Communications of the Association for Information Systems

Volume 37 Article 25

9-2015

Developing a Typological Theory Using a Quantitative Approach: A Case of Information Security Deviant Behavior

Amanda M. Y. Chu
Department of Mathematics and Statistics, Hang Seng Management College

Patrick Y. K. Chau
Faculty of Business and Economics, The University of Hong Kong, pchau@business.hku.hk

Mike K. P. So
School of Business and Management, The Hong Kong University of Science and Technology

Communications of the Association for Information Systems

Research Paper ISSN: 1529-3181

Developing a Typological Theory Using a Quantitative Approach: A Case of Information Security Deviant Behavior

Amanda M. Y. Chu
Department of Mathematics and Statistics, Hang Seng Management College, Shatin, Hong Kong

Patrick Y. K. Chau
Faculty of Business and Economics, The University of Hong Kong, Pokfulam Road, Hong Kong
pchau@business.hku.hk

Mike K. P. So
School of Business and Management, The Hong Kong University of Science and Technology, Clear Water Bay, Hong Kong

Abstract:

Different from classification and taxonomy, typology meets the criteria of a theory and is a unique form of theory building. Typology is a good first step in exploring a research topic, and, therefore, we are concerned with building typological theories for underdeveloped topics with limited studies. We propose a four-step approach involving content analysis, multidimensional scaling, judgmental analysis, and empirical testing to guide researchers in developing typological theories in their domains of interest using a quantitative approach that rides on empirical methods and industry wisdom. Previous research in information security has paid little attention to employees' deviant behavior in the workplace. We, therefore, built a typology of information security deviant behavior as an example to illustrate the theory development process. We discuss the theoretical, methodological, and practical implications of this study.

Keywords: Information Security, Deviant Behavior, Typological Theory, Theory Building, Multidimensional Scaling.

The manuscript was received 07/07/2014 and was with the authors 4 months for 2 revisions.

1 Introduction

Typology has been a popular approach in management and social sciences to understand organizational phenomena (Doty & Glick, 1994) and is useful for providing an explanatory framework for discussion and for formulating hypotheses (Clinard, Quinney, & Wildeman, 1994). However, it has not been broadly developed in the information systems area (Nevo, Nevo, & Ein-Dor, 2010). Guillemette and Paré (2012) have proposed a new typological theory of the IT function's contribution in organizations. However, as Guillemette and Paré (2012) emphasize, they used a qualitative approach that depends heavily on literature to establish the typology, and such a methodology may not be useful for exploring underdeveloped topics in the literature. Therefore, we need to develop a quantitative approach that develops a fully specified typology based on empirical methods in a systematic manner. With this study, we present just such an attempt. We present how a typological theory can be built for a relatively underdeveloped topic in information security—employees' information security deviant behavior (ISDB) in organizations (e.g., writing down passwords and installing untrusted applications). We chose to study ISDB because it is an important but underdeveloped topic. Twenty years ago, Loch, Carr, and Warkentin (1992, p. 184) commented that "employees and internal organizational procedures are a greater threat than competitors" and in more recent times, Hu, Xu, Diney, & Ling (2011, p. 54) emphasize that "human agents are still the weakest link in the defense against outside attacks and the most dangerous to the organizations from within". However, scholars have found prior research work in this area to be insufficient (Siponen, Willison, & Baskerville, 2008), and the concept of information security deviance is still unclear (Willison & Siponen, 2009). Typology is a good first step in exploring a behavior because it provides a clearer picture of what a behavior is and how its variants are interrelated. Our quantitative approach shows how it does.

This paper has several useful implications for both researchers and managers. Theory development is crucial to the growth of information systems research and IS scholars encourage researchers to build new theories in information systems research topics (Gregor, 2006; Weber, 2012). The typology developed in this paper meets the criteria for being a theory (Doty & Glick 1994). In terms of theoretical contributions, we demonstrate how a typological theory can be built for a relatively underdeveloped topic and how the typology developed forms a basis for further theoretical work. It is a useful starting point for developing an organized and theoretical framework for systematic research on ISDB and a critical starting point for deriving measures of the deviance. Regarding practical significance, with our findings, managers can understand different forms of ISDB, their relationships, and their impacts on organizations. In terms of methodological contributions, we use MDS, together with some statistical analysis methods, to develop the typological theory. MDS itself depends solely on data and is usually used to develop inductive and empirically derived models. However, we use it to develop a typological theory that may provide another approach for theory building. The proposed procedure for developing a typology is useful for exploring a behavior with infinite forms such as ISDB.

We structure the paper as follows: in Section 2, we review the criteria for a typological theory. In Section 3, we discuss why a typology is needed for ISDB. In Section 4, we describe in detail the quantitative approach for developing a typological theory of ISDB. In Section 5, we discuss the implications of the findings and directions for future research. Finally, in Section 6, we conclude the paper.

2 Typological Theory

Many researchers view typology as classification or taxonomy and use these three terms interchangeably (e.g., Campbell & Lu, 2007; Earl, 2001; Heo & Han, 2003). Doty and Glick (1994), however, argue that typology is different from classification and taxonomy because typology is a unique form of theory building and that classification and taxonomy are not. Guilllemette and Paré (2012) discuss this point in detail but they do not mention the criteria for being a typological theory. Doty and Glick (1994, p. 233) propose that, for a typology to be a theory, it must fulfill three primary criteria: "a) constructs must be identified", "b) relationships among these constructs must be specified", and "c) these relationships must be falsifiable". Based on these three criteria, many existing typologies are then not typologies but classification systems. In addition to the above three primary criteria, many researchers have addressed the need to set boundaries when building a theory and stated that all theories are constrained by their specific bounding assumptions because the implicit values of the theorist and explicit limitations of the theory are embedded

in the assumptions (Bacharach, 1989; Dubin, 1978; Weber, 2012). Therefore, besides the three primary criteria, we should take the notion of boundaries into consideration when developing a typology.

3 Information Security Deviant Behavior

3.1 Lack of Studies in Information Security Deviant Behavior

Previous information security research is dominated by the subject's technical, management, and policy aspects and seldom studies information security behavior (Chu, Chau, & So, Forthcoming; von Solms, 2000, 2006; Zafar & Clark, 2009). Siponen et al. (2008) conducted an in-depth review of literature published between 1990 and 2004 on information security and found that only 1.17 percent (15 out of 1,280 papers) studied information security behavior. Even when information security behavior was studied, most studies focused on positive forms of behavior such as employees' adoption of security measures (e.g., Hu & Dinev, 2005; Lee & Kozar, 2008; Lee & Larsen, 2009) or their protective behavior on information security (e.g., Hu, Diney, Hart, & Cooke, 2012; Posey, Roberts, Lowry, Bennett, & Courtney, 2013). Although these studies shed light on how employees protect their computers from being hacked or attacked and the findings help managers to create better awareness programs to increase the organizational information security level, a more proactive way to protect organizational information security is to avert employees from being threats to their organizations (Fenz, Ekelhart, & Neubauer, 2011), and, thus, the need to understand ISDB demands greater research emphasis (Choobineh, Dhillon, Grimaila, & Rees, 2007; Chu & Chau, 2014; Mahmood, Siponen, Straub, & Rao, 2010; Willison & Warkentin, 2013). However, to date, we still poorly understand the information security deviance of employees in the workplace (Willison & Siponen, 2009). Few attempts have been made to organize the behavior. Campbell and Lu (2007) classify information technology abuse. The authors divide information technology abuse into four types—nonproductive use, negligent use, counterproductive use, and corrupt use. However, the classification was mainly based on subjective arguments. Stanton, Stan, Mastrangelo, & Jolton (2005) use an empirical approach to analyze positive forms of end user security-related behavior and refer to constructive deviance that results in organizational benefits and negative forms of end user security-related behavior, which represents destructive deviance that leads to organizational harm. After collecting opinions on the security behavior from 110 interviewees, the authors developed a six-element taxonomy of the behavior. The six elements were intentional destruction, detrimental misuse, dangerous tinkering, naïve mistakes, aware assurance, and basic hygiene. The classification provides some insights on the different types of positive and negative security behavior. However, we still do not know the relationships among the types of the behavior or how the classification is operationalized. To explore this topic, we need to develop a typology of ISDB and understand how different types of the behavior are interrelated and organized.

The literature covers various topics in information security deviance such as password behavior (Hoonakker, Bornoe, & Carayon, 2009), information systems misuse (D'Arcy & Hovav, 2007a, 2007b; D'Arcy, Hovav, & Galletta, 2009; Hovav & D'Arcy 2012), and Internet abuse (Schechtman, Marett, & Wells, 2006), but previous studies have seldom showed the interrelationships among different forms of the deviance. A shortcoming of some previous studies is that they do not adequately define the behaviors they describe because relatively little is known about broadening the range of deviant behavior in information security over time and an organizing framework for the behavior is unavailable. Therefore, we need to understand and clarify the deviant behavior in information security, which we do in this paper. As such, our three research questions are: 1) what is ISDB?; 2) what are the set of "ideal types" of the behavior, each of which shows unique characteristics of organizations and can be described by a construct?; and 3) how are different types of the behavior interrelated and organized? Accordingly, we provide a systematic and methodological process to define and describe ISDB. We develop a typology of the behavior to provide a theoretical framework for describing the similarities and differences among the types of the behavior and help researchers and managers to better understand the many variants of the behavior. We integrate knowledge from the literature with industry wisdom to develop a typology of ISDB.

3.2 Defining Information Security Deviant Behavior

We identified studies on negative forms of information security behavior in organizations based on Webster and Watson's (2002) paper-identification methodology (which includes searching: 1) journal databases, 2) the citations of identified papers, and 3) the social sciences citation index and the Web of Science) that many researchers such as Melville, Kraemer, and Gurbaxani (2004) and Brown and Grant

(2005) have adopted. We used the key words “information security”, “behavior/behaviour”, and “organization/organisation”. Appendix A lists the different types of negative forms of information security behavior studied in the past. We found that the nature of the negative forms of information security behavior discussed varies a lot and the perpetrators differ. For example, computer abuse could be in the form of misuse, theft, hacking, attacking, or intrusion committed by external hackers, while omissive behavior is exhibited by employees who forget to implement the necessary measures. Computer abuse and omissive behavior are, to a certain extent, mutually exclusive. We explore employees’ deviant behavior in information security in organizations to understand which specific acts of employees violate information security norms We need a study on ISDB to explain this organizational phenomenon and to help organize the interrelationships among the various types of the deviance.

Some previous works have attempted to examine specific forms of deviant workplace behavior in information security such as non-work-related computing. Pee, Woon, and Kankanhali (2008) refers to non-work-related computing as employees’ usage of the Internet or information systems resources for personal purposes in the workplace. This and other such studies offer us some constructive insights on why employees spend time on non-work-related computing and the influence of this unwanted usage on job performance. However, some researchers (e.g., Belanger & Slyke, 2002; Oravec, 2002) suggest that allowing employees to use the Internet for non-work-related activities in a supervised manner could make them more creative and productive. In other words, non-work-related computing may be beneficial to organizations if it is properly supervised. Hence, under the definition that Pee et al. (2008) provide, non-work-related computing may not be directly considered as information security deviance. Therefore, we need to define clearly what ISDB is and how different types of the behavior are organized. Without clearly defining the behavior and knowing the interrelationships of different types of it, further investigations may be difficult. This could be the very reason why only isolated research efforts on information security deviance have been made in the past.

We define ISDB here as the voluntary behavior of employees in organizations that differs markedly from the organizations’ information security norms and that other employees normally consider to be inappropriate behavior in organizations. We use “deviant” (i.e., in information security deviant behavior) because the behavior we primarily consider in this study violates information security norms in organizations but is usually not regarded as criminal behavior, which is best defined and assessed by a legal system (Griffin & Lopez, 2005). We compared different definitions of information security from previous studies and adopted Whitman and Mattord’s (2004, p. 4) definition—“the protection of information and its critical elements, including the systems and hardware that use, store, and transmit that information”—because their definition includes the protection of systems and hardware and is not restricted to the disclosure of information. We explore employees’ ISDB by developing a typology for the behavior. We exclude any behavior resulting from accidents (e.g., accidental entry of incorrect data), external factors (e.g., outsider hackers), or incidents not involving humans (e.g., electrical power failures) that influence the levels of information security of organizations from the current study.

4 A Quantitative Approach for Developing a Typology

Table 1 shows a table of the sequence of research methodologies one can use to develop a typology. The first column of Table 1 describes the four important criteria that a theory should meet (the setting of boundaries that Bacharach (1989), Dubin (1978), and Weber (2012) propose, plus the three criteria that Doty and Glick (1994) suggest). We summarize the research methodologies and techniques used in Guilllemette and Paré (2012) to meet the four criteria for building a typology of IT function in organizations in columns 2 and 3. The authors depended on intensively reviewing the literature to establish the typology. We propose a quantitative approach of developing a typology that involves four key steps: content analysis, multidimensional scaling (MDS) (Kruskal & Wish, 1978), judgmental analysis, and empirical testing, which correspond to the four criteria in columns 4 and 5. The advantage of our quantitative approach is that we integrate knowledge with industry wisdom to develop a typology of ISDB. That is, instead of using our collective judgment on the literature, we conducted surveys to collect industry opinions. As Chiasson and Davidson (2005, p. 591) state: “Industry provides an important contextual ‘space’ to build new IS theory and to evaluate the boundaries of existing IS theory”. We follow the four steps to illustrate how one can develop a typology of ISDB that meets the four criteria.

Table 1. Procedure for Developing a Typology

Steps for building typology	Qualitative method *(expanding the understanding on well-developed topics)*		Quantitative method *(exploring underdeveloped topics)*	
	Research methodologies	**Techniques**	**Research methodologies**	**Techniques**
Setting boundaries	Content analysis	Literature	Content analysis	Survey *(*Survey I) Expert opinions
Identifying constructs	Authors' collective judgment	Literature	Multidimensional scaling	Survey *(*Survey II)
Specifying relationship among the constructs	Authors' collective judgment	Literature	Judgmental analysis	Survey *(*Survey III)
Testing the relationships	Pattern matching analysis	Executive interviews	Empirical testing	Survey *(*Survey IV*)*

In step 1 (content analysis), we set the bounding assumptions for developing theory. We conducted a survey (Survey I) to compile a list of typical descriptions in ISDB based on definitions and assumptions. In step 2 (MDS), we identified the constructs for the typology. We conducted another survey (Survey II) and used MDS to develop dimensions for describing ISDB. We derived ideal types of ISDB and a typology based on the MDS findings. In step 3 (judgmental analysis), we interpreted the dimensions. We carried out a third survey (Survey III) to determine the best attributes for describing the identified dimensions of the typology and specifying the relationships among different types of ISDB. Kruskal and Wish (1978) suggest this step for interpreting dimensions. In step 4 (empirical testing), we demonstrated the falsifiability of the typology. We conducted a fourth survey (Survey IV) to collect opinions from IT professionals to validate the interaction of the constructs in the typology. Appendix B summarizes a profile of the samples in Surveys I, II, III, and IV.

4.1 Step 1: Content Analysis

We conducted Survey I to generate a list of typical and representative descriptions in ISDB for research. We approached five non-profit making organizations that organized various business activities and seminars for employees in various positions and from various industries to attend and obtained their permission to distribute questionnaires to the attendees during those activities and seminars, some of which were information technology (IT)-related while others were not. We briefly introduced the study to our target respondents before distributing the questionnaires to them. The questionnaires provided the definitions of ISDB and information security on their first page. We asked our target respondents to describe three incidents of "employee engaging in something considered to be information security deviant behavior in organization". We did not require names or personal identities from the respondents, which assured their complete anonymity. We received a total of 204 usable responses.

After the survey, the first author and a research assistant worked independently to simplify and reword the descriptions of the incidents provided by the respondents into clear statements describing different forms of ISDB. We then compared and discussed their work. We constructed a pool of descriptions in ISDB. This content development procedure has been commonly adopted in social sciences research (e.g., Anandarajan, Devine, & Simmers, 2004; Robinson & Bennett, 1995). To further ensure that the descriptions on the consolidated list of behavior were clear enough and were representative of all the incidents the respondents described, we invited a doctoral student in the MIS field to double-check the pool of descriptions against the responses collected. We obtained a list of 43 descriptions in ISDB. Two MIS academics and two information security professionals then reviewed the list to ensure that the descriptions would be easily understood by most people who use computers at work and that they were applicable to various types of organizations. Basically, the reviewers agreed with the descriptions and made only minor changes to the wording.

We then invited ten judges—five MIS academics and five information security professionals—to assess independently whether or not the descriptions of the behavior identified in the list were ISDB based on our definition. The descriptions needed to pass three key criteria. First, the behavior needed to be voluntary. Second, the behavior needed to be conducted by employees in their organizations. Third, the behavior

needed to violate the information security norms of most organizations. We also asked the judges to suggest any other descriptions in ISDB not covered in the list. Basically, all judges agreed that the 43 descriptions in the list described ISDB according to our definition. One of the industry judges, however, had reservations about three descriptions of the behavior—"employee being too lazy to change password at work periodically", "employee using the same password for all company system logins for convenience", and "employee abusing business email account for personal purposes at work". That judge felt that the first two descriptions were controversial because both forms of password behavior are too common in the workplace and so should not be treated as deviance. The judge also felt that the third description may not be relevant because the behavior affects personal data security rather than a company's information security. To remove possible ambiguities and to make sure that the list is representative, we decided to delete these three descriptions. All judges also thought that the list was comprehensive enough and that no additional incidents needed to be included. The first column in Table 2 lists a final pool of 40 descriptions in ISDB.

4.2 Step 2: Multidimensional Scaling

4.2.1 Advantages of Using MDS

We used MDS to develop the typology. MDS is a statistical method that helps one to systematize the relationships among n objects (or variables) in a map—a graphical representation of a k-dimensional coordinate system, where k is predetermined. MDS can be a useful tool for developing typologies for topics such as ISDB in which the organizing concepts and underlying dimensions are not well-developed because MDS adopts an inductive approach to understand the relationships among objects and presents their similarity relationships in a map. However, few researchers in the information systems field have adopted MDS to develop typologies (Nevo et al., 2010). Even when scholars have used MDS, they have adopted it to set up classification systems (e.g., Hult & Chabowski, 2008; Larsen 2003; McQuaid, Ong, Chen, & Nunamaker, 1999; Posey et al., 2013). MDS itself depends solely on data and is usually used to develop inductive and empirically derived models. In this study, we use it to develop a typology that provides another approach for theory building.

4.2.2 Data Collection

We conducted Survey II to identify the constructs for the typology of ISDB. We invited 195 employees from 10 organizations from various industries—three finance/insurance companies, two government departments, one retail company, one IT firm, two logistics-related companies, and one business service company—to participate in this study. We gave them a questionnaire containing the list of 40 descriptions in ISDB; the top of each page briefly described a target behavior (one of the 40 descriptions). This means that we had 40 versions of the questionnaire in total. Before answering the questionnaire, we briefly instructed all respondents to make sure that they understood all descriptions in the list. We required all respondents to perform two tasks. First, they had to rate each form of the behavior in terms of its similarity to or difference from that of the target behavior by using nine-point Likert scales (1 = very similar, 9 = very different). Second, they had to write down the criterion/criteria they had used to distinguish between the target behavior and the different forms of ISDB in the list. We did not record names or individual identities in the questionnaires to obtain honest responses.

4.2.3 MDS Results

A common measure for assessing how well a particular MDS configuration represents the proximity/dissimilarity among different forms of a behavior is the stress index (Kruskal, 1964). The smaller the stress index, the better the fit of the particular configuration. We plotted the stress of the best-fitted configuration in one, two, three, four, and five dimensions in the scree plot of stress. The respective stress levels were 0.47, 0.27, 0.18, 0.13, and 0.1. The scree plot does not exactly illustrate the number of dimensions needed but it does suggest that two is the minimum because we found a sudden drop from 0.47 to 0.27 in the stress value in the two-dimensional solution. Besides stress values, Kruskal and Wish (1978) suggests that interpretability and ease of use are crucial decision factors when selecting the "correct" or "true" dimensionality and the number of interpretable directions can be less than the dimensionality of the space. Therefore, we selected the two-dimensional solution. Appendix C provides more details of the MDS implementation.

Table 2 lists the coordinates of the 40 descriptions in ISDB in the two-dimensional configuration. Some values of the coordinates are positive while others are negative. Figure 1 shows a two-dimension perceptual map for ISDB based on the coordinates. For clearer illustration, we display only the numbers representing their respective forms of ISDB in Table 2. There are four regions in a two-dimensional space, which means that four distinct first-order constructs are expected according to the degree of similarity of different forms of ISDB.

Table 2. The Coordinates of the 40 Descriptions in ISDB in the Two-dimensional Configuration

Item	Dimension 1	Dimension 2
1. Employee not locking his/her work computer when away for convenience.	1.50	0.22
2. Employee not shutting down his/her work computer after finished using it for convenience.	1.49	0.32
3. Employee leaving his/her removable storage devices with company information unattended in office.	1.44	0.01
4. Employee leaving printouts with company information unattended in office.	1.33	0.55
5. Employee allowing non-employees to freely use his/her work computer.	1.29	0.18
6. Employee using colleague's computer without permission.	0.82	-0.40
7. Employee using simple or no password at work for convenience.	1.23	-0.90
8. Employee sharing personal password/account at work with colleagues.	1.47	-0.54
9. Employee writing down personal passwords in visible place.	1.43	-0.35
10. Employee gaining unauthorized access to look at or change company data or files.	0.74	-0.88
11. Employee guessing his/her colleague's password to gain unauthorized access at work.	0.99	-1.25
12. Employee taking away company information without permission.	0.68	1.40
13. Employee copying company documents into his/her removable storage devices without permission.	0.68	1.16
14. Employee not encrypting company documents when they are required to do so.	0.68	0.12
15. Employee using untrusted network (e.g., the Internet) for data transmission at work.	-0.46	0.85
16. Employee disclosing company information for non-work-related purposes.	1.10	1.30
17. Employee using removable storage devices at work without following company security guidelines.	0.33	1.13
18. Employee saving documents in improper locations (e.g., shared folder, mailbox) at work.	0.74	0.54
19. Employee installing untrusted applications for personal purposes at work.	-1.46	0.61
20. Employee running untrusted applications for personal purposes at work.	-1.36	0.46
21. Employee intentionally stopping company's security protection (e.g., antivirus software, Web filtering) at work.	-0.77	-0.12
22. Employee making company information accessible by unauthorized peer-to-peer applications.	0.25	0.58
23. Employee using instant messaging services at work without permission.	-1.32	1.34
24. Employee intentionally opening suspicious e-mails/Web links at work.	-1.65	-0.05
25. Employee intentionally forwarding suspicious e-mails/Web links to colleagues at work.	-1.49	-0.38
26. Employee intentionally browsing untrusted/suspicious websites at work.	-1.55	0.08
27. Employee processing company data in his/her personal notebook at work without permission.	0.13	1.61
28. Employee purposely distributing malicious code (e.g., virus, Trojans, spyware) at work.	-1.54	-0.82

Table 2. The Coordinates of the 40 Descriptions in ISDB in the Two-dimensional Configuration

29. Employee downloading illegal materials (e.g., applications, music, videos) from the Internet at work.	-1.77	0.43
30. Employee extending corporate network (e.g., adding extra access points) in office without permission.	-0.62	0.45
31. Employee using personal email account for business purposes at work without permission.	-0.61	1.54
32. Employee connecting to unauthorized wireless network at work.	-1.02	0.91
33. System administrator not properly destroying information in computer hard disk which is going to be disposed of.	0.46	-1.51
34. System administrator over-granting access permissions to users.	0.06	-1.33
35. System administrator not performing critical security audits and assessments for company.	-0.51	-1.19
36. System administrator not performing essential data backups for company.	-0.79	-1.91
37. System administrator being reluctant to fix security-related application errors/loopholes for company.	-0.82	-0.91
38. System administrator using default password setting or configuration in company's servers for convenience.	-0.14	-1.60
39. System administrator not employing reliable security controls over the wireless network (such as WPA or above) at work.	-0.63	-1.05
40. System administrator enabling remote access to company network without permission.	-0.32	-0.64

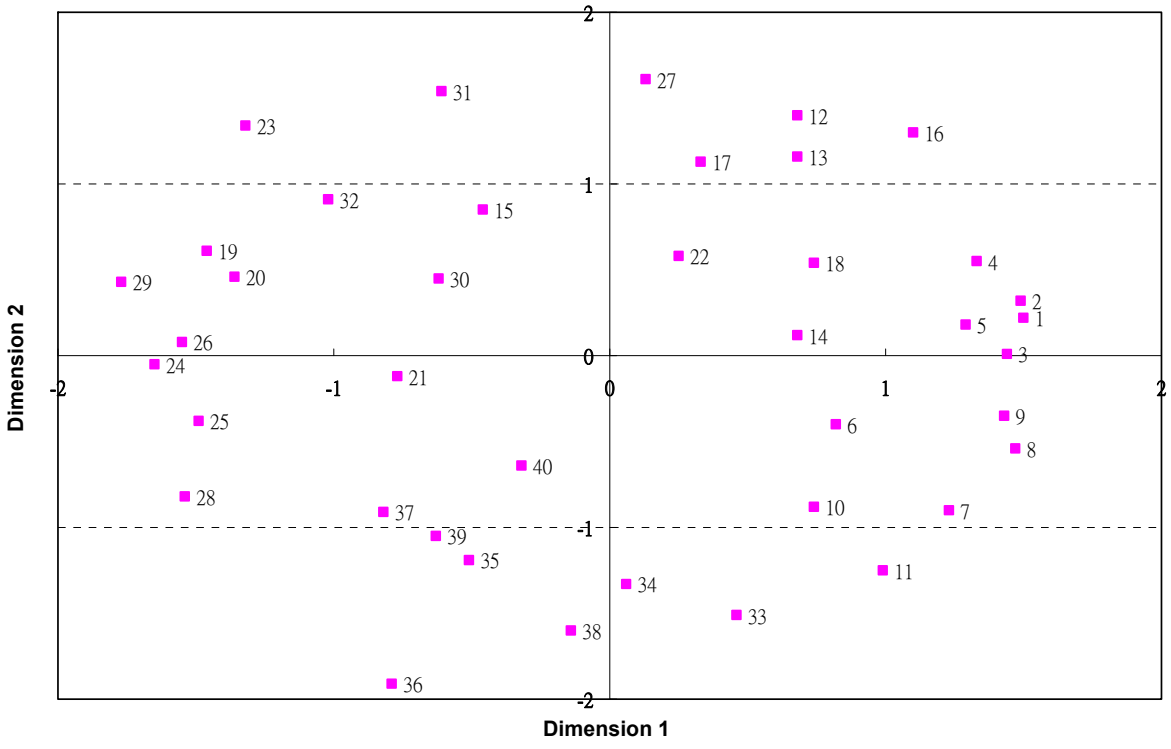

Figure 1. A Two-dimensional Perceptual Map[1]

[1] Only the numbers representing their respective forms of ISDB are shown.

4.3 Step 3: Judgmental Analysis

4.3.1 Opinion Elicitation

In Survey II, we asked respondents not only to rate each form of the behavior in terms of its overall similarity to the target behavior but also to state the criterion/criteria they had used to make their judgments of comparison. We generated several potential attributes that describe the two dimensions on the perceptual map based on the criteria the respondents stated. We then translated the potential attributes into a number of bipolar scales. For example, one respondent wrote that his criterion to distinguish between the target behavior and the different forms of ISDB in the list was "risk of exposing sensitive data". We interpreted this attribute as "high risk of exposing sensitive data/low risk of exposing sensitive data". We decided whether to include an attribute based on the high frequency cited by the respondents and reasonable interpretability of the dimensions. At last, we identified 12 bipolar scales: "planned/spontaneous", "serious/not serious", "difficult to commit/easy to commit", "frequent occurrence/occasional occurrence", "direct harm to organization/indirect harm to organization", "data leakage to outsiders/data leakage to insiders", "desire to gain personal benefits/desire to hurt organization", "high risk of exposing data/low risk of exposing data", "protection-related issue/destruction-related issue", "easy to detect/difficult to detect", "may incur severe punishment/may incur mild punishment", and "security policy can help avert the deviance/security policy cannot help avert the deviance".

Again, we elicited industry wisdom and used regression analysis to interpret the two dimensions. We conducted Survey III and invited 30 industry practitioners with various expertise and from various backgrounds to evaluate how well the potential attributes explain ISDB. Ten such practitioners were academics in various fields, ten were information security professionals, and the remaining ten were managers in non-IT departments. We conducted this exercise, for respondents from different backgrounds to give their opinions on the attributes because the ISDB should be relevant to a wide range of careers and organizations. We provided each respondents with an Excel worksheet with a list of the 40 descriptions in ISDB and the 12 bipolar scales, which they measured on a seven-point rating scale. They were required to rate the degree of relatedness of the 40 descriptions with each other along each of the 12 scales. Altogether, we received 40x12 = 480 ratings from each judge. The bipolar scale ratings collected could guide the interpretation of the two dimensions developed. All respondents worked independently and the findings show that they did not misunderstand the meanings of the 40 descriptions before completing the task.

4.3.2 Interpreting the Two Dimensions

We calculated the mean ratings from the 30 respondents for each of the 40 descriptions in ISDB along each bipolar scale. In other words, we ended up with 40x12 mean ratings associated with the 40x12 combinations of description in ISDB and bipolar scale. We then regressed each of the means of the bipolar scales (dependent variable) on the coordinates of the two dimensions (independent variables) listed in Table 2. We ran separate regressions for each bipolar scale to assess the fitness of each attribute. Table 3 shows the regression results on the 12 bipolar scales and the two-dimension configuration, together with the correlations among the bipolar scales. The first two columns of Table 3 give $\beta 1$ and $\beta 2$, the beta weights on dimensions one and two, respectively. The third column of Table 3 shows the multiple correlation coefficient (R) between the two dimensions and the respective bipolar scales, which assess the predictive power of the two dimensions. A positive/negative value for the beta weight shows a positive/negative association of the dimension with the bipolar scale and the larger the magnitude of beta implies a stronger the relationship between the dimension and the bipolar scale. We found that only eight of the bipolar scales significantly described the two-dimensional configuration—three of the multiple correlation coefficients were significant at the 0.001 level, three at the 0.01 level, and two at the 0.05 level.

Table 3. Potential Attributes for the Dimensions

	Regression		
	Dimension 1 β1	**Dimension 2 β2**	**R**
1. Planned/spontaneous	0.47*	0.82***	0.61***
2. Serious/not serious	0.71***	0.57**	0.68***
3. Difficult/easy to commit	0.21	0.08	0.14
4. Frequent/occasional occurrence	-0.12	-0.60**	0.46**
5. Direct/indirect harm to organization	0.90***	0.22	0.71***
6. Data leakage to outsiders/insiders	0.69*	-0.14	0.39*
7. Desire to gain personal benefits/hurt organization	0.37	-0.48	0.35
8. High/low risk of exposing data	0.51**	-0.25	0.50**
9. Protection/destruction-related issue	-0.45*	-0.32	0.44*
10. Easy/difficult to detect	0.21	0.08	0.15
11. May incur sever/mild punishment	0.47*	0.71**	0.54**
12. Security policy helps/can't help	0.33	0.35	0.36
* p<0.05; ** p<0.01; *** p<0.001			

To select the best attributes for the dimensions, Kruskal and Wish (1978) suggest two selection criteria: 1) a high multiple correlation for the scale with significance at the 0.01 level or better, and 2) a high beta weight on that dimension. Considering the multiple correlation criterion, we found that six bipolar scales ("difficult to commit/easy to commit", "data leakage to outsiders/data leakage to insiders", "desire to gain personal benefits/desire to hurt organization", "protection-related issue/destruction-related issue", "easy to detect/difficult to detect", and "security policy can help to avert the deviance/security policy cannot help to avert the deviance") were unlikely to explain the dimensions because their respective multiple correlation coefficient was either not significant or significant at only the 0.05 level. Table 4 rearranges the order of the bipolar scales with the above six bipolar scales deleted according to their beta weights on the dimensions of each MDS space. We interpret each dimension of the space by examining Table 4.

Table 4. Coordinates of Sorted Attributes

	Dimension 1		**Dimension 2**
Direct/indirect harm	**0.9*** **	Planned/spontaneous	**0.82*** **
Serious/not serious	**0.71*** **	May incur severe/mild punishment	**0.71** **
High/low risk of exposing data	**0.51** **	Serious/not serious	0.57**
Planned/spontaneous	0.47*	Direct/indirect harm	0.22
May incur severe/mild punishment	0.47*	High/low risk of exposing data	-0.25
Frequent/occasional occurrence	-0.12	Frequent/occasional occurrence	-0.60**
Note: These loadings are sorted to correspond with the two-dimensional space			
** p<0.05; ** p<0.01; *** p<0.001*			

Dimension 1 (perceived losses): Table 4 shows that the attributes that best explain dimension 1 are those related to the perceived losses to the organizations from the behavior. Direct/indirect harm to organization is listed at the top ($\beta = 0.9$, $p < 0.001$), followed by serious/not serious ($\beta = 0.71$, $p < 0.001$) and high/low risk of exposing data ($\beta = 0.51$, $p < 0.01$). Thus, one end of the first dimension refers to high perceived losses while the other end refers to low perceived losses. Consequently, we label dimension 1 as "deviance with high perceived losses versus deviance with low perceived losses". Dimension 1 is like a mirror image of the general deterrence theory (GDT), a criminological theory that focuses on "disincentives" or sanctions in deterring people from committing criminal and deviant acts (Blumstein, Cohen, & Nagin, 1978; Straub, 1990). GDT tells us that employees are less likely to commit deviant acts if

they find the chance of being punished is high and the penalty serious. GDT considers deviant behavior from an organizational perspective, while dimension 1 explains an individual's beliefs about the deviant behavior. Employees are concerned about the consequences of the behavior. They understand that some types of behavior are more serious and may have a chance to lead to high losses to the organizations and that others are less serious and less risky. The dimension label "deviance with high perceived losses versus deviance with low perceived losses" is consistent with the findings in the two-dimensional configuration in Table 2. We can find from observation that the types of deviant behavior that are less serious and have lower risk of exposing data are on the positive side of dimension 1 and that the types of behavior that are more serious and have higher risk of exposing data are on the negative side of dimension 1.

We can reasonably say that some types of behavior are expected to create higher losses. Very often, we classify losses as expected losses and unexpected losses. The Basel Committee on Banking Supervision (2001, p. 33) refers to expected losses as "the mean of the loss distribution" and to unexpected losses as "the tail of the loss distribution". In other words, expected losses are expected regular losses that are relatively trivial, but unexpected losses are greater and sustainable losses. This suggests that deviance with high perceived losses may involve unexpected losses that affect organizations' computer systems or a large amount of company data, whereas deviance with low perceived losses may mainly be expected losses that affect individual computers or a small amount of data.

Dimension 2 (frequency): Table 4 shows that the attribute that best explains dimension 2 is planned/spontaneous ($\beta = 0.82$, $p < 0.001$), followed by severe/mild punishment ($\beta = 0.71$, $p < 0.01$) and frequent/occasional occurrence ($\beta = -0.6$, $p < 0.01$). The negative sign of the β value of frequent/occasional occurrence means that employees perceive frequent deviance as spontaneous deviance that deserves less punishment and occasional deviance as planned behavior that deserves more punishment. We can deduce that one extreme of the dimension indicates more common ISDB and that the other extreme represents less common ISDB. Therefore, we use the label "high frequency deviance versus low frequency deviance" for dimension 2. By observation, the two-dimensional configuration in Table 2 supports the label used. We can say that, in general, the forms of ISDB with positive values in dimension 2 occur more commonly in the workplace. On the contrary, the forms of ISDB with negative values in dimension 2 are relatively less common.

We can reasonably say that some types of ISDB are committed more frequently while others are committed less frequently. According to the rational choice theory, individuals are inclined to make choices that maximize total utility (Herrnstein, 1990). Individuals are assumed to maximize utility in a given and stable set of preferences when choosing the course of action (Smelser & Swedberg, 1994). In other words, when individuals make choices, they evaluate the costs and benefits of all choices in the process of choosing and then select the one that maximizes the value of consequences. When they find that the course of action benefits them, they are more likely to go along with it. On the contrary, when they better understand the costs of a course of action, they are less likely to follow it through. These points imply that those frequently committed types of ISDB must be the ones that provide some personal benefits to the employees or incur lower costs to them, whereas those less commonly committed types of ISDB must be the ones that provide fewer personal benefits or are more destructive.

4.4 Typology

4.4.1 Four Ideal Types of Behavior

In the two dimensions and the two-dimensional configuration, we conducted further investigation by organizing ISDB into interrelated types of behavior. Figure 2 exhibits the typology of ISDB. We can organize the behavior into four ideal types that are interrelated along two dimensions—perceived losses and frequency. They are "high frequency, high perceived losses" deviance, "high frequency, low perceived losses" deviance, "low frequency, low perceived losses" deviance, and "low frequency, high perceived losses" deviance.

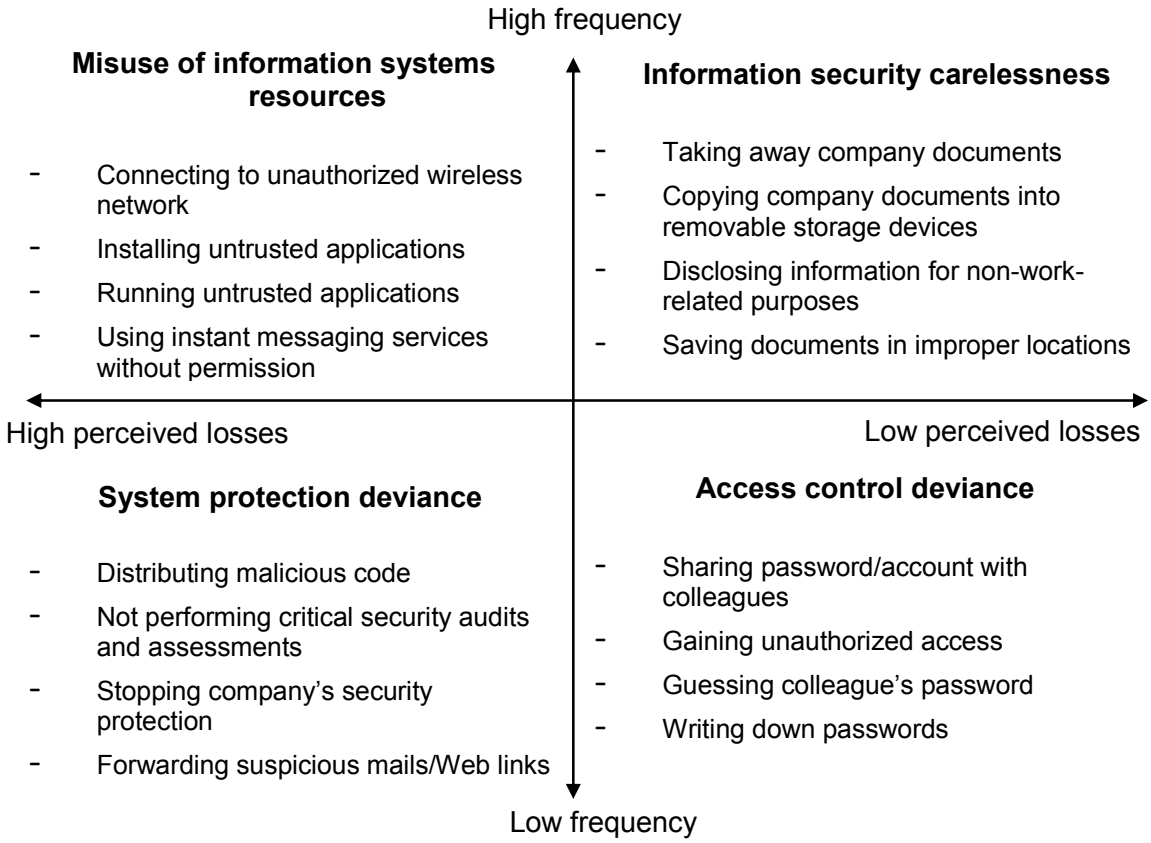

Figure 2. Typology of Information Security Deviant Behavior[2]

"High frequency, high perceived losses" deviance (misuse of information systems resources): this type of ISDB is common in the workplace and can lead to severe consequences. From the MDS results, this type of behavior is mainly related to the misuse or unauthorized use of any information systems resources including applications, the Internet, and network in the workplace. Therefore, we name this type of ISDB misuse of information systems resources. It embraces Schechtman et al.'s (2006) idea about Internet abuse and is similar to D'Arcy et al.'s (2009, p. 79) information systems misuse, which is "intentional insider misuse of information systems resources". Note, however, that employees' unauthorized access to company data, which was one of the scenarios of D'Arcy et al. (2009), is not included in this type. This echoes D'Arcy and Havav's (2007a) observation that research on information security misuse produced conflicting results. It could be the result of the scenarios selected for study. We can reasonably classify misuse of information systems resources as a "high frequency, high perceived losses" deviance. Employees receive instant tangible benefits, such as time savings or extra information, via public resources from misusing resources. It is a deviance with high perceived losses because it can affect the company network and, thus, involves both high expected losses (e.g., computer breakdown) and high unexpected losses (e.g., huge data losses due to hacking). We can see why existing information security studies emphasize information systems misuse because its impacts on organizational security are relatively more significant.

"High frequency, low perceived losses" deviance (information security carelessness): this type of ISDB is expected to be mild in nature and more common. From the MDS results, we can see that this type of behavior is related to employees' bad habits in using computers or handling data in daily operations. Employees commit the behavior mainly due to convenience or bad habits, which are less related to personal benefits. They do not intend to damage their organizational information systems, but they are not security conscious. In addition, they do not feel that the behavior creates any costs for them since they think that others are acting the same way in the workplace. This type of behavior tends to bring high

[2] The list is not exhaustive. The figure contains only some typical forms of ISDB from Figure 1 for illustration purposes.

expected losses but relatively low unexpected losses because it usually has less impact on the organizational network or information systems. Consequently, security carelessness is a "high frequency, low perceived losses" deviance. Previous literature has studied similar deviance. For example, Workman, Bommer, and Straub (2008) investigated omissive security behavior to understand the "knowing-doing" gap in information security.

"Low frequency, high perceived losses" deviance (system protection deviance): this type of ISDB is usually fairly uncommon in the workplace but can result in severe consequences. From the MDS results, we can see that this type of behavior is usually committed by irresponsible employees and can lead to security disasters in organizations. Thus, we label this type of behavior as system protection deviance. The employees usually do not receive instant personal benefits from committing this type of ISDB. However, this type of behavior can harm organizations seriously and, thus, create not only expected losses but also unexpected losses because the impact is more likely at the system or network level. Therefore, system protection deviance is a "low frequency, high perceived losses" deviance. Relatively little behavioral research has been conducted on this type of ISDB because the topic is relatively sensitive.

"Low frequency, low perceived losses" deviance (access control deviance): this type of ISDB is believed to be mild in nature and less common in the workplace. From the MDS results, we can see that this type of behavior is related to passwords or access and violates the company rules of data security or data protection. Therefore, we label this type of behavior as access control deviance. Employees may not receive instant benefits from committing access control deviance but they may perceive a high cost associated with it because most organizations use password authentication to prevent security breaches (Zhang, Luo, Akkaladevi, & Ziegelmayer, 2009) and request their employees to be aware of password-related issues. Moreover, this type of ISDB usually results in relatively low expected losses and unexpected losses because the deviance is inside the organization and the impact is normally limited to individual cases. Accordingly, access control deviance is a "low frequency, low perceived losses" deviance. Researchers have studied password behavior in the past. For example, Hoonakker et al. (2009) studied the bad password practices of end users.

4.5 Step 4: Empirical Testing

4.5.1 Falsifiability

The two dimensions we propose in the "Interpreting the Two Dimensions" section above support Straub and Welke's (1998, pp. 442-443) proposition regarding systems security risk, which refers to "the risk that the firm's information and/or information systems are not sufficiently protected against certain kinds of damage or loss". The basic concept of risk is as follows:

Risk exposure = probability of risk occurring x losses incurred

By considering the above formula, we can create a risk exposure index for each form or each type of ISDB based on the findings in Table 1 because frequency can be a measurement of probability and perceived losses can be a measurement of losses incurred. The two dimensions are noteworthy for at least two reasons. First, Doty and Glick (1994) emphasize that one can use a typology to predict a specific outcome. We can now use the findings from the typology developed in this paper to predict the risk exposure of each type of the deviance. Second, the findings are also important for quantifying ISDB, which are sources of systems security risk, because we can now identify each form of the behavior according to its frequency and perceived losses.

At this point, we have fulfilled and discussed two criteria for a theory: identifying constructs (misuse of information systems resources, information security carelessness, access control deviance, and system protection deviance) and specifying relationships among these constructs (the constructs are interrelated based on perceived losses and frequency). Next, we consider the falsifiability of the typology, which implies that the typology must be testable and subjected to disconfirmation (Doty & Glick, 1994). Lee (2004, p. 3) suggests using the term "empirically testable" to describe the falsifiability property. The typology developed in Figure 2 offers some interesting propositions for empirical testing. In terms of frequency, we expect misuse of information systems resources to be a more common type of ISDB in the workplace than system protection deviance, and information security carelessness to be a more common type than access control deviance. In terms of perceived losses, we expect misuse of information systems

resources to be higher than information security carelessness and system protection deviance to be higher than access control deviance. As such, we hypothesize that:

H1. Relative to system protection deviance, misuse of information systems resources is a more common type of ISDB.

H2. Relative to access control deviance, information security carelessness is a more common type of ISDB.

H3. Relative to information security carelessness, misuse of information systems resources is higher in perceived losses.

H4. Relative to access control deviance, system protection deviance is higher in perceived losses.

4.5.2 Data Collection

We conducted a Web-based survey (Survey IV) consisting of all 40 descriptions in ISDB in Table 2 to understand the relative frequency and perceived losses of the four types of ISDB in a real business environment. We surveyed a group of IT professionals who we randomly picked from a database maintained by a marketing research company that had substantial experience in conducting information security surveys with IT professionals who work in IT-related departments and whose organizational positions varied from programmer to information systems manager across various industries. We chose IT professionals as our respondents because they were the most relevant group of people to evaluate all 40 descriptions in ISDB. We asked them two research questions: first, "how common is the behavior within the IT profession?" This question was related to the frequency of ISDB committed by the IT professionals. We required respondents to indicate the extent of engagement in each of the 40 forms of ISDB on seven-point Likert scales (1 = never, 2 = almost never, 3 = a very few times, 4 = occasionally, 5 = often, 6 = quite often, and 7 = very many times). The second question was: "what do you think the expected financial losses are if incident occurs from the behavior?". This question was associated with the perceived losses of ISDB. We used the expected financial losses incurred to represent the perceived losses of the behavior because it is one of the most popular measures in risk assessment (King, 2001). The respondents indicated their answers based on seven-point Likert scales (1 = very low to 7 = very high). A total of 102 respondents participated in this study.

4.5.3 Data Analysis and Results

We created measurement items for the four constructs developed in this study—misuse of information systems resources, information security carelessness, access control deviance, and system protection deviance—based on the two-dimensional perceptual map in Figure 1. We grouped nine items out of the 40 items under misuse of information systems misuse (items 15, 19, 20, 23, 26, 29, 30, 31, and 32), 13 under information security carelessness (items 1, 2, 3, 4, 5, 12, 13, 14, 16, 17, 18, 22, and 27), eight under access control deviance (items 6, 7, 8, 9, 10, 11, 33, and 34), and 10 under system protection deviance (items 21, 24, 25, 28, 35, 36, 37, 38, 39, and 40). We computed a composite score for each construct by averaging the scores obtained from its respective measurement items. This technique is similar to that employed by D'Arcy and Hovav (2007a) when they generalized patterns of information systems misuse from specific scenarios. We tested the four hypotheses by comparing the mean composite scores using one-tailed paired t-tests. Table 5 displays the mean score differences between misuse of information systems resources and system protection deviance as well as between information security carelessness and access control deviance in terms of frequency. Supporting H1, misuse of information systems resources was more common than system protection deviance ($t = 13.11$, $p < 0.001$). We found that information security carelessness was more common than access control deviance ($t = 9.87$, $p < 0.001$), which supports H2. Table 6 shows the mean score differences between misuse of information systems resources and information security carelessness and between system protection deviance and access control deviance in terms of perceived losses. Supporting H4, system protection deviance was higher in perceived losses than access control deviance ($t = 9.55$, $p < 0.001$). However, no significant evidence supports H3 (i.e., that misuse of information systems resources is higher in perceived losses than information security carelessness).

Table 5. Mean Score Differences (Frequency)

	N	Mean	Mean difference	S.D.	Test statistic	Significance
Misuse of information systems resources	102	2.23	0.75	0.58	13.11	P < 0.001
System protection deviance	102	1.48				
Information security carelessness	102	2.21	0.56	0.58	9.87	P < 0.001
Access control deviance	102	1.65				

Table 6. Mean Score Differences (Perceived losses)

	N	Mean	Mean difference	S.D.	Test statistic	Significance
Misuse of information systems resources	102	4.88	-0.11	0.46	-2.39	n.s.
Information security carelessness	102	4.98				
System protection deviance	102	5.61	0.39	0.41	9.55	P < 0.001
Access control deviance	102	5.23				

5 Discussion

Employees' information security deviance is a major concern for organizations. However, due to its sensitive nature, ISDB has been an underdeveloped topic (Kotulic & Clark, 2004; Werlinger, Hawkey, & Beznosov, 2009). With this research, we explore ISDB and investigate the interrelationships among different types of ISDB by constructing a typology that fulfills four primary criteria of being a theory. First, we clearly define ISDB and the study's boundaries. We define ISDB as the voluntary behavior of employees within organizations that differs markedly from the information security norms of the organizations and that is normally considered by other employees to be inappropriate behavior in organizations. We consolidate a pool of 40 descriptions in ISDB. Second, we identify four types of ISDB: misuse of information systems resources, information security carelessness, access control deviance, and system protection deviance. Third, we found that these four types of ISDB were interrelated along two dimensions—perceived losses and frequency. Fourth, we subjected the relationships among the four types of ISDB to hypothesis testing. Theory development is crucial to growing information systems research (Gregor, 2006, Weber, 2012). This paper makes an important theoretical contribution by demonstrating how we can develop a typology, which is a unique form of theory building, for a relatively underdeveloped topic. The suggested procedure can help researchers to develop typologies of interested areas. Typology is useful for understanding the nature of a behavior and as a framework for building theories for the behavior because it explains what the variants of the behavior are and how they are interrelated. However, many researchers have built their typologies in an unsystematic or a subjective way that can only be called classification systems or taxonomies. The quantitative approach we suggest in this study could be adopted for developing typologies. The approach can be used to develop a fully specified typology based on empirical methods in a systematic manner. We use MDS, together with other statistical techniques, to uncover two underlying dimensions and identify four ideal types of ISDB. MDS itself is data driven and can only be used to develop an inductive and empirically derived model that cannot be treated as a theory. However, by using MDS in the suggested way, a theory can be built for a relatively underdeveloped topic. This theory building procedure is useful for exploring new or underdeveloped research topics.

This study's findings have implications for both research and practice. For research, the study clarifies the different types of ISDB and their interrelationships and differences. The findings are useful for researchers when adopting scenario study in their ISDB-related research. Some researchers have limited their studies to a few specific hypothetical scenarios when they studied information security deviance. This is a reasonable and effective survey method when studying a behavior that has many variants. For example, D'Arcy and Hovav (2007a) computed a composite score for information systems misuse by averaging the

scores obtained from five scenarios—password sharing, inappropriate use of email, use of unlicensed software, unauthorized access to computerized data, and unauthorized modification of computerized data—when they studied the influence of user awareness of security countermeasures on information systems misuse. Our findings suggest that one should select the scenarios carefully because the behavior studied may be described along a continuum of dimensions. If extreme forms of the behavior are included, the results may be misinterpreted. D'Arcy and Hovav (2007a) report that research on information security misuse produced conflicting results. This conflict might have something to do with their selection of scenarios. Therefore, the typology is important for scenario selection.

Without a clear definition of a behavior and knowing the interrelationships of different types of the behavior, further investigations may be difficult to conduct. This could be the very reason why only isolated research efforts on information security deviance have been made in the past. We propose a theoretical ISDB framework for constituting a critical starting point for the development of instruments of the behavior and the further development of research models on ISDB. We developed a two-dimensional ISDB typology that identifies the relationships among different types of ISDB and their underlying constructs. Researchers can follow the framework to develop reliable and valid instruments to measure ISDB or start to build and test theoretical models of the different types of ISDB, such as information security careless and access control deviance. The framework may enable researchers to systematically investigate behaviors.

Some practical implications also emerge from our findings. The list of the 40 typical descriptions in ISDB and the findings of perceived losses and frequency as the two dimensions provide more insights for managers to understand different forms of ISDB, their relationships, and their impacts on organizations. Special attention should be paid to the forms of ISDB in misuse of information systems resources because it is a "high frequency, high perceived losses" deviance. Bennett and Robinson (2000) and Robinson and Bennett (1997) suggest that, if an employee engages in behavior that belongs to a particular behavioral family, then that employee has a greater tendency to engage in other forms of behavior in that family relative to other families. For instance, if staff member Sarah likes to take away company information without permission (a form of information security carelessness), she has a higher chance to perform other forms of information security carelessness such as copying company documents into her removable storage devices without permission or disclosing company information for non-work-related purposes. This information is useful for managers to understand the information security level in organizations from different aspects by observing staff behavior so as to develop better security strategy.

Moreover, this paper also helps managers measure ISDB under the typology setting. Normally, it is difficult to quantify a behavior. However, under our typological framework involving the two dimensions—perceived losses and frequency, we can now quantify ISDB. One could adopt an appropriate actuarial model to assess the risk of ISDB. For example, Wang, Chaudhury, and Rao (2008) use the concept of value-at-risk (VaR) (Crouhy, Galai, & Mark, 2001; Duffie & Pan 1997; Jorion, 2007)—a statistical analysis method that takes expected losses and unexpected losses into account and has been widely used as a tool for measuring financial risk (e.g., So & Yu, 2006; Wong & So, 2003)—to develop an actuarial model for information security investment strategy. By extending the VaR concept to ISDB, we can also derive an actuarial model for ISDB. Managers can then use this model to formulate security investment strategy for preventing ISDB. Therefore, one future avenue of research may be in using statistical or financial analysis techniques to quantify the risk of ISDB.

The falsifiability test examines the relationships among the four types of ISDB. Consistent with our expectation, misuse of information systems resources was more common than system protection deviance and security carelessness was more common than access control deviance. Moreover, system protection deviance was higher in perceived losses than access control deviance. However, we found no significant evidence that misuse of information systems resources was higher in perceived losses than security carelessness from our survey results, which we did not expect. We can explain this finding in two ways. First, the result may be affected by the expected losses and unexpected losses, which we did not explicitly consider because we asked the respondents only about the expected financial losses. Second, we considered all items in the list of ISDB. However, some forms of the behavior perform differently from others even if they are all of the same deviance type. These explanations should be verified in the future.

One limitation of this study is that our pool of ISDB may not be exhaustive. However, we do not mean to compile an exhaustive list of ISDB because technology is advancing on a daily basis and new forms of ISDB emerge all the time. Instead, we demonstrate how to construct a typological theory for a relatively underdeveloped topic, which allows future researchers to adopt the typology development process

suggested herein to explore new research topics in their domains of interest. In this study, we use ISDB as an exemplar and develop a typology on ISDB that can explain the relationships among different types of ISDB based on some underlying dimensions. Another limitation is that the significance of the falsifiable test of the typology tends to rely on self-reported data. was Although, with this falsifiable test, we mean to demonstrate how the four types of deviance can be tested, we paid every effort to collect the most representative responses, such as using diverse samples and anonymous responses. A typology is a good start to describe and understand organizational diversity, but a limitation in using typology to study a behavior is that it focuses on examining differences between types of the behavior in general situations, ignores differences that may exist in a specific type of the behavior, and excludes specific circumstances. This reduces the individuality of cases. For example, items in a type of ISDB could lead to different degree of severe consequences and the degree of the severe consequences may change owing to specific situations. It would be worthwhile discovering how different types of ISDB affect organizations in various scenarios. Further, a limitation on MDS to develop a typology is the configurations generated through MDS may not always fully interpretable. Thus, the interpretation process can be subjective and result in researcher bias. To reduce the bias and develop more representative attributes in interpreting the dimensions, we used both qualitative judgment (opinion elicitation from survey respondents) and a quantitative methodology (judgmental analysis using multiple regression).

In summary, we provide answers to the questions of what ISDB is and how its types are organized by developing a typology for ISDB using a quantitative approach. The consolidated list of ISDB and the four types of the behavior proposed can help managers to understand the influence of the behavior in organizations more deeply and, thus, develop appropriate awareness programs to increase the organizational security level and strategy to prevent the occurrence of security incidents. For researchers, the proposed procedure provides another approach for theory building. Moreover, with the understanding of the interrelationships among different types of ISDB, the selection of deviance situations for research purposes would be more appropriate as ISDB can be different in nature and can be in various forms. To our best knowledge, this is one of the pioneer studies to profile ISDB in detail theoretically. The need to call for more empirical research to study the dark side of security behavior demands greater research emphasis (Mahmood et al., 2010; Willison & Warkentin, 2013). A typology of ISDB, as presented in this study, provides an organized and theoretical framework for researchers to conduct further studies on ISDB.

6 Conclusion

Previous research has sometimes confused typology with classification or taxonomy. Typology is a unique form of theory building but classification and taxonomy are not. Following a systematic review of the literature, Guilllemette and Paré (2012) developed a new typology of the contribution of IT function. However, their proposed qualitative methodology may not be useful for underdeveloped or new topics in the literature. As such, in this paper, we outline a generic procedure for developing a typology that fulfills the criteria of a theory using a quantitative approach for researchers to develop typological theories in their domains of interest. We expect that our rigorous quantitative approach in developing typological theories will help researchers to explore new topics or behavior in the information systems field.

References

Anandarajan, M., Devine, P., Simmers, C. (2004). A multidimensional scaling approach to personal Web usage in the workplace. In M. Anandarajan & C. Simmers (Eds.), *Personal Web usage in the workplace: A guide to effective human resource* management (pp. 61-78). Hershey, PA: Information Science Publishing.

Bacharach, S. B. (1989). Organizational theories: Some criteria for evaluation. *Academy of Management Review, 14*(4), 496-515.

Basel Committee on Banking Supervision. (2001). *Working paper on the regulatory treatment of operational risk*. Retrieved from http://www.bis.org/publ/bcbs_wp8.pdf

Belanger, F., & Slyke, C. V. (2002). Abuse or Learning? *Communications of the ACM, 45*(1), 64-65.

Bennett, R. J., & Robinson, S. L. (2000). Development of a measure of workplace deviance. *Journal of Applied Psychology, 85*(3), 349-360.

Blumstein, A., Cohen, J., & Nagin, D. (1978). *Deterrence and incapacitation: Estimating the effects of criminal sanctions on crime rates*. Washington, DC: National Academy of Sciences.

Bock, G.-W., & Ho, S. L. (2009). Non-work related computing (NWRC). *Communications of the ACM, 52*(4), 124-128.

Brown, A., & Grant, G. G. (2005). Framing the frameworks: A review of IT governance research. *Communications of the Association for Information Systems, 15*, 696-712.

Campbell, M., & Lu, Y. (2007). Managing the dark side of computer use at work: A typology of information technology abuse and management strategy. In *Proceedings of the 13th Americas Conference on Information Systems.*

Chiasson, M. W., & Davidson, E. (2005). Taking industry seriously in information systems research. *MIS Quarterly, 29*(4), 591-605.

Choobineh, J., Dhillon, G., Grimaila, M. R., & Rees, J. (2007). Management of information security: Challenges and research directions. *Communications of the Association for Information Systems, 20*, 958-971.

Chu, A. M. Y., & Chau, P. Y. K. (2014). Development and validation of instruments of information security deviant behavior. *Decision Support Systems, 66*, 93-101.

Chu, A. M. Y., Chau, P. Y. K., & So, M. K. P. (Forthcoming). Explaining the misuse of information systems resources in the workplace: A dual-process approach. *Journal of Business Ethics.*

Clark, V. (2004). *SAS/STAT 9.1: User's guide*. Cary, NC: SAS Pub.

Clinard, M. B., Quinney, R., & Wildeman, J. (1994). *Criminal behavior systems: A typology (*3rd ed.). Cincinnati: Anderson Publishing Company.

Crouhy, M., Galai, D., & Mark, R. (2001). *Risk management.* New York: McGraw-Hill.

D'Arcy, J., & Devaraj, S. (2012). Employee misuse of information technology resources: Testing a contemporary deterrence model. *Decision Sciences, 43*(6), 1091-1124.

D'Arcy, J., & Hovav, A. (2007a). Deterring internal information systems misuse. *Communications of the ACM, 50*(10), 113-117.

D'Arcy, J., & Hovav, A. (2007b). Towards a best fit between organizational security countermeasures and information systems misuse behaviors. *Journal of Information System Security, 3*(2), 3-31.

D'Arcy, J., Hovav, A., & Galletta, D. (2009). User awareness of security countermeasures and its impact on information systems misuse: A deterrence approach. *Information Systems Research, 20*(1), 79-98.

Doty, D. H., & Glick, W. H. (1994). Typologies as a unique form of theory building: Toward improved understanding and modeling. *Academy of Management Review, 19*(2), 230-251.

Dubin, R. (1978). *Theory building* (Rev. ed.). New York: Free Press.

Duffie, D., & Pan, J. (1997). An overview of value at risk. *The Journal of Derivatives, 19*(1), 106-120.

Earl, M. (2001). Knowledge management strategies: Toward a taxonomy. *Journal of Management Information Systems,* (18)1, pp. 215-233.

Fenz, S., Ekelhart, A., & Neubauer, T. (2011). Information security risk management: In which security solutions is it worth investing? *Communciations of the Association for Information Systems, 28*, 329-356.

Gregor, S. (2006). The nature of theory in information systems. *MIS Quarterly, 30*(3), 611-642.

Griffin, R. W., & Lopez, Y. P. (2005). "Bad behavior" in organizations: A review and typology for future research. *Journal of Management, 31*(6), 988-1005.

Guillemette, M. G., & Paré, G. (2012). Toward a new theory of the contribution of the IT function in organizations. *MIS Quarterly, 36*(2), 529-551.

Guo, K. H., Yuan, Y., Archer, N. P., & Connelly, C. E. (2011). Understanding nonmalicious security violations in the workplace: A composite behavior model. *Journal of Management Information Systems, 28*(2), 203–236.

Harrington, S. J. (1996). The effect codes of ethics and personal denial of responsibility on computer abuse judgments and intentions. *MIS Quarterly, 20*(3), 257-278.

Heo, J., & Han, I. (2003). Performance measure of information systems (IS) in evolving computing environments: An empirical investigation. *Information & Management, 40*(4), 243-256.

Herrnstein, R. J. (1990). Rational choice theory: Necessary but not sufficient. *American Psychologist, 45*(3), 356-367.

Hoonakker, P., Bornoe, N., & Carayon, P. (2009). Password authentication from a human factors perspective: Results of a survey among end-users. *Proceedings of the 53rd Annual Meeting of the Human Factors and Ergonomics Society Annual Meeting*, *53*(6), 459-463.

Hovav, A., & D'Arcy, J. (2012). Applying an extended model of deterrence across cultures: An investigation of information systems misuse in the U.S. and South Korea. *Information & Management*, *49*(2), 99–110.

Hu, Q., & Dinev, T. (2005). Is spyware an internet nuisance or public menace? *Communications of the ACM, 48*(8), 61-66.

Hu, Q., Xu, Z., Dinev, T., & Ling, H. (2011). Does deterrence work in reducing information security policy abuse by employees? *Communications of the ACM, 54*(6), 54-60.

Hu, Q., Dinev, T., Hart, P., & Cooke, D. (2012). Managing employee compliance with information security policy: The critical role of top management and organizational culture. *Decision Sciences, 43*(4), 615-659.

Hult, G. T. M., & Chabowski, B. R. (2008). Sourcing research as an intellectual network of ideas. *Decision Sciences, 39*(3), 323-335.

Jorion, P. (2007). *Value at risk: The new benchmark for managing financial risk.* New York: McGraw-Hill.

King, J. L. (2001). *Operational risk: Measurement and modelling.* New York: Wiley.

Kotulic, A. G., & Clark, J. G. (2004). Why there aren't more information security research studies. *Information & Management, 41*(5), 597-607.

Kruskal, J. B. (1964). Multidimensional scaling by optimizing goodness of fit to a non-metric hypothesis. *Psychometrica, 29*(1), 1-27.

Kruskal, J. B., & Wish, M. (1978). *Multidimensional scaling*. London: Sage.

Kwan, S. K., So, K. P., & Tam, K. Y. (2010). Applying randomized response technique to elicit truthful responses to sensitive questions in IS research: The case of software piracy behavior. *Information Systems Research, 21*(4), 941-959.

Larsen, K. R. T. (2003). A taxonomy of antecedents of information systems success: Variable analysis studies. *Journal of Management Information Systems, 20*(2), 169-246.

Lee, A. S. (2004). Thinking about social theory and philosophy for information systems. In J. Mingers & L. Willcocks (Eds.), *Social theory and philosophy for information systems* (pp. 1-26). Chichester, UK: Wiley.

Lee, S. M., Lee, S.-G., & Yoo, S. (2004). An integrative model of computer abuse based on social control and general deterrence theories. *Information & Management, 41*(6), 707-718.

Lee, Y., & Kozar, K. A. (2008). An empirical investigation of anti-spyware software adoption: A multitheoretical perspective. *Information & Management, 45*(2), 109-119.

Lee, Y., & Larsen, K. R. (2009). Threat or coping appraisal: Determinants of SMB executives' decision to adopt anti-malware software. *European Journal of Information Systems, 18*(2), 177-187.

Loch, K. D., Carr, H. H., & Warkentin, M. E. (1992). Threats to information systems: Today's reality, yesterday's understanding. *MIS Quarterly, 16*(2), 173-186.

Lowry, P. B., Moody, G., Galletta, D., & Vance, A. (2012). The drivers in the use of online whistle-blowing reporting system. *Journal of Management Information Systems, 20*(1), 153-177.

Mahmood, M. A., Siponen, M., & Straub, D., & Rao, H. R. (2010). Moving toward black hat research in information systems security: An editorial introduction to the special issue. *MIS Quarterly, 34*(3), 431-433.

McQuaid, M. J., Ong, T.-H., Chen, H., & Nunamaker, J. F. (1999). Multidimensional scaling for group memory visualization. *Decision Support Systems, 27*(1-2), 163-176.

Melville, N., Kraemer, K., & Gurbaxani, V. (2004). Review: Information technology and organizational performance: An integrative model of IT business value. *MIS Quarterly, 28*(2), 283-322.

Nevo, S., Nevo, D., & Ein-Dor, P. (2010). Classifying information technologies: A multidimensional scaling approach. *Communications of the Association for Information Systems, 27*, 831-842.

Oravec, J. A. (2002). Constructive approaches to Internet recreation in the workplace. *Communications of the ACM, 45*(1), 60-63.

Peace, A. G., Galletta, D., & Thong, J. Y. L. (2003). Software privacy in the workplace: A model and empirical test. *Journal of Management Information Systems, 20*(1), 153-177.

Pearce, P. L., & Amato, P. R. (1980). A taxonomy of helping: A multidimensional scaling analysis. *Social Psychology Quarterly, 43*(4), 363-371.

Pee, L. G., Woon, I. M. Y., & Kankanhalli, A. (2008). Explaining non-work-related computing in the workplace: A comparison of alternative models. *Information & Management, 45*(2), 120-130.

Posey, C., Bennett, R. J., & Roberts, T. L. (2011a). Understanding the mindset of the abusive insider: An examination of insiders' causal reasoning following internal security changes. *Computers & Security, 30*(6), 486-497.

Posey, C., Bennett, R. J., Roberts, T. L., & Lowry, P. B. (2011b). When computer monitoring backfires: Privacy invasions and organizational injustice as precursors to computer abuse. *Journal of Information Systems Security, 7*(1), 24-47.

Posey, C., Roberts, T., Lowry, P. B., Bennett, R. J., & Courtney, J. F. (2013). Insiders' protection of organizational information assets: Development of a systematics-based taxonomy and theory of diversity for protection-motivated behaviors. *MIS Quarterly, 37*(4), 1189-1210.

Robinson, S. L., & Bennett, R. J. (1995). A typology of deviant workplace behaviors: A multidimensional scaling study. *Academy of Management Journal, 38*(2), 555-572.

Robinson, S. L., & Bennett, R. J. (1997). Workplace deviance: Its definition, its manifestations, and its causes. *Research on Negotiations in Organizations, 6*, 3-27.

Schechtman, G. M., Marett, K., & Wells, J. D. (2006). *Internet abuse: A general theory of crime framework.* Paper presented at the 12th Americas Conference on Information Systems, Acapulco, Mexico.

Schiffman, S. S., Reynolds, M. L., & Young, F. W. (1981). *Introduction to multidimensional scaling: Theory, methods, and applications.* New York: Academic Press.

Shropshire, J. (2009). A canonical analysis of intentional information security breaches by insiders. *Information Management & Computer Security, 17*(4), 296-310.

Simon, S. A., & Eby, L. T. (2003). A typology of negative mentoring experiences: A multidimensional scaling study. *Human Relations, 56*(9), 1083-1106.

Siponen, M., Willison, R., & Baskerville, R. (2008). Power and practice in information systems security research. In *Proceedings of the 29th International Conference on Information Systems.*

Siponen, M., & Vance, A. (2010). Neutralization: New insights into the problem of employee information systems security policy violations. *MIS Quarterly, 34*(3), 487-502.

Smelser, N. J., & Swedberg, R. (1994). The sociological perspective on the economy. In N. J. Smelser & R. Swedberg (Eds.), *The handbook of economic sociology* (pp. 3-26). Princeton, NJ: Princeton University Press.

So, M. K. P., & Yu, P. L. H. (2006). Empirical analysis of GARCH models in value at risk estimation. *Journal of International Financial Markets, Institutions and Money, 16*(2), 180-197.

Stanton, J. M., Stam, K. R., Mastrangelo, P., & Jolton, J. (2005). Analysis of end user security behavior. *Computers & Security, 24*(2), 124-133.

Straub, D. W., Jr. (1990). Effective IS security: An empirical study. *Information Systems Research, 1*(3), 255-276.

Straub, D. W., Jr., & Nance, W. D. (1990). Discovering and disciplining computer abuse in organizations: A field study. *MIS Quarterly, 14*(1), 45-60.

Straub, D. W., & Welke, R. J. (1998). Coping with systems risk: Security planning models for management decision making. *MIS Quarterly, 22*(4), 441-469.

Thompson, P. (1983). Some missing data patterns for multidimensional scaling. *Applied Psychological Measurement, 7*(1), 45-55.

Von Solms, B. (2000). Information security—the third wave? *Computers & Security, 19*(7), 615-620.

Von Solms, B. (2006). Information security—the fourth wave. *Computers & Security, 25*(3), 165-168.

Vance, A., & Siponen, M. (2012). IS security policy violations: A rational choice perspective. *Journal of Organizational and End User Computing, 24*(1), 21-41.

Wang, J., Chaudhury, A., & Rao, H. R. (2008). A value-at-risk approach to information security investment. *Information Systems Research*, *19*(1), 106-120.

Weber, R. (2012). Evaluating and developing theories in the information systems discipline. *Journal of the Association for Information Systems, 13*(1), 1-30.

Webster, J., & Watson, R. T. (2002). Analyzing the past to prepare for the future: Writing a literature review. *MIS Quarterly, 26*(2), xiii-xxiii.

Werlinger, R., Hawkey, K., & Beznosov, K. (2009). An integrated view of human, organizational, and technological challenges of IT security management. *Information Management & Computer Security, 17*(1), 4-19.

Whitman, M. E., & Mattord, H. J. (2004). *Management of information security.* Cambridge, Mass: Course Technology.

Willison, R., & Siponen, M. (2009). Overcoming the insider: Reducing employee computer crime through situational crime prevention. *Communications of the ACM, 52*(9), 133-137.

Willison, R., & Warkentin, M. (2013). Beyond deterrence: An expanded view of employee computer abuse. *MIS Quarterly, 37*(1), 1-20.

Wong, C.-M., & So, M. K. P. (2003). On conditional moments of GRACH models, with applications to multiple period value at risk estimation. *Statistica Sinica, 13*(4), 1015-1044.

Workman, M., Bommer, W. H., & Straub, D. (2008). Security lapses and the omission of information security measures: A threat control model and empirical test. *Computers in Human Behavior, 24*(6), 2799-2816.

Workman, M., & Gathegi, J. (2007). Punishment and ethics deterrents: A study of insider security contravention. *Journal of The American Society for Information Science and Technology, 58*(2), 212-222.

Young, F. W. (1975). Scaling replicated conditional rank-order data. *Sociological Methodology, 6*, 129-170.

Zafar, H., & Clark, J. G. (2009). Current state of information security research in IS. *Communication of the Association for Information Systems, 24*, 557-596.

Zhang, J., Luo, X., Akkaladevi, S., & Ziegelmayer, J. (2009). Improving multiple-password recall: An empirical study. *European Journal of Information Systems, 18*(2), 165-176.

Appendix A: Literature on Negative Forms of Information Security Behavior

Table A1. Literature on Negative Forms of Information Security Behavior

Behavior	References
Computer abuse	Harrington (1996), Lee, Lee, & Yoo (2004), Lowry, Moody, Galletta, & Vance (2012), Posey, Bennett, & Roberts (2011a, 2011b), Straub (1990), Straub & Nance (1990), Willison & Warkentin (2013)
End user security behavior	Stanton et al. (2005)
Information systems misuse	D'Arcy et al. (2007a, 2007b), D'Arcy et al. (2009), Hovav & D'Arcy (2012)
Information technology abuse	Campbell & Lu (2007)
Intentional information security breaches by insider	Shropshire (2009)
Internet abuse	Schechtman et al. (2006)
Insider security contravention	Workman & Gathegi (2007)
IS security policy violation/ Information security policy abuse	Hu et al. (2011), Siponen & Vance (2010), Vance & Siponen (2012)
Misuse of information technology resources	D'Arcy and Devaraj (2012)
Nonmalicious security violations/non-malicious computer and information security deviations	Hoonakker et al. (2009), Guo, Yuan, Archer, & Connelly (2011)
Non-work-related computing	Bock & Ho (2009), Pee et al. (2008)
Omissive behavior	Workman et al. (2008)
Software privacy	Peace, Galletta, & Thong (2003), Kwan, So, & Tam (2010)

Appendix B: Writing Style Guidelines

Table B1. Literature on Negative Forms of Information Security Behavior

	Survey I (N = 204)	Survey II (N = 195)	Survey III (N = 30)	Survey IV (N = 102)
Percentage of respondents				
Industry				
Manufacturing	6	0	0	13
Wholesale and retail	9	18	7	2
Education and health	23	0	20	5
Business services	2	13	7	7
Finance and insurance	9	22	13	8
Transportation, information technology, and communications	22	23	30	32
Social and personal services	20	0	7	7
Government	5	24	16	18
Others	4	0	0	8
Company size *(# of employees)*				
Fewer than 100	38	30	27	52

Table B1. Literature on Negative Forms of Information Security Behavior

100-499	22	30	23	15
500 or more	40	40	50	33
Position				
Managerial	25	28	50	43
Technical	28	21	17	35
Professional staff	12	9	33	22
Administrative/clerical	35	42	0	0
Department				
IT-related department	31	38	40	100
Non-IT-related department	69	62	60	0
Gender				
Male	62	60	63	68
Female	38	40	37	32
Age				
18-24	22	2	0	12
25-34	28	45	33	43
35-44	34	50	50	24
45-54	12	3	10	13
55 and over	4	0	7	8
Education level				
High school/non-degree	21	0	0	7
Degree or above	79	100	100	93

Appendix C: Implementation of Multidimensional Scaling

In this study, we analyzed the n = 40 forms of ISDB by using multidimensional scaling (MDS). We collected dissimilarities of all $n(n-1)/2$ pairwise combinations of the 40 forms of ISDB by survey. The dissimilarities $(i \text{ and } j = 1,\ldots, 40)$ represent how people rated the similarity among the 40 forms of the behavior.

We recruited a total of 195 employees from 10 organizations. Because of the large number of distinct pairs of the descriptions to rank $(n(n-1))/2 = 40x39/2 = 780)$, we required each respondent to only evaluate a subsample (40 ratings) of the distinct pairs. That is, we gave each respondent one of the 40 versions of the questionnaire randomly to complete. That means each possible pair of descriptions was rated by 10 randomly selected respondents $(195x40/780 = 10)$. We then obtained each dissimilarity by averaging the ratings given by the 10 respondents on the similarity between behavior i and behavior j. Scholars have suggested this conditional rank order process of asking respondents to compare a subset instead of the full set to be a valid method to avoid potential difficulties and errors associated with comparing a large number of pairs of stimuli (Thompson, 1983; Young, 1975). Some studies that have adopted MDS in their surveys used this process to reduce information overload for respondents (e.g., Pearce & Amato, 1980; Robinson & Bennett, 1995; Schiffman, Reynolds, & Young, 1981; Simon & Eby, 2003).

Implementing MDS

We primarily used MDS in this study to identify a configuration matrix X that best represents the proximity/dissimilarity of the 40 forms of ISDB. This X has n rows where the i^{th} row gives the k $(<= n)$ coordinates of behavior i in a k-dimensional map. In other words, X determines the location of the n forms of the behavior and the dissimilarity among different forms of the behavior by $d_{ij}(X)$, the distance between behavior i and behavior j where $i, j = 1, \ldots, n$. The distance in a map can be calculated as:

$$d_{ij}(X) = \sqrt{\sum_{b=1}^{k} (X_{ib} - X_{jb})^2},$$

where X_{ib} is the b^{th} coordinate of the i^{th} behavior. Since δ_{ij} is the "observed" dissimilarity (given by the Likert scores in our case), a good configuration X should produce $d_{ij}(X)$ close to δ_{ij}. However, it is unlikely to find a configuration of points whose pairwise distance matches exactly or is montonically related to the original dissimilarities. To obtain the best X for a given dimension k, we minimized Kruskal's (1964) Stress index defined by

$$\text{Stress} = \frac{\sum_{i=1}^{n} \sum_{j=1}^{n} (\delta_{ij} - d_{ij}(X))^2}{\sum_{i=1}^{n} \sum_{j=1}^{n} d_{ij}(X)^2}$$

with respect to X. The smaller the stress value, the smaller the discrepancy between the observed dissimilarities δ_{ij} and $d_{ij}(X)$. We used the MDS procedure in the SAS system (Clark, 2004) by adopting a nonlinear least-squares method to obtain X for various k. We created a similarities/dissimilarities matrix by merging the data collected from the questionnaire to run the SAS program. When dimension k increases, the stress value decreases. However, a higher dimension means a more complex configuration map which may not be desirable in the interpretation perspective. The stress value is a good reference for identifying a suitable k for developing a parsimonious configuration X while maintaining a reasonably good match between δ_{ij} and $d_{ij}(X)$.

About the Authors

Amanda M. Y. Chu is an Assistant Professor at the Hang Seng Management College. She obtained her PhD in MIS from the University of Hong Kong and her MBA degree from the Chinese University of Hong Kong. Her current research interests include information security, ethics and privacy, and business intelligence. She has published in journals such as *Decision Support Systems* and *Journal of Business Ethics*. Prior to studying for her PhD, she was a consultant in information systems for over 8 years.

Patrick Y. K. Chau is Padma and Hari Harilela Professor in Strategic Information Management at the Faculty of Business and Economics of The University of Hong Kong. He received his PhD in business administration from the Richard Ivey School of Business at the University of Western Ontario, Canada. His research interests include IS/IT adoption and implementation, information presentation, knowledge management and IT outsourcing. He has published papers in journals such as *MIS Quarterly*, *Communications of the AIS*, *Journal of the AIS*, *Journal of Management Information Systems*, *Decision Sciences*, *Information and Management*, *Decision Support Systems*, *Journal of Global Information Management*, and *Communications of the ACM*, among others.

Mike K. P. So is an Associate Professor of the Department of Information Systems, Business Statistics and Operations Management at the Hong Kong University of Science and Technology. His research interests include nonlinear time series analysis, dynamic modeling of economic & financial data, Bayesian analysis, risk management, and data analytics.