that relied on the managerial assessments of information security which usually suffered from self-reporting bias, this study proposes a tool to evaluate OSPs from an outsider's perspective. This approach is appropriate given the customer-oriented nature of the e-commerce systems, which implies customers' assessments of online security are also necessary. Second, since management disclosure credibility is a major research issue [33] and other study has found mixed results [5], our findings provide evidence to support the assertion that information security disclosures are credible. Third, unlike positive IT, the benefits of protective IT are less observable, and the TOE framework has seldom applied to study protective IT in the past. Thus, our significant findings further extend the applicability of the TOE framework.

Implications for practices

Prior research has suggested that when people use online services, they cannot identify the security measures deployed on the Web sites [35]. Our scale can allow users to gauge the OSPs of their service providers. In addition, it provides guidelines for managers to evaluate their OSPs and the outcomes could assist their security technologies investment decisions. The scale can also remind managers to post the information online if they have adopted any security measures because such transparency may gain their customers' confidence in using the online financial services [43]. Our findings also provide regulators with information on the OSPs of FIs. Security concerns have frequently been cited as obstacles in using online financial services. Regulators could assess whether there are adequate guidelines to help the FIs to improve their OSPs. Furthermore, security technologies vendors and consultants can use our results to focus their sales and marketing effort on FIs that are likely to purchase their products or services in the future.

LIMITATIONS AND FUTURE RESEARCH

Our research has several limitations. First, our research sample only contains firms from a single industry – financial services. To improve the result generalizations, future research could include firms from other industries. Second, the FIs in our sample are mainly conducting business in the Greater China region. Future research could compare the OSPs of firms from different countries or regions. Third, the contents of Web sites are dynamic, and our data collection only happens at a particular point in time. Fourth, our 18-item scale may not be comprehensive, as they were developed based on the security information and

features available on the Web sites. It is possible that some FIs have implemented security measures but they have not disclosed them on their Web sites. Fifth, future research could examine the managers' incentives to disclose information security voluntarily in the annual reports.

ACKNOWLEDGEMENT

This study was supported by a Departmental General Research Fund (Project No. 4-ZZB2) from The Hong Kong Polytechnic University.

REFERENCES

[1] APWG, "Global Phishing Survey: Trends and Domain Name Use 1H2012", available at: http://docs.apwg.org/reports/APWG_GlobalPhishingSurvey_1H2012.pdf, 2012 (accessed 18 March 2013).

[2] Bose, I., and Chung, A., "Assessing anti-phishing preparedness: A study of online banks in Hong Kong", Decision Support Systems (45:4), 2008, pp. 897–912.

[3] Chang, I.-C., Hwang, H.-G., Hung, M.-C., Lin, M.-H. and Yen, D.C., "Factors affecting the adoption of electronic signature: Executives' perspective of hospital information department", Decision Support Systems (44:1), 2007, pp. 350–359.

[4] Chau, P. Y. K., and Tam, K. Y., "Factors affecting the adoption of open systems: An exploratory study", MIS Quarterly (21:1), 1997, pp. 1–21.

[5] Clarkson, M. P., Li, Y., Richardson, D. G. and Vasvari, P. F., "Revisiting the relation between environmental performance and environmental disclosure: An empirical analysis", Accounting, Organizations and Society (22), 2008, pp. 303-327.

[6] Cohen, J., Statistical Power Analysis for the Behavioral Sciences, 2nd ed. Lawrence Erlbaum, Hillsdale, NJ, 1988, pp. 26.

[7] Criado-Jimenez, I., Fernandez-Chulian, M., Husillos-Carques, F. J. and Larrinaga-Gonzalez, C., "Compliance with Mandatory Environmental Reporting in Financial Statements: The Case of Spain (2001–2003)", Journal of Business Ethics (79:3), 2008, pp. 245–262.

[8] Dinev, T. and Hu, Q., "The centrality of awareness in the formation of user behavioral intention toward protective information technologies", Journal of the Association for Information Systems (8:7), 2007, pp. 386-408.

[9] Dye, R.A., "Disclosure of Nonproprietary Information", Journal of Accounting Research (23:1), 1985, pp. 123-145.

[10] Faul, F., Erdfelder, E., Buchner, A. and Lang, A. G., "Statistical power analyses using G*Power 3.1: Tests for correlation and regression analyses", Behavior Research Methods (41), 2009, pp. 1149-1160.

[11] FFIEC, "Authentication in an Internet Banking Environment", available at: http://www.ffiec.gov/pdf/ authentication_guidance.pdf, 2005 (accessed 10 September 2012).

[12] FFIEC, "Supplement to Authentication in an Internet Banking Environment", available at: http:// www.ffiec.gov/pdf/Auth-ITS-Final%206-22-11%20(FFIEC%20Formated).pdf, 2011 (accessed 10 September 2012).

[13] Frankel, R., Johnson, M., Skinner, D. J., "An empirical examination of conference calls as a voluntary disclosure medium", Journal of Accounting Research (37:1), 1999, pp. 133–150.

[14] Goodhue, D. L. and Straub, D., "Security concerns of system users: A study of perceptions of the adequacy of security measures", Information & Management (20:1), 1991, pp. 13–27.

[15] Gordon, L.A., Loeb, M. P. and Sohail, T., "Market value of voluntary disclosures concerning information security", MIS Quarterly (34:3), 2010, pp. 567-594.

[16] Hair, J. F., Black, W. C., Babin, B. J., Anderson, R. L., Multivariate Data Analysis with Readings, Prentice Hall, Englewood Cliffs, NJ, 2010, pp. 661.

[17] Hasnah, H., Dato, D. N. I., Jeyaraman, K. and Ong, H. C., "Determinants of internal control characteristics influencing voluntary and mandatory disclosures: A Malaysian perspective", Managerial Auditing Journal (25:2), 2010, pp. 140-159.

[18] Holt, P. T., "The effects of internal audit role and reporting relationships on investor perceptions of disclosure credibility", Managerial Auditing Journal (27:9), 2012, pp. 878-898.

[19] Hsu, C., Lee, J.-N. and Straub, D. W., "Institutional Influences on IS Security Innovations", Information Systems Research (23:3), 2012, pp. 918–939.

[20] Jeyaraj, A., Rottman, J. and Lacity, M., "A review of the predictors, linkages, and biases in IT innovation adoption research", Journal of Information Technology (21), 2006, pp. 1–23.

[21] Kim, C., Tao, W., Shin, N., Kim, K.-S., "An empirical study of customers' perceptions of security and trust in e-payment systems", Electronic Commerce Research and Applications (9:1), 2010, pp. 84-95.

[22] Kotulic, A. G., and Clark, J. G., "Why there aren't more information security research studies", Information & Management (41:5), 2004, pp. 597–607.

[23] Krippendorff, K., Content analysis: An introduction to its methodology, Sage Publications, Thousand Oaks, CA, 2013.

[24] Kuan, K. Y. K. and Chau, P. Y. K., "A perception-based model for EDI adoption in small businesses using a technology-organization-environment framework", Information and Management (38:8), 2001, pp. 507-521.

[25] Laux, D., Luse, A., Mennecke, B. and Townsend, A. M., "Adoption of biometric authentication systems: Implications for research and practice in the deployment of end-user security systems", Journal of Organizational Computing and Electronic Commerce (21:3), 2011, pp. 221-245.

[26] Lee, S., and Ahn, H., "The organizational contexts, controls and implementation of e-business", The Journal of Computer Information Systems (51:1), 2010, pp.114-124.

[27] Lee, O. K., Wang, M., Lim, K. H. and Peng, Z., "Knowledge Management Systems Diffusion in Chinese Enterprises: A Multistage Approach Using the Technology-Organization-Environment Framework", Journal of Global Information Management (17:1), 2009, pp. 70-84.

[28] Lee, Y. and Larsen K.R., "Threat or coping appraisal: determinants of SMB executives' decision to adopt anti-malware software", European Journal of Information Systems (18), 2009, pp. 177–187.

[29] Li, D., Lai, F. and Wang, J., "E-Business Assimilation in China's International Trade Firms: The Technology-Organization-Environment Framework", Journal of Global Information Management (18:1), 2010, pp. 39-65.

[30] Lim, N., Yeow, P. H. P. and Yuen, Y. Y., "An Online Banking Security Framework and a Cross-Cultural Comparison", Journal of Global Information Technology Management (13:3), 2010, pp. 39-62.

[31] Low, C., Chen, Y. and Wu, M., "Understanding the determinants of cloud computing adoption", Industrial Management and Data Systems (111:7), 2011, pp. 1006-1023.

[32] Mao, Z., Florencio, D. and Herley, C., Painless migration from passwords to two-factor authentication. Retrieved from http://research.microsoft.com/apps/pubs/default.

aspx?id=155648, 2011 (Accessed 25 August, 2012)
[33] Mercer M., "How do investors assess the credibility of management disclosures", Accounting Horizons (18:3), 2004, pp. 185-196.
[34] Network World, "Banks: Hackers more aggressive in attacking customer accounts", available at: http://www.networkworld.com/news/2012/061412-banks-hackers-260208.html, 2012 (accessed 25 March 2013).
[35] Ray, S., Ow, T. and Kim, S. S., "Security assurance: How online service providers can influence security control perceptions and gain trust", Decision Science (42:2), 2011, pp. 391-412.
[36] Swanson, E.B., "Information systems innovation among organizations", Management Science (40:9), 1994, pp. 1069–1092.
[37] Tanaka, H., Matsuura, K. and Sudoh, O., "Vulnerability and information security investment: An empirical analysis of e-local government in Japan", Journal of Accounting and Public Policy (24:1), 2005, pp. 37–59.
[38] Thong, J. Y. L., "An integrated model of information systems adoption in small businesses", Journal of Management Information Systems (15:44), 1999, pp. 187- 214.
[39] Tornatzky, L. G. and Fleischer, M., The processes of technological innovation, Lexington Books, Lexington, MA, 1990, pp. 161-174.
[40] Verrecchia, R.E., "Discretionary disclosure", Journal of Accounting and Economics (5), 1983, pp. 179-194.
[41] Wang, T., Kannan, N. K. and Ulmer, R. J., "The association between the disclosure and the realization of information security risk factors", Information Systems Research (24:2), 2013, pp. 201-218.
[42] Yeh, Q.-J., and Chang, A. J.-T., "Technology-push and need-pull roles in information system security diffusion", International Journal of Technology Management (54:2/3), 2011, pp.321-343.
[43] Yuen, Y.Y., Yeow, H.P. P., Lim, N. and Saylani, N., "Internet banking adoption: Comparing developed and developing countries", The Journal of Computer Information Systems (51:1), 2010, pp. 52-61.
[44] Zhu, K., Kraemer, K. L. 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, pp. 251-268.