sustainability

Article

Organizational Information Security Management for Sustainable Information Systems: An Unethical Employee Information Security Behavior Perspective

Amanda M. Y. Chu [1,*] and Mike K. P. So [2]

[1] Department of Social Sciences, The Education University of Hong Kong, Hong Kong, China
[2] Department of Information Systems, Business Statistics and Operations Management, The Hong Kong University of Science and Technology, Hong Kong, China
* Correspondence: amandachu@eduhk.hk

Received: 13 March 2020; Accepted: 9 April 2020; Published: 14 April 2020

Abstract: This article examines the occurrences of four types of unethical employee information security behavior—misbehavior in networks/applications, dangerous Web use, omissive security behavior, and poor access control—and their relationships with employees' information security management efforts to maintain sustainable information systems in the workplace. In terms of theoretical contributions, this article identifies and develops reliable and valid instruments to measure different types of unethical employee information security behavior. In addition, it investigates factors affecting different types of such behavior and how such behavior can be used to predict employees' willingness to report information security incidents. In terms of managerial contributions, the article suggests that information security awareness programs and perceived punishment have differential effects on the four types of unethical behavior and that certain types of unethical information security behavior exert negative effects on employees' willingness to report information security incidents. The findings will help managers to derive better security rules and policies, which are important for business continuity.

Keywords: business continuity; information security; information systems misuse; insider; unethical behavior

1. Introduction

Organizations have been increasingly using information technology (IT) to enhance business operations and decision-making processes and thus information security is one of the most pressing issues facing organizations worldwide, influencing organizational sustainable information systems and business continuity [1]. However, many managers and employees do not pay sufficient attention to information security issues in their organizations [2]. As a result, the computer systems of most organizations are far less secure than they should be, and damages due to information security breaches are on the rise [3].

Employees are the weakest link in information security and the root cause of information security breaches, either because they engage in unethical activities in the workplace that threaten organizational information security or because they provide opportunities for computer hackers to attack or hack into their organization's computers [4,5]. However, few prior studies have attempted to understand employees' unethical behavior related to IT usage, especially from an ethical theory perspective [6], because of the lack of validated instruments to measure such behavior [7]. The objectives of this research were to (a) develop a short battery of self-report instruments for an assessment of unethical information security behavior and (b) establish a theoretical model linking factors affecting such behavior and its effects to employees' security efforts to maintain sustainable organizational information systems.

In order to understand unethical information security behavior, it is important to identify what constitutes such behavior and to develop instruments to measure it. Various types of security-related bad behavior on the part of employees have been identified, including computer abuse [8–10], information systems misuse [11–13], IT abuse [14], non-work-related computing [15,16], omissive behavior [17], and information security violation [18]. These studies have provided us with additional understanding on security-related bad behavior. However, most of these studies did not define such behavior or develop instruments to assess the behavior in question [7,19]. In addition, behavior may involve various degrees of intent, with some behavior involving serious acts such as theft or damage to computer terminals (computer abuse), unauthorized access to company data (information systems misuse), and computer hacking (IT abuse), which seldom occur within organizations and are difficult to observe. The main focus of this research is commonly found acts that are relatively easy to observe or monitor in the workplace, allowing the development of short self-report instruments to learn more about employees' efforts to protect organizational information security through their behavior. To integrate various types of security-related employee misbehavior, we followed Lewis [20], Mason [21,22], and Kaptein [23] to identify unethical information security behavior. One significant contribution of this research is its development of reliable and valid instruments to measure different types of unethical information security behavior in the workplace, which will be useful for researchers to examine the different properties of such behavior.

Another contribution of the current research is that it applies agency theory to an examination of how different deterrent controls can be used to reduce the occurrence of different types of unethical employee information security behavior and how such behavior can be used to predict employees' willingness to report information security incidents in the workplace. As the current research examines different types of unethical employee information security behavior, its findings can shed light on which types of such behavior exert a stronger influence on information security management for sustainable information systems, thus offering another contribution to the literature.

Previous research has tended to focus on the antecedents of a specific type of behavior: for example, some studies have examined the predictive factors of computer security behavior, including organizational factors such as security policies [13,24]; individual factors such as self-efficacy [25] or perceived threats [17]; and situational factors such as workload [26]. However, little empirical research or theoretical work has explicitly examined the link between employee behavior that may create a security threat to organizational information security and the protection of that security. Behavior is the purest reflection of an individual's priorities and feelings [27]. If employees' engagement in unethical information security behavior has a significantly negative effect on their efforts to protect their work computers or their organization's computer systems, then organizations can use effective indicators of such behavior to predict their efforts on information security in the workplace. Despite the factors affecting security behavior having been empirically evaluated, no investigation to date has examined the effects of unethical employee behavior on information security management. Another contribution of this research is to identify the relationships between typical types of unethical information security behavior and employees' willingness to report information security incidents.

The remainder of the article is structured as follows. We begin by identifying unethical information security behavior. We then develop instruments of such behavior that map onto the conceptual framework of unethical information security behavior established in the research. Next, we inquire into the causal relationships among deterrence controls, employees' unethical information security behavior and employees' willingness to report information security incidents. A discussion of the theoretical foundations, framework, hypotheses, research methods, and results is included. We then discuss the implications of the findings and directions for future research. In the final section, we present our conclusions.

2. Unethical Information Security Behavior

Lewis [20] (p. 381) defined business ethics as “rules, standards, codes, or principles which provide guidelines for morally right behavior and truthfulness in specific situation.” A number of studies in sociology, psychology, and organizational behavior have attempted to define a construct to measure unethical behavior in the workplace, for example, antisocial behavior [28], workplace deviance [29], employee vice [30], organizational misbehavior [31], workplace aggression and violence [32], organization-motivated aggression [33], organizational retaliation behavior [34], and noncompliant behavior [35]. However, none of these constructs captures unethical behavior in the realm of information security, which refers to the protection of information and the systems and hardware used to store and transmit that information [36].

Kaptein [23] suggested that unethical behavior in the workplace should be measured in five dimensions: unethical behavior toward financiers, customers, employees, suppliers, and society. He added that unethical workplace behavior may not bring or intend to bring harm, but it should still be considered misbehavior if fundamental interests are at stake. Kaptein [23] investigated unethical workplace behavior from the stakeholder perspective to give managers a better understanding of such behavior. However, information security-related unethical behavior was not considered. As an organization is a unit in which structures, technology (including information systems), people, and tasks are interrelated and mutually influential [37,38], and given the widespread use of computers and the Internet in today’s work environments, unethical information security behavior has become a major concern to organizations, which cannot be ignored.

Mason [21] suggested that privacy, accuracy, property, and accessibility are the four major ethical guidelines relevant to the use of computers and the handling of information. Privacy relates to the need to safeguard information, whereas accuracy relates to users’ responsibility to avoid misinformation. Property is concerned with the ownership of information and intellectual property rights, and accessibility with the right to obtain information. Violations of the above ethical guidelines will have negative effects on organizations. Banerjee et al. [39] and Leonard and Cronan [40] used these ethical guidelines to develop scenarios of unethical behavior in organizations, and Mason [22] further emphasized that such behavior affects organizations’ ability to pursue their goals.

Following Lewis [20], Mason [21,22], and Kaptein [23], we broadly define unethical information security behavior as voluntary employee behavior characterized by a failure to follow organizational rules, standards, codes, or principles that may affect the privacy, accuracy, property, and/or accessibility of information in the workplace. Employees who engage in unethical information security behavior may not have malicious intentions, but they may try to benefit themselves, such as saving time or accessing extra information to complete a task. The aim of this research was not to identify criminal behavior, which is unlikely to be committed by employees within organizations and is usually not observable. Therefore, acts that may constitute serious crimes in the workplace, such as cyberattacks [41], cybercrimes [42], computer crimes [43], and cyberterrorism [44], are beyond the scope of this article, although they can be considered forms of unethical information security behavior under the definition adopted herein. Our aim was to identify types of unethical information security behavior that are commonly found and relatively easy to observe or monitor in the workplace and to provide information that managers, who play crucial role in securing sustainable computing [45], can use to derive better security rules and policies for their employees. The research comprised two studies.

3. Study 1

In Study 1, we developed instruments which are the key constructs that we hypothesize to be foundational to unethical information security behavior in the workplace.

3.1. Development of Theoretical Types of Unethical Information Security Behavior

Little empirical research has focused on employees' unethical information security behavior in the workplace because of the sensitive nature of the topic [46] and the absence of valid instruments [7]. Therefore, our first step was to develop reliable and valid instruments to measure different types of unethical information security behavior in the workplace. We referred to the procedures for developing instruments recommended by Hinkin [47,48], whose paradigm comprises three major stages: (i) item generation, (ii) instrument development, and (iii) instrument evaluation. In the next two sections ("3.2. Instrument Generation" and "3.3. Instrument Development"), we discuss how we used both a qualitative method (authors' collective judgment) and a quantitative method (survey) to generated items and develop instruments. For the instrument evaluation, we assessed the reliability and validity of all of the instruments we developed before reporting our research findings in Study 2. In addition, to address the representativeness and practicality of the instruments, we integrate industry wisdom into the research discussed in the literature.

3.2. Instrument Generation

We first determined whether different types of unethical information security behavior are reflective constructs or formative constructs. Reflective constructs have observed measures that are influenced by an underlying latent construct, whereas formative constructs are a combination of multiple measures [49]. In a reflective construct, the correlation between any two measurement items should be positive [50]. Different types of unethical information security behavior are latent constructs, and we attempted to find observable activities to measure these constructs. The relationships between the measurement items (observable activities) and their respective constructs (different types of unethical information security behavior) are reflective. Previous studies have found that if an employee engages in workplace behavior that belongs to a particular behavioral family, he or she has a greater tendency to engage in other forms of behavior within that family than in a behavior within another family [29,51]. The implication is that any two forms of behavior within the same family are highly positively correlated, and thus the relationship between the measurement items and respective constructs for particular types of behavior are reflective in nature. This idea is reflected in one of the decision rules related to correlation among the items used to identify constructs as reflective [52]. The other three decision rules in Javis et al. [52] are direction of causality, interchangeability of items, and nomological item net. Items are manifestations of the construct, and thus we expected a principal factor (reflective) model. In addition, the items have similar content and dropping an indicator will not alter the conceptual domain of the construct. Moreover, we expected the same antecedents and consequences for the items since the items refer to different activities of unethical employee information security behavior. On the basis of the arguments above, we can determine that different types of unethical information security behavior are reflective constructs.

Drawing on the literature, we used content analysis to identify different types of unethical information security behavior in the workplace, and compiled a list of typical activities for use in the development of our instruments. We identified studies of unethical information security behavior that affects information security within organizations using the research article identification methodology suggested by Webster and Watson [53], which includes three search stages—journal database, citations of identified articles, and the Social Sciences Citation Index and the Web of Science. We first searched the ABI/Inform Global database using the key words: "information security," "unethical behavior," AND "organization" for the period up to 2018. We then used the citations in the identified articles as further sources. Finally, we searched the Social Sciences Citation Index and the Web of Science to identify additional candidate articles. After reviewing all articles from the search results, we found 36 peer-reviewed articles, but only two of which [7,54] developed instruments for the type of behavior studied. These results support the observation in Mahmood et al. [55] that a lack of understanding of bad behavior affects academic discipline growth in information security research. We carefully read all the 36 articles and attempted to classify the actions studied into different types of unethical information security behavior based on similarities in content according to the authors' collective judgment. Four major types of unethical information security behavior were identified: (i) misbehavior in networks/applications; (ii) dangerous Web use; (iii) omissive security behavior; and (iv) poor access control. Each of the four types is discussed in the following paragraphs. A complete list of the articles consulted is provided in Appendix A.

3.2.1. Misbehavior in Networks/Applications

The activities in this category focus on the misuse of networks and/or applications in the workplace. Such misbehavior has been problematic since at least the 2000s [56] and is a common unethical workplace behavior [57]. Misbehavior in networks/applications is a problem within organizations as it may provide opportunities for outsiders to attack or otherwise harm an organization's computers and lead to company information loss and leakage to third parties, thereby threatening the privacy, property, and accessibility of company information. In addition, by definition, misbehavior in networks/applications involves the use of illegal software, which affects the privacy of information and is a common workplace problem [58,59]. Employees engage in misbehavior in networks/applications mainly because they want to receive personal benefits such as time savings [57].

3.2.2. Dangerous Web Use

The activities involved in dangerous Web use are related to misuse of the Internet. Employees' personal Web use refers to non-work-related use of the Internet for personal purposes at work, and this is a common but relatively new form of unethical behavior in the workplace [60]. According to Websense [61], about two thirds of the employees it surveyed admitted to spending time on personal Internet surfing using office computers, with the average amount of time spent on such activity being around three hours per week. However, some researchers [62,63] have suggested that allowing employees to use the Internet for personal reasons in a supervised manner can make them more creative and productive. In other words, personal Web use may be beneficial to organizations if properly supervised. Therefore, under our definition of unethical information security behavior, employees' personal Web use cannot be counted as unethical information security behavior if employees surf the Internet with great care and such use does not affect the privacy, accuracy, property, or accessibility of company information. However, if employees use the Web dangerously, for example, to view suspicious websites, that act immediately becomes an example of unethical information security behavior. It is because suspicious websites are often sources of malware and scams that such behavior could result in the leakage of company information or the hacking of a company's computer system, thereby posing an information security threat to the organization. Dangerous Web use is therefore a type of unethical information security behavior that affects the property and accessibility of company information. In addition, if employees are not allowed to surf the Web at all in their workplace (i.e., all personal use of the Internet is prohibited), then any Internet use for personal reasons constitutes dangerous Web use under our definition of unethical information security behavior as such behavior is not compliant with organizational policies [64]. Employees can receive personal benefits via dangerous Web use: for example, downloading music files from suspicious websites for enjoyment [65].

3.2.3. Omissive Security Behavior

Previous studies have attempted to study this type of unethical behavior. Workman et al. [17] investigated omissive security behavior, which occurs when employees who know how to protect company information fail to do so. It concerns the "knowing–doing" gap in information security. Employees who engage in this type of behavior may not intend to damage their organizational computer systems, but they are not security conscious [7]. However, such behavior can dangerously affect the availability, confidentiality, and integrity of information as the omissive activities involved can cause information leakage, which in turn threatens the property of the company information. As Workman et al. [17] (p. 2813) emphasized, "omissive security behavior threatens the integrity of mission-critical systems and needs to be seriously addressed." Omissive security behavior covers a broad variety of employee activities, such as leaving printouts unattended in the office or forgetting to back up computer systems. To have a more specific range of behaviors for research, we considered only omissive security behavior that is related to employees' bad habits when using computers or handling data during daily operations. Password- or access-related behavior was excluded as it is included in the poor access control type of behavior. We consider omissive security behavior to be a relatively unconscious form of physical behavior that causes information leakage. Employees commit such behavior mainly because it is convenient to do so or because of bad habits, not because they are seeking personal benefits or attempting to damage organizational security systems.

3.2.4. Poor Access Control

Access control is strongly related to information security vulnerability [66] and information privacy [67]. A successful access control approach safeguards information security and prevents unauthorized access to company data [68]. In contrast, poor access control violates company rules on data security. Poor access control involves not only the inadequate control of data security, such as unauthorized access, but also weak data protection measures such as bad password practices. Both types of behavior can result in information leakage. Many studies have found that employees do not have good protection measures in place to protect the information on their work computers and tend to create simple and easy-to-remember passwords for convenience [69]. Some employees even leave written passwords in visible places, such as on post-it notes stuck to their monitors [70]. Although employees usually do not receive instant personal benefits from committing such behavior, poor access control is a physical type of unethical information security behavior that can lead to the improper access of company information by unauthorized users.

3.3. Instrument Development

After compiling a list of typical activities on the basis of the literature, we used a quantitative method by conducting an industry Web-based survey to refine the instruments. The survey participants were 50 IT professionals and 50 non-IT professionals from a variety of organizations in the public and private sectors. They indicated, on a 7-point Likert scale, the extent to which they had engaged in each form of behavior in the past year. The scale anchors were (1) never, (2) almost never, (3) a very few times, (4) occasionally, (5) often, (6) quite often, and (7) very many times. In addition, they were also asked to suggest any other activities in the behavior that had not been covered in the list.

The industry survey showed that the list is representative as no respondent suggested any other activities. As our aim was to create practical and representative constructs for unethical information security behavior that can be applied to various industries and occupations, we referred to Chu and Chau [7] and removed some items that had an extremely low frequency of self-report occurrences of the unethical information security behavior in question. The final instruments contained 13 items in total: four for misbehavior in networks/applications, three for dangerous Web use, three for omissive security behavior, and three for poor access control. These items are presented in Table 1. Instrument validation is discussed in Study 2.

Table 1. Items for misbehavior in networks/applications, dangerous Web use, omissive security behavior, and poor access control.

Misbehavior in Networks/Applications	
1.	Using untrusted networks for company data transmission at work (RES1).
2.	Installing untrusted applications for personal purposes on work computer (RES2).
3.	Running untrusted applications for personal purposes on work computer (RES3).
4.	Connecting work computer to unauthorized wireless networks (RES4).

Table 1. *Cont.*

Dangerous Web Use
1. Browsing suspicious websites using work computer (DWU1). 2. Forwarding suspicious Web links to colleagues at work (DWU2). 3. Downloading files from suspicious websites using work computer (DWU3).
Omissive Security Behavior
1. Not locking work computer from preventing unauthorized use when away (OSB1). 2. Leaving removable storage devices unattended in office (OSB2). 3. Leaving printouts unattended in office (OSB3).
Poor Access Control
1. Allowing non-employees to freely use work computer (PAC1). 2. Using easy-to-guess passwords at work (PAC2). 3. Writing down personal passwords in visible places in office (PAC3).

4. Study 2

In Study 2, we applied agency theory [71,72] to develop a research model to investigate the antecedents and consequences of unethical information security behavior. The research model is depicted in Figure 1.

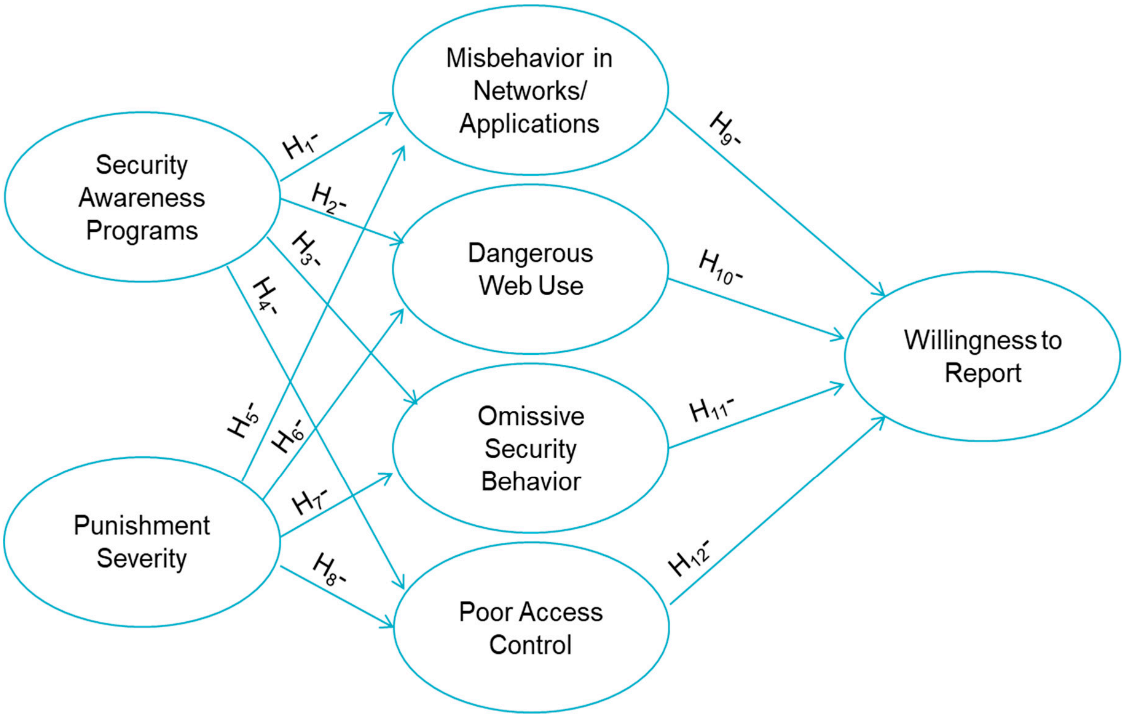

Figure 1. Research model.

4.1. *Theoretical Framework and Hypotheses*

Information security is important to organizations, and therefore employers expect their employees to secure the IT and sustainable environment and protect organizational computer systems from being hacked or attacked. Employers do not want their employees to engage in any unethical information security behavior as such behavior may create security breaches in computer systems and lead to data leakage. However, employees may engage in unethical behavior out of self-interest, disregarding information security issues. As a result, there may be a goal conflict between employees and employers in relation to information security issues [73]. Agency theory, which describes the structuring of economic exchange relationships between principal (a person or organization who employs another party to conduct specific work) and agent (who conducts that work), suggests that a conflict of interests between these two parties may lead to the moral hazard problem because of information asymmetry; as the agent has more information than the principal and the agent's behavior cannot be easily observed, the agent may engage in behavior that is not favorable to the principal and that cannot be monitored by the principal perfectly and without cost [74,75].

Numerous researchers have adopted agency theory to study ethics issues or risk-related problems. For instance, Hannafey and Vitulano [76] applied the agency theory to understand executive coaching practice and its ethical dimension, providing a needed ethical grounding and basis for moral thinking about executive coaching. Bahli and Rivard [77] made good use of agency theory to study the risks of outsourcing IT, finding that such risks arise from the incongruent goals of the parties involved in such outsourcing. However, relatively few researchers have used the agency theory to study empirically the conflict of employees and employers in the context of information security behavior. In the current research, we investigated factors affecting different types of unethical information security behavior, which in turn influence employees' willingness to report information security incidents.

Agency theory has three human assumptions: self-interest, bounded rationality, and risk aversion [71]. Previous studies tended to investigate the use of incentives to motivate people and suggested that incentives are useful to control a behavior of rational self-interested agents [71,78,79]. However, some researchers [80] have opposed the use of incentives, especially monetary incentives, in controlling an agent's behavior because it will somewhat "coarsen" humanity. In our study, we attempted to examine deterrence controls that we can use to motivate employees not to engage in unethical information security behavior by stressing the altruism and risk aspects, instead of using incentives.

4.1.1. Altruism and Awareness

Altruism is the concern for others' well-being. Although agency theory suggests that people are self-interested, there is nothing inconsistent between self-interested behavior and altruistic behavior as people are seldom perfect agents and can make decisions with concern both for themselves and for another, including an employer or principal [79]. It is commonly believed that employees' awareness is an important security countermeasure to curb employee-caused security breaches and enhance organizational information security performance [81–84], and we expect that information security awareness programs, which aim to increase employees' awareness of their responsibilities in regard to their organization's information resources and the consequences of misusing such resources and to provide employees with the necessary skills to help fulfill these responsibilities, can encourage employees' altruistic tendencies and educate employees on concerns regarding the company's information security management (group interests). Some researchers have adopted a hypothetical scenario method to study the influence of information security awareness programs on intention to misuse information systems; these studies found that such programs are useful in reducing employees' information systems misuse [11–13]. Nevertheless, we still do not know how information security awareness programs influence employees' actual unethical behavior with respect to information systems and what effects they have on different types of such behavior. Therefore, we propose the following hypotheses:

Hypothesis 1. *Information security awareness programs are negatively associated with an employee's misbehavior in networks/applications.*

Hypothesis 2. *Information security awareness programs are negatively associated with an employee's dangerous Web use.*

Hypothesis 3. *Information security awareness programs are negatively associated with an employee's omissive security behavior.*

Hypothesis 4. *Information security awareness programs are negatively associated with an employee's poor access control.*

4.1.2. Risk and Punishment

Agency theory states that agents do not like risk and will not accept options where the risk is not fully compensated. To decrease the risk of engaging in deviant behavior, the analysis of the use of punishment has recently been applied in the agency theory context [78]. Previous studies have investigated the effect of punishment on the intention to engage in a specific type of unethical behavior, such as software piracy [59], information systems misuse [13,85], and unethical IT use [6]. Nevertheless, few have studied how punishment severity influences different types of actual employee unethical information security behavior. We expect that employees are less likely to engage in such behavior if they perceive the penalty to be serious. Similarly, if employees perceive the penalty to be minor, they are more likely to engage in the behavior. Therefore, we test the following hypotheses:

Hypothesis 5. *Punishment severity is negatively associated with an employee's misbehavior in networks/applications.*

Hypothesis 6. *Punishment severity is negatively associated with an employee's dangerous Web use.*

Hypothesis 7. *Punishment severity is negatively associated with an employee's omissive security behavior.*

Hypothesis 8. *Punishment severity is negatively associated with an employee's poor access control.*

4.1.3. Conflict of Interest in Reporting Information Security Incidents

Information security incidents refer to any security-related adverse events involving a loss of data confidentiality, disruption of data or system integrity, or disruption or denial of availability [86]. The Hong Kong Computer Emergency Response Team Coordination Center (www.hkcert.org) provides the following examples of such incidents: malware installation, Web defacement, phishing, scams, denial of service attacks, malicious codes, and unauthorized access. Such incidents may affect the IT system to operate continuously and organizations cannot afford it [87]. If an information security incident is observed, the employee who observes it should report the incident to management to minimize potential losses and reduce the effect on business operations. However, owing to a goal conflict between employees who engage in unethical information security behavior and employers concerned with information security, it is expected that employees may have a tendency not to report information security incidents as they may be afraid of the company discovering their own unethical information security behavior or even tracking back and blaming them for engaging in such behavior once incidents are reported. In addition, only the employee knows whether he/she observes the incident. Due to information asymmetry, the employee may engage in behavior that is favorable to him/her rather than the employer and is less willing to report the incident. Therefore, we propose the following hypotheses:

Hypothesis 9. *Misbehavior in networks/applications is negatively associated with an employee's willingness to report information security incidents.*

Hypothesis 10. *Dangerous Web use is negatively associated with an employee's willingness to report information security incidents.*

Hypothesis 11. *Omissive security behavior is negatively associated with an employee's willingness to report information security incidents.*

Hypothesis 12. *Poor access control is negatively associated with an employee's willingness to report information security incidents.*

5. Method

A Web-based survey consisting of the 13 items shown in Table 1, two items measuring company's information security awareness program based on D'Arcy and Hovav [11], three items measuring punishment severity based on D'Arcy and Hovav [24], and three items measuring willingness to report information security incidents with reference to Hassan et al. [88] was conducted. Subjects were asked to complete two tasks. First, they were required to indicate on a 7-point Likert scale the extent to which they had engaged in the 13 types of unethical behavior in the past year. The scale anchors were (1) never, (2) almost never, (3) a very few times, (4) occasionally, (5) often, (6) quite often, and (7) very many times. Second, they were required to assess on a 7-point Likert scale (1 = strongly disagree; 7 = strongly agree) their company's information security awareness program, the severity of punishment for unethical information security behavior, and their willingness to report information security incidents. The information security awareness program items were "My organization provides training to help employees improve their awareness of computer and information security issues" (SAP1) and "My organization educates employees on their computer security responsibilities" (SAP2). The items for punishment severity were "If I were caught engaging in unethical employee information security behavior, I would be severely reprimanded" (PUN1), "I would probably be caught eventually after engaging in unethical employee information security behavior" (PUN2), and "If caught engaging in unethical employee information security behavior, my punishment would be severe" (PUN3). The items for willingness to report were "I feel comfortable reporting information security incidents to my organization" (WTR1), "I am willing to report to my direct manager about information security incidents" (WTR2), and "I am willing to report information security incidents to upper management" (WTR3).

5.1. Data Collection

To ensure the quality of the Web-based survey, it was pretested on 20 employees from various industries before the main field survey. The pretest results showed that respondents were able to answer all of the survey questions without difficulty, and only a few minor modifications were made to the wording of the introduction to the survey after the pretest. A link to the final version of the Web-based survey with a covering letter stating the purpose of the survey, an information sheet defining the key terms, and a password to access the survey were e-mailed to 1000 employees who used computers in the workplace. Target respondents were selected from a database of a marketing research company with substantial experience in conducting information security surveys. A total of 210 usable responses were obtained, representing a response rate of 21%. Of these respondents, 112 were male (53%), 181 were degree holders (86%), and 70 held managerial positions (30%). They came from various industries, including financial services (23%), transportation, information, and communications (22%), education (19%), manufacturing (8%), wholesale and retail (8%), social and personal services (6%), and other (14%).

5.2. Instrument Validation

Table 2 lists the means, standard deviations, and participation rates of all items. The participation rates for misbehavior in networks/applications, dangerous Web use, omissive security behavior, and poor access control were all quite high (ranging from 41.9% to 93.8%), indicating that many of the respondents engaged in these types of behavior at least once in the year before the survey.

Table 2. Descriptive statistics and factor loadings of measurement items.

Construct	Item	Mean	S.D.	No. of "Never"	Participation Rate *
Misbehavior in Networks/Applications	RES1	2.448	1.387	55	73.8%
	RES2	2.210	1.292	78	62.9%
	RES3	2.257	1.257	72	65.7%
	RES4	2.057	1.290	94	55.2%
Dangerous Web Use	DWU1	1.695	1.050	122	41.9%
	DWU2	1.748	1.237	118	43.8%
	DWU3	1.905	1.320	107	49.0%
Omissive Security Behavior	OSB1	4.076	1.826	13	93.8%
	OSB2	2.790	1.439	42	80.0%
	OSB3	3.024	1.262	23	89.0%
Poor Access Control	PAC1	1.938	1.145	93	55.7%
	PAC2	2.643	1.503	56	73.3%
	PAC3	1.814	1.084	100	52.4%
Information Security Awareness Programs	SAP1	4.267	1.368		
	SAP2	4.376	1.358		
Punishment Severity	PUN1	4.462	1.620		
	PUN2	4.429	1.546		
	PUN3	4.310	1.378		
Willingness to Report	WTR1	5.129	1.236		
	WTR2	4.986	1.288		
	WTR3	4.871	1.001		

N = 210. * Percentage of respondents who indicated that they had engaged in the behavior at least once in the past year.

SmartPLS 3 was used for the data analysis. We used partial least squares (PLS), a structural modeling technique, to analyze the data because the item responses were not normally distributed. PLS makes fewer demands regarding the distribution of the underlying data [24,89]. To show the predictiveness of a model, Chin [89] also recommended that an item in a construct should have a factor loading of 0.7 or above. All of the items in the misbehavior in networks/applications, dangerous Web use, omissive security behavior, and poor access control categories fulfilled this criterion (see Table 3). The findings supported the use of the four types of behavior as distinct constructs and suggested the items in each construct are useful for measuring that construct.

We assessed the internal consistency, reliability, convergent validity, and discriminant validity of the constructs by looking at the Cronbach's alpha, composite reliability (CR), factor loadings, average variance extracted (AVE), and square root of the AVE of each. The Cronbach's alpha values of the constructs ranged from 0.696 to 0.973, which suggests that the constructs had satisfactory internal consistency [90]. The CR of each construct was above 0.7, the benchmark for acceptable reliability [91]. With regard to convergent validity, all of the factor loadings exceeded 0.7 (see Table 3), and the AVE for each construct was larger than 0.5, showing that the items satisfied the convergent validity criterion [92,93]. Regarding discriminant validity, the square root of the AVE of each construct exceeded the construct's correlations with all of the other constructs [93]. These results demonstrated the satisfactory reliability and validity of the constructs. Table 4 presents the Cronbach's alpha, CR, AVE, and cross-correlations of all the constructs.

Table 3. Cross loadings.

	Information Security Awareness Program	Punishment Severity	Willingness to Report	Misbehavior in Networks/Applications	Dangerous Web Use	Omissive Security Behavior	Poor Access Control
SAP1	**0.986**	0.528	0.532	−0.153	−0.277	−0.425	−0.384
SAP2	**0.988**	0.542	0.501	−0.173	−0.314	−0.445	−0.388
RES1	−0.156	−0.306	−0.132	**0.820**	0.628	0.221	0.266
RES2	−0.054	−0.309	−0.039	**0.923**	0.641	0.159	0.298
RES3	−0.077	−0.297	−0.067	**0.905**	0.627	0.101	0.276
RES4	−0.280	−0.229	−0.203	**0.768**	0.625	0.257	0.477
DWU1	−0.088	−0.231	−0.090	0.683	**0.755**	0.194	0.324
DWU2	−0.229	−0.371	−0.218	0.659	**0.856**	0.200	0.406
DWU3	−0.345	−0.344	−0.313	0.586	**0.856**	0.314	0.496
OSB1	−0.414	−0.248	−0.390	−0.080	0.031	**0.768**	0.306
OSB2	−0.294	−0.316	−0.272	0.338	0.384	**0.826**	0.294
OSB3	−0.305	−0.257	−0.241	0.346	0.350	**0.761**	0.319
PAC1	−0.337	−0.333	−0.299	0.386	0.535	0.317	**0.790**
PAC2	−0.320	−0.307	−0.270	0.289	0.320	0.309	**0.800**
PAC3	−0.285	−0.352	−0.248	0.257	0.372	0.316	**0.828**
WTR1	0.521	0.531	**0.953**	−0.131	−0.276	−0.372	−0.365
WTR2	0.489	0.532	**0.947**	−0.106	−0.246	−0.385	−0.299
WTR3	0.452	0.423	**0.880**	−0.122	−0.255	−0.345	−0.274
PUN1	0.519	**0.961**	0.491	−0.329	−0.363	−0.298	−0.401
PUN2	0.547	**0.931**	0.555	−0.293	−0.366	−0.347	−0.355
PUN3	0.465	**0.927**	0.469	−0.348	−0.388	−0.331	−0.399

Table 4. Cronbach's alpha, composite reliability, average variance extracted, and cross-correlations of the constructs.

Construct	α	CR	AVE	1	2	3	4	5	6	7
1. Misbehavior in Networks/Applications	0.849	0.901	0.697	**0.835**						
2. Dangerous Web Use	0.776	0.863	0.679	0.756	**0.824**					
3. Omissive Security Behavior	0.696	0.828	0.617	0.219	0.296	**0.785**				
4. Poor Access Control	0.731	0.848	0.650	0.388	0.512	0.390	**0.806**			
5. Information Security Awareness Programs	0.973	0.987	0.974	−0.165	−0.300	−0.441	−0.391	**0.987**		
6. Punishment Severity	0.934	0.958	0.883	−0.345	−0.397	−0.346	−0.410	0.542	**0.940**	
7. Willingness to Report	0.918	0.948	0.860	−0.129	−0.410	−0.396	−0.339	0.509	0.536	**0.927**

* α = Cronbach's alpha; CR = composite reliability; AVE = average variance extracted. Diagonal elements represent the square root of AVE. N = 210.

6. Results

Nine of our 12 hypotheses were supported. Consistent with hypotheses 3 to 4 and hypotheses 5 to 8, information security awareness programs were negatively related to employees' omissive security behavior (β = −0.359, $p < 0.001$) and poor access control (β = −0.239, $p < 0.05$), while punishment severity was negatively related to employees' misbehavior in networks/applications (β = −0.361, $p < 0.001$), dangerous Web use (β = −0.331, $p < 0.001$), omissive security behavior (β = −0.151, $p < 0.05$), and poor access control (β = −0.281, $p < 0.001$). In addition, dangerous Web use (β = −0.247, $p < 0.05$), omissive security behavior (β = −0.299, $p < 0.001$), and poor access control (β = −0.169, $p < 0.05$) were negatively related to employees' willingness to report information security incidents, thus supporting hypotheses 10 to 12. However, information security awareness programs did not have significant relationships with either misbehavior in networks/applications (β = 0.03, $p > 0.05$) or dangerous Web use (β = −0.120, $p > 0.05$), and misbehavior in networks/applications did not have a significant relationship with employees' willingness to report information security incidents (β = 0.118, $p > 0.05$); thus, hypotheses 1, 2, and 9 were not supported. In short, punishment severity reduced the occurrence of the four types of unethical information security behavior but information security awareness programs only reduced the occurrence of omissive security behavior and poor access control. Moreover, dangerous Web use, omissive security behavior, and poor access control predicted employees' willingness to report information security incidents, but misbehavior in networks/applications did not. Table 5 summarizes the results of the hypothesis testing.

Table 5. Results of hypothesis testing.

Hypothesis	Path Coefficient	*p*-Value	Supported?
H1 (-): *Awareness Programs → Misbehavior in Networks/Applications*	0.030	>0.05	No
H2 (-): *Awareness Programs → Dangerous Web Use*	−0.120	>0.05	No
H3 (-): *Awareness Programs → Omissive Security Behavior*	−0.359	<0.001	Yes
H4 (-): *Awareness Programs → Poor Access Control*	−0.239	<0.05	Yes
H5 (-): *Punishment Severity → Misbehavior in Networks/Applications*	−0.361	<0.001	Yes
H6 (-): *Punishment Severity → Dangerous Web Use*	−0.331	<0.001	Yes
H7 (-): *Punishment Severity → Omissive Security Behavior*	−0.151	<0.05	Yes
H8 (-): *Punishment Severity → Poor Access Control*	−0.281	<0.001	Yes
H9 (-): *Misbehavior in Networks/Applications → Willingness to Report*	0.118	>0.05	No
H10 (-): *Dangerous Web Use → Willingness to Report*	−0.247	<0.05	Yes
H11 (-): *Omissive Security Behavior → Willingness to Report*	−0.299	<0.001	Yes
H12 (-): *Poor Access Control → Willingness to Report*	−0.169	<0.05	Yes

7. Discussion

Although there is tremendous interest in the role that employees play in information security management for sustainable information systems in the workplace, relatively few research studies of employees' security-related behavior, particularly the dark side of such behavior, have been carried out [25,55]. Drawing upon agency theory, the two-study research reported herein investigated how information security awareness programs and punishment severity affect the four typical types of unethical information security behavior and in turn how they predict employees' willingness to report information security incidents.

7.1. Theoretical Implications

The research extends the agency theory to study empirically the goal conflict of employees and employers and confirms its applicability to the unethical workplace behavior domain. In addition, it is one of the very few empirical examinations of unethical information security behavior. Our development of four instruments makes an important contribution to future research on unethical information security behavior by providing a means to measure it, thus facilitating its empirical study and theoretical investigation. D'Arcy and Hovav [11] reported that research on information security behavior has produced conflicting results. For example, some researchers e.g., [94] have found security policies to have little or no impact on the misuse of information systems, whereas others e.g., [11,13] have suggested a significant impact. Our findings may provide an answer to why this has been the case. One possible reason may be the selection of the types of behavior studied. Therefore, knowledge about the characteristics of different types of unethical information security behavior is important. Our research not only provides a response to Siponen and Vance's [19] request for instruments of this type of behavior, but is also a good starting point for developing theoretical models for such behavior.

Previous studies have suggested that information security awareness programs and punishment severity prevent security incidents in organizations e.g., [11,13], but few have investigated and compared to what extent information security awareness programs and punishment severity improve information security in organizations. Our results suggest that the degree of usefulness of information security awareness programs in preventing the four types of behavior differs: Information security awareness programs prevent employees' omissive security behavior and poor access control but have no relationships with employees' misbehavior in networks/applications and dangerous Web use.

To the best of our knowledge, this study is pioneer research that demonstrates that unethical information security behavior can be used to predict employees' attitudes (willingness to report information security incidents). The research findings generally provide support for the supposition that employees devote less effort to maintaining an organization's information security if they engage in unethical information security behavior.

7.2. Practical Implications

One important practical implication of the findings is that some types of unethical behavior, including dangerous Web use, omissive security behavior, and poor access control, diminish employees' willingness to report incidents. Of these three types of behavior, omissive security behavior displayed the strongest negative correlation. Very often, employees do not tell their managers directly about their efforts to protect the organization's computer systems. However, their behavior may reveal the degree of their efforts. If managers find that their employees frequently engage in dangerous Web use, omissive security behavior, and/or poor access control, that discovery constitutes a warning signal that their employees are less willing to bolster information security, thus possibly leading to security breaches. We should note an interesting and unexpected finding that misbehavior in networks/applications does not have a significant relationship with employees' efforts to maintain information security. In other words, this type of misbehavior cannot predict employees' willingness to report information security incidents.

The research findings show that information security awareness programs are not strong enough to reduce the types of unethical information security behavior that bring employees personal benefits, such as misbehavior in networks/applications and dangerous Web use, but they can increase altruistic values so that employees consider the company's benefit as a whole and therefore would be more likely to choose not to engage in unethical information security behaviors, such as omissive security behavior and poor access control, that are, relatively speaking, for convenience. Regarding punishment severity, it prevents all four types of unethical information security behavior, but, relatively, its degree of usefulness is stronger for employees' misbehavior in network/applications and dangerous Web use and weaker for employees' omissive security behavior and poor access control. This may imply that employees have a perception that misbehavior in network/applications and dangerous Web use are relatively serious unethical information security behaviors but omissive security behavior and poor access control are minor behaviors. The findings are useful for managers seeking to develop suitable information security strategies to tackle different problems related to unethical information security behavior.

Deterrent controls aim to dissuade employees from committing unethical behavior with regard to information systems [95]. Passive deterrents may include guidelines, policies, and education, whereas active deterrents may involve punishment. The findings of this research may suggest that passive deterrents are relatively useful for reducing the occurrence of omissive security behavior and poor access control but less effective in controlling misuse of networks/applications and dangerous Web use. If management does not want their employees to engage in all these activities, they should implement security measures beyond simply providing security training and education to their employees. It is recommended that management enforces active deterrent controls that state clearly the costs and risks associated with such behavior (e.g., getting punished after being caught) rather than just providing training for their employees. From the agency theory perspective, employees pay more attention to information security management when their goals are aligned with the organizational goals for information security. It is recommended that management share the organization's values and goals concerning information security with their employees in a formal and serious way. Management may also consider developing information security targets for employees to follow to achieve goal alignment in order to increase employees' willingness to play their part in organizational information security management.

The research findings presented in Table 2 suggest that many employees engage in unethical information security behavior, and the relatively high participation rates for the different forms of such behavior studied here (particularly those activities in the omissive security behavior arena) provide empirical support for the argument that employees are a critical factor in maintaining sustainable organizational information security that management cannot afford to neglect [25].

8. Limitations and Future Research

Like most empirical research, this research has limitations that warrant further consideration. One limitation is that the instruments used to measure the four types of unethical information security behavior do not encompass all possible activities. We had to make trade-offs between ensuring reliability and ensuring that all unethical activities were covered. To ensure reliability, we decided to eliminate items with low frequencies and only include relatively common activities. We balanced these aims for two major reasons. First, previous research has found that if an employee engages in workplace behavior that belongs to a particular behavioral family, he or she has a greater tendency to engage in other forms of behavior within that family than in a behavior within another family [29,51]. This logic suggests that an instrument measuring types of unethical information security behavior does not need to include a complete set of possible activities for each type. Second, if we had not eliminated certain items, the instrument would have lacked reliability and thus would have less practical value for other researchers. Therefore, we followed a rigorous instrument development process to ensure reliability and applicability to other research. To reconfirm the reliability and validity of all the constructs, we calculated the CR and AVE and found high values for both, indicating the satisfactory reliability and validity of the constructs. In addition, to make sure that the items were representative of their respective instruments and can be broadly applied to a variety of organizational contexts and occupations, we not only compiled measurement items from the literature but also consulted industry players to verify the items.

Another limitation is the use of self-report data, which may lead to common method variance (CMV) and social desirability biases. We tried to avoid CMV by adopting ex ante approaches in the research design stage, including using diverse samples and assuring anonymous responses and the confidentiality of the study, as well as using different sources of information for different constructs [96]. In an examination of the effect of CMV on the inferences drawn from survey research in the information systems area, Malhotra et al. [97] found that such biases are not substantial, even though CMV is present. Furthermore, concerns about social desirability biases may be unwarranted because, according to the meta-analysis of Ones et al. [98], self-report criteria tend to result in higher estimates of validities than external measures of counterproductive behavior. Besides ex ante approaches, research may consider using statistical remedies such as the marker variable technique to detect and reduce CMV [99,100]. The high participation rate in unethical information security behavior reported by the respondents in Study 2 suggests that the respondents who answered our questionnaire were willing to admit to engaging in unethical behavior in the workplace. Therefore, it is our belief that a self-report questionnaire is a sound scientific method of collecting primary data as long as respondents are assured of anonymity. Nevertheless, future research should investigate the potential biases between actual and reported behavior and develop a methodology such as using randomized response technique to reduce response distortion due to social desirability [101–103].

This research has demonstrated how information security awareness programs and punishment severity affect the four typical types of unethical behavior in organizations and, in turn, how they can be used to predict employees' willingness to report information security incidents. The results suggest two future research directions. One fruitful research direction is to fit different structural equation models to demographic groups defined by, such as, different gender groups. For example, besides deterrent controls, security measures designed to protect organizations, such as preventive controls which use technology (e.g., the use of security software and access management) to increase the costs of committing unethical employee information security behavior [104], could be included in the model to compare the relative importance of deterrent controls and preventive controls in reducing the occurrence of such behavior. In this research, we focused on commonly found types of unethical information security behavior. Other types of such behavior and their relationships with employees' willingness to report information security incidents could also be considered.

9. Conclusions

The sustainability of the information systems that speeds up the decision-making processes drives sustainable business [68]. Unethical information security behavior in the workplace has long been an important research topic on information security management to maintain sustainable information systems. This article develops instruments for misbehavior in networks/applications, dangerous Web use, omissive security behavior, and poor access control to measure such behavior. In addition, we adopt agency theory to examine the influences of information security awareness programs and punishment severity on the four types of behavior in terms of influencing information security management and, in turn, whether they exert negative effects on employees' willingness to report information security incidents. Our results suggest that information security awareness programs prevent omissive security behavior and poor access control while punishment severity is more effective in reducing misbehavior in networks/applications and dangerous Web use. In addition, employees' dangerous Web use, omissive security behavior, and poor access control have a significant negative effect on their willingness to report incidents. However, employees' misbehavior in networks/applications has no significant effects on willingness to report incidents. From a theoretical perspective, this article takes the lead in investigating the effects of information security awareness programs and punishment severity on four different types of unethical information security behavior and, in turn, whether they predict employees' willingness to report information security incidents. In addition, the developed instruments can further facilitate empirical studies for understanding the factors affecting such behavior. Concerning the managerial implications, the findings will help managers to understand the different manifestations of unethical information security behavior and develop better security strategies to maintain sustainable information systems.

Author Contributions: Conceptualization, A.M.Y.C.; methodology, A.M.Y.C. and M.K.P.S.; formal analysis, A.M.Y.C.; data curation, A.M.Y.C.; writing, A.M.Y.C. and M.K.P.S. All authors have read and agreed to the published version of the manuscript.

Funding: This research was partially funded by the Research Grants Council of the Hong Kong Special Administrative Region, grant number UGC/FDS14/P05/16.

Acknowledgments: The authors would like to thank the editor and the three anonymous reviewers for their valuable suggestions and comments.

Conflicts of Interest: The authors declare no conflict of interest.

Appendix A Unethical Information Security Behavior in the Workplace

Profile	Article	Name Given to Profile in the Article	Definition (if any)	Examples/Activities Studies	Intent	Any Instruments Developed?
Misbehavior in Networks/ Applications	Harrington [94], Lee et al. [8], Lowry et al. [105], Posey et al. [9,10], Straub [104], Straub and Nance [106], Willison and Warkentin [84]	Computer abuse	"The unauthorized and deliberate misuse of assets of the local organizational information system by individuals, including violations against: hardware, programs, data, and computer service" [104] (p. 257).	Theft or damage to terminals, CPUs, disk drives, and printers, theft or modification of programs, embezzlement or modification of data, and unauthorized use of service or purposeful interruption of service.	Self-benefiting, but can be malicious, which does not match with our definition.	No
Misbehavior in Networks/ Applications, Poor Access Control	D'Arcy and Hovav [11,12], D'Arcy et al. [13], Hovav and D'Arcy [107]	Information systems misuse	"A behavior that is defined by the organization as a misuse of IS resources" [13] (p. 4).	Password sharing, inappropriate use of e-mail, software piracy, unauthorized access to company data, and unauthorized modification of company data.	Self-benefiting	No
Misbehavior in Networks/ Applications, Dangerous Web Use	Campbell and Lu [14]	Information technology abuse	"The personal use of a work computer that violates formal organizational policies or informal norms and generates potential legal or ethical consequences" (p. 2).	Negligent use: downloading illegal content, making illegal copies of software, and sending sexually explicit jokes. Corrupt use: computer hacking, theft of confidential data, and viewing sexually explicit content. Nonproductive use: using personal e-mail or chat, and conducting personal business. Counterproductive use: moonlighting (working on outside projects).	Self-benefiting, but can be malicious which does not match with our definition.	No
Misbehavior in Networks/ Applications, Dangerous Web Use	Liao et al. [108]	Internet misuse	"Any voluntary acts of employees using their companies' Internet access during office hours to surf non-job-related websites for personal purposes and to check personal emails" (p. 50).	Browsing non-work-related websites or taking time to check personal e-mails, moonlighting for additional income, downloading or transmitting confidential data.	Self-benefiting	No
Misbehavior in Networks/ Applications, Poor Access Control	D'Arcy and Devaraj [85]	Misuse of information technology resources	/	Sending an inappropriate e-mail, use of unlicensed software, unauthorized access to data, and unauthorized modification of data.	Self-benefiting	No
Misbehavior in Networks/ Applications, Poor Access Control	Guo and Yuan [109], Guo et al. [110]	Non-malicious security violation	"The behaviors engaged in by end users who knowingly violate organizational IS security policies without malicious intents to cause damage" [110] (p. 205).	Writing down passwords, unauthorized portable devices for storing and carrying organizational data, installation and use of unauthorized software, and use of an insecure public wireless network for business purposes.	Self-benefiting, for convenience	No

Misbehavior in Networks/ Applications, Dangerous Web Use	Chu and Chau [7], Chu et al. [57], Chu et al. [111]	Resource misuse	"Information security deviant behavior that is related to the misuse of information systems resources" [7] (p. 93).	Using untrusted networks (e.g., the Internet) for data transmission at work, running untrusted applications for personal purposes at work, and installing untrusted applications for personal purposes at work, and using instant messaging services at work without permission.	Self-benefiting	Yes
Misbehavior in Networks/ Applications	Peace et al. [59]	Software privacy	"Any illegal software copying activity" (p. 155).	Access to software that could be copied.	Self-benefiting	No
Dangerous Web Use	Vitak et al. [112]	Cyberslacking (also referred to as cyberloafing, non-work-related computing, cyber deviance, personal use at work, Internet abuse, workplace Internet leisure browsing, and junk computing)	"Use of Internet and mobile technology during work hours for personal purposes" (p. 1751).	Online shopping, blogging, gaming, gambling, auction, personal investing, pornography, and instant messaging during work hours.	Self-benefiting	No (but a cumulative index of 9 activities and a cumulative index of 4 cyberslacking types of behavior were developed.)
Dangerous Web Use	Lim [54]	Cyberloafing	"Any voluntary act of employees' using their companies' internet access during office hours to surf non-job-related websites for personal purposes and to check (including receiving and sending) personal e-mail" (p. 677).	Browsing activities: sports related websites, investment related websites, entertainment related websites, general news sites, non-job-related websites, download non-work-related information, shop online for personal goods, and adult-oriented (sexually explicit) websites. E-mailing activities: check non-work-related e-mail, send non-work-related e-mail, and receive non-work-related e-mail.	Self-benefiting	Yes
Dangerous Web Use	Bock and Ho [15], Pee et al. [16]	Non-work-related computing	"Employees' use of the Internet in their workplace for personal purposes" [16] (p. 120).	Using office resources, instant messaging, data search for personal interest, file downloading, Internet gaming.	Self-benefiting	No
Dangerous Web Use	Arnesen and Weis [113], Lee et al. [60]	Personal web use	"Non-work-related use of the Internet for personal purposes during work hours" [60] (p. 76).	Accessing pornography sites, and on-line shopping, banking, checking stock prices, watching sporting events, playing on-line poker, listening to Internet radio, booking travel.	Self-benefiting	No
Omissive Security Behavior, Poor Access Control	Herath et al. [2]	IS Security Policy Violation	/	Password sharing, password write-down, no log-off, carrying data on USB.	Self-benefiting, for convenience	No

Omissive Security Behavior, Poor Access Control	Siponen and Vance [114], Vance and Siponen [115]	Information systems security policy violation	"Employees' failure to comply with information systems security policies" [114] (p. 487).	Failing to lock or log out of workstations; writing down personal passwords in visible places; sharing passwords with colleagues or friends; copying sensitive data to insecure USB practices; revealing confidential information to outsiders; disabling security configurations; using laptops carelessly outside of the company; sending confidential information unencrypted; creating easy-to-guess passwords.	Self-benefiting, but some acts do not happen in the workplace, which is beyond the scope of the current research.	No
Omissive Security Behavior, Poor Access Control	Workman et al. [17]	Omissive behavior	/	Passwords were not updated and protected, security and virus software were not kept up to date, and systems were not backed up.	Self-benefiting, for convenience	No
Omissive Security Behavior	Chu and Chau [7], Chu et al. [57]	Security careless	"Information security deviant behavior that is related to the employees' omissive activities when using computers or handling data" [7] (p. 93).	Not locking work computer when away for convenience, not shutting down work computer after finished using it for convenience, leaving removable storage devices with company information unattended in office.	For convenience	Yes
Omissive Security Behavior, Dangerous Web Use	Li et al. [18]	Consequence-delayed information security violation (CDISV)	No definition but three particular characteristics of CDISV were stated out: a. The ultimate consequence caused by CDISV is delayed; b. CDISV is an indirect cause of IS damage; and c. the risk created by CDISV could not be automatically eliminated.	Unauthorized portable devices for storing corporate data, sending unencrypted emails, downloading suspicious files from the internet.	Self-benefiting, for convenience	No
Poor Access Control	Chu et al. [57]	Access control deviance	/	Sharing password/account with colleagues, gaining unauthorized access, guessing colleague's password, writing down passwords.	For convenience	No
Poor Access Control	Hoonakker et al. [66]	Deviations from best password practices	/	Using the same password for every system they access, writing down passwords, storing passwords in electronic files, and reusing or recycling old passwords.	For convenience	No
Poor Access Control	Hu et al. [116]	Information security policy abuse	"Any act by an employee using computers that is against the established rules and policies of an organization for personal gains" (p. 54).	Unauthorized access to data and systems, unauthorized copying or transferring of confidential data, or selling confidential data to a third party for personal gains.	Self-benefiting, but can be malicious, which does not match with our definition	No
Poor Access Control	Johnston et al. [117]	Information security policy violation	/	Disregarding a mandatory password encryption procedure.	For convenience	No
Poor Access Control	Stanton et al. [118]	Naive mistakes	"Behavior requires minimal technical expertise and no clear intention to do harm to the organization's information technology and resources" (p. 126).	Writing password on a sticky note and putting it on a monitor, choosing a password consisting of four digits, using a social security number as a password, writing password on a slip of paper and taping it under a keyboard, and sharing account information with a friend.	For convenience	No

References

1. Choi, M.; Lee, C. Information security management as a bridge in cloud systems from private to public organizations. *Sustainability* **2015**, *7*, 12032–12051. [CrossRef]
2. Herath, T.; Yim, M.S.; D'Arcy, J.; Nam, K.; Rao, H.R. Examining employee security violations: Moral disengagement and its environmental influences. *Inf. Technol. People* **2018**, *31*, 1135–1162. [CrossRef]
3. Wu, S.M.; Guo, D.; Wu, Y.; Wu, Y.C. Future development of taiwan's smart cities from an information scurity perspctive. *Sustainability* **2018**, *10*, 4520. [CrossRef]
4. Hu, Q.; West, R.; Smarandescu, L. The role of self-control in information security violations: Insights from a cognitive neuroscience perspective. *J. Manag. Inf. Syst.* **2015**, *31*, 6–48. [CrossRef]
5. Sen, R. Challenges to cybersecurity: Current state of affairs. *Commun. Assoc. Inf. Syst.* **2018**, *43*, 2. [CrossRef]
6. Chatterjee, S.; Sarker, S.; Valacich, J.S. The behavioral roots of information systems security: Exploring key factors related to unethical IT use. *J. Manag. Inf. Syst.* **2015**, *31*, 49–87. [CrossRef]
7. Chu, A.M.Y.; Chau, P.Y.K. Development and validation of instruments of information security deviant behavior. *Decis. Support Syst.* **2014**, *66*, 93–101. [CrossRef]
8. Lee, S.M.; Lee, S.G.; Yoo, S. An integrative model of computer abuse based on social control and general deterrence theories. *Inf. Manag.* **2004**, *41*, 707–718. [CrossRef]
9. Posey, C.; Bennett, R.J.; Roberts, T.L. Understanding the mindset of the abusive insider: An examination of insiders' causal reasoning following internal security changes. *Comput. Secur.* **2011**, *30*, 486–497. [CrossRef]
10. Posey, C.; Bennett, R.J.; Roberts, T.L.; Lowry, P.B. When computer monitoring backfires: Privacy invasions and organizational injustice as precursors to computer abuse. *J. Inf. Syst. Secur.* **2011**, *7*, 24–47.
11. D'Arcy, J.; Hovav, A. Deterring internal information systems misuse. *Commun. ACM* **2007**, *50*, 113–117. [CrossRef]
12. D'Arcy, J.; Hovav, A. Towards a best fit between organizational security countermeasures and information systems misuse behaviors. *J. Inf. Syst. Secur.* **2007**, *3*, 3–31.
13. D'Arcy, J.; Hovav, A.; Galletta, D. User awareness of security countermeasures and its impact on information systems misuse: A deterrence approach. *Inf. Syst. Res.* **2009**, *20*, 79–98. [CrossRef]
14. Campbell, M.; Lu, Y. 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, Keystone, CO, USA, 10–12 August 2007.
15. Bock, G.-W.; Ho, S.L. Non-work related computing (NWRC). *Commun. ACM* **2009**, *52*, 124–128. [CrossRef]
16. Pee, L.G.; Woon, I.M.Y.; Kankanhalli, A. Explaining non-work-related computing in the workplace: A comparison of alternative models. *Inf. Manag.* **2008**, *45*, 120–130. [CrossRef]
17. Workman, M.; Bommer, W.H.; Straub, D. Security lapses and the omission of information security measures: A threat control model and empirical test. *Comput. Hum. Behav.* **2008**, *24*, 2799–2816. [CrossRef]
18. Li, Y.; Zhang, N.; Siponen, M. Keeping secure to the end: A long-term perspective to understand employees' consequence-delayed information security violation. *Behav. Inf. Technol.* **2019**, *38*, 435–453. [CrossRef]
19. Siponen, M.; Vance, A. Guidelines for improving the contextual relevance of field surveys: The case of information security policy violations. *Eur. J. Inf. Syst.* **2014**, *23*, 289–305. [CrossRef]
20. Lewis, P.V. Defining "business ethics": Like nailing jello to a wall. *J. Bus. Eth.* **1985**, *4*, 377–385. [CrossRef]
21. Mason, R.O. Four ethical issues of the information age. *MIS Q.* **1986**, *10*, 5–12. [CrossRef]
22. Mason, R.O. Applying ethics to information technology issues. *Commun. ACM* **1995**, *38*, 55–57. [CrossRef]
23. Kaptein, M. Developing a measure of unethical behavior in the workplace: A stakeholder perspective. *J. Manag.* **2008**, *34*, 978–1008. [CrossRef]
24. D'Arcy, J.; Hovav, A. Does one size fit all? Examining the differential effects of IS security countermeasures. *J. Bus. Eth.* **2009**, *89* (Suppl. 1), 59–71. [CrossRef]
25. Ng, B.-Y.; Kankanhalli, A.; Xu, Y.C. Studying users' computer security behavior: A health belief perspective. *Decis. Support Syst.* **2009**, *46*, 815–825. [CrossRef]
26. Albrechtsen, E.A. A qualitative study of users' view on information security. *Comput. Secur.* **2007**, *26*, 276–289. [CrossRef]
27. Bacon, T. You are how you behave: Customers can't be fooled. *J. Bus. Strateg.* **2004**, *25*, 35–40. [CrossRef]
28. Giacalone, R.A.; Greenberg, J. *Antisocial Behavior in Organizations*; Sage Publications: Thousand Oaks, CA, USA, 1997.

29. Robinson, S.L.; Bennett, R.J. Workplace deviance: Its definition, Its manifestations, and its causes. *Res. Negotiat. Organ.* **1997**, *6*, 3–27.
30. Moberg, D.J. On employee vice. *Bus. Eth. Q.* **1997**, *7*, 41–60. [CrossRef]
31. Vardi, Y.; Wiener, Y. Misbehavior in organizations: A motivational framework. *Organ. Sci.* **1996**, *7*, 151–165. [CrossRef]
32. Neuman, J.H.; Baron, R.A. Workplace violence and workplace aggression: Evidence concerning specific forms, potential causes, and preferred targets. *J. Manag.* **1998**, *24*, 391–419. [CrossRef]
33. O'Leary-Kelly, A.M.; Griffin, R.W.; Glew, D.J. Organization-motivated aggression: A research framework. *Acad. Manag. Rev.* **1996**, *21*, 225–253. [CrossRef]
34. Skarlicki, D.P.; Folger, R. Retaliation in the workplace: The roles of distributive, procedural, and interactional justice. *J. Appl. Psychol.* **1997**, *82*, 434–443. [CrossRef]
35. Puffer, S.M. Prosocial Behavior, noncompliant behavior, and work performance among commission salespeople. *J. Appl. Psychol.* **1987**, *72*, 615–621. [CrossRef]
36. Whitman, M.E. In defense of the realm: Understanding threats to information security. *Int. J. Inf. Manag.* **2004**, *24*, 43–57. [CrossRef]
37. Keen, P.G. Information systems and organizational change. *Commun. ACM* **1981**, *24*, 24–33. [CrossRef]
38. Leavitt, H.J. Applying organizational change in industry: Structural, technological and humanistic approaches. In *Handbook of Organizations*; March, J.G., Ed.; Rand McNally: Chicago, IL, USA, 1965; pp. 1144–1170.
39. Banerjee, D.; Cronan, T.P.; Jones, T.W. Modeling IT ethics: A study in situational ethics. *MIS Q.* **1998**, *22*, 31–60. [CrossRef]
40. Leonard, L.N.; Cronan, T.P. Illegal, inappropriate, and unethical behavior in an information technology context: A study to explain influences. *J. Assoc. Inf. Syst.* **2001**, *1*, 12. [CrossRef]
41. Ye, N.; Giordano, J.; Feldman, J. A process control approach to cyber attack detection. *Commun. ACM* **2001**, *44*, 76–82. [CrossRef]
42. Icove, D.; Seger, K.; VonStorch, W. *Computer Crime: A Crimefighter's Handbook*; O'Reilly & Associates: Sebastopol, CA, USA, 1995.
43. McQuade, S.C. *Understanding and Managing Cybercrime*; Pearson Allyn and Bacon: Boston, MA, USA, 2006.
44. Pollitt, M.M. *Cyberterrorism—Fact or Fancy?* FBI Laboratory: Washington, DC, USA, 2002.
45. Choi, M. Leadership of information security manager on the effectiveness of information systems security for secure sustainable computing. *Sustainability* **2016**, *8*, 638. [CrossRef]
46. Kotulic, A.G.; Clark, J.G. Why there aren't more information security research studies. *Inf. Manag.* **2004**, *41*, 597–607. [CrossRef]
47. Hinkin, T.R. A review of scale development practices in the study of organizations. *J. Manag.* **1995**, *21*, 967–988. [CrossRef]
48. Hinkin, T.R. A brief tutorial on the development of measures for use in survey questionnaires. *Organ. Res. Methods* **1998**, *1*, 104–121. [CrossRef]
49. MacCallum, R.C.; Browne, M.W. The use of causal indicators in covariance structure models: Some practical issues. *Psychol. Bull.* **1993**, *114*, 533–541. [CrossRef] [PubMed]
50. Bollen, K.; Lennox, R. Conventional wisdom on measurement: A structural equation perspective. *Psychol. Bull.* **1991**, *110*, 305–314. [CrossRef]
51. Bennett, R.J.; Robinson, S.L. Development of a measure of workplace deviance. *J. Appl. Psychol.* **2000**, *85*, 349–360. [CrossRef] [PubMed]
52. Jarvis, C.B.; MacKenzie, S.B.; Podsakoff, P.M. A critical review of construct indicators and measurement model misspecification in marketing and consumer research. *J. Consum. Res.* **2003**, *30*, 199–218. [CrossRef]
53. Webster, J.; Watson, R.T. Analyzing the past to prepare for the future: Writing a literature review. *MIS Q.* **2002**, *26*, xiii–xxiii.
54. Lim, V.K. The IT way of loafing on the job: Cyberloafing, neutralizing and organizational justice. *J. Organ. Behav.* **2002**, *23*, 675–694. [CrossRef]
55. Mahmood, M.A.; Siponen, M.; Straub, D.; Rao, H.R. Moving toward black hat research in information systems security: An editorial introduction to the special issue. *MIS Q.* **2010**, *34*, 431–433. [CrossRef]
56. Lin, C.-P.; Ding, C.G. Modeling information ethics: The joint moderating role of locus of control and job insecurity. *J. Bus. Eth.* **2003**, *48*, 335–346. [CrossRef]

57. Chu, A.M.Y.; Chau, P.Y.K.; So, M.K.P. Developing a typological theory using a quantitative approach: A case of information security deviant behavior. *Commun. Assoc. Inf. Syst.* **2015**, *37*, 25. [CrossRef]
58. Moores, T.T.; Esichaikul, V. Socialization and software pivacy: A study. *J. Comput. Inf. Syst.* **2011**, *51*, 1–9.
59. Peace, A.G.; Galletta, D.F.; Thong, J.Y.L. Software piracy in the workplace: A model and empirical test. *J. Manag. Inf. Syst.* **2003**, *20*, 153–177.
60. Lee, Y.; Lee, Z.; Kim, Y. Understanding personal web usage in organizations. *J. Organ. Comput. Electron. Commer.* **2007**, *17*, 75–99.
61. Websense. 2006 Web@work Survey. 2006. Available online: https://www.01net.it/wp-content/uploads/sites/14/2014/10/websense_internet_dipendenti.pdf (accessed on 30 March 2020).
62. Belanger, F.; Slyke, C.V. Abuse or learning? *Commun. ACM* **2002**, *45*, 64–65. [CrossRef]
63. Oravec, J.A. Constructive approaches to internet recreation in the workplace. *Commun. ACM* **2002**, *45*, 60–63. [CrossRef]
64. DeGeorge, R.T. Business ethics and the challenge of the information age. *Bus. Eth. Q.* **2000**, *10*, 63–72. [CrossRef]
65. Chen, Y.C.; Shang, R.A.; Lin, A.K. The intention to download music files in a P2P environment: Consumption value, fashion, and ethical decision perspectives. *Electron. Commer. Res. Appl.* **2009**, *7*, 411–422. [CrossRef]
66. Hoonakker, P.; Bornoe, N.; Carayon, P. Password authentication from a human factors persective: Results of a survey among end-users. In Proceedings of the 53rd Annual Meeting of the Human Factors and Ergonomics Society, San Antonio, TX, USA, 1 October 2009; pp. 459–463.
67. Culnan, M.J.; Williams, C.C. How ethics can enhance organizational privacy: Lessons from the choicepoint and TJX data breaches. *MIS Q.* **2009**, *33*, 673–687. [CrossRef]
68. Muntean, M.; Dijmarescu, L. Sustainable implementation of access control. *Sustainability* **2018**, *10*, 1808. [CrossRef]
69. Adams, A.; Sasse, M.A. Users are not the enemy. *Commun. ACM* **1999**, *42*, 41–46. [CrossRef]
70. Horowitz, A.S. Top 10 Security Mistakes. Computerworld. 2001. Available online: https://www.computerworld.com/article/2582953/security0/top-10--security--mistakes.html (accessed on 30 March 2020).
71. Eisenhardt, K.M. Agency theory: An assessment and review. *Acad. Manag. Rev.* **1989**, *14*, 57–74. [CrossRef]
72. Jensen, M.C.; Meckling, W.H. Theory of the firm: Managerial behavior, agency costs, and ownership structure. *J. Financ. Econ.* **1976**, *3*, 305–360. [CrossRef]
73. Deckop, J.R.; Mangel, R.; Cirka, C.C. Getting more than you pay for: Organizational citizenship behavior and pay-for-performance plans. *Acad. Manag. J.* **1999**, *42*, 420–428.
74. Heath, J. The uses and abuses of agency theory. *Bus. Eth. Q.* **2009**, *19*, 497–528. [CrossRef]
75. Sappington, D.E. Incentives in principal-agent relationships. *J. Econ. Perspect.* **1991**, *5*, 45–66. [CrossRef]
76. Hannafey, F.; Vitulano, L.A. Ethics and executive coaching: An agency theory approach. *J. Bus. Eth.* **2013**, *115*, 599–603. [CrossRef]
77. Bahli, B.; Rivard, S. The information technology outsourcing risk: A transaction cost and agency theory-based perspective. *J. Inf. Technol.* **2003**, *18*, 211–221. [CrossRef]
78. Herath, T.; Rao, H.R. Encouraging information security behaviors in organizations: Role of penalties, pressures and perceived effectiveness. *Decis. Support Syst.* **2009**, *47*, 154–165. [CrossRef]
79. Jensen, M.C. Slef-interest, altruism, incentives, and agency theory. *J. Appl. Corp. Financ.* **1994**, *7*, 40–45. [CrossRef]
80. Brennan, M.J. Incentives, rationality, and society. *J. Appl. Corp. Financ.* **1994**, *7*, 31–39. [CrossRef]
81. Furnell, S. End-user security culture: A lesson that will never be learnt? *Comput. Fraud Secur.* **2008**, *4*, 6–9. [CrossRef]
82. Hagen, J.M.; Albrechtsen, E.; Hovden, J. Implementation and effectiveness of organizational information security measures. *Inf. Manag. Comput. Secur.* **2008**, *16*, 377–397. [CrossRef]
83. Spears, J.L.; Barki, H. User participation in information systems security risk management. *MIS Q.* **2010**, *34*, 503–522. [CrossRef]
84. Willison, R.; Warkentin, M. Beyond deterrence: An expanded view of employee computer abuse. *MIS Q.* **2013**, *37*, 1–20. [CrossRef]
85. D'Arcy, J.; Devaraj, S. Employee misuse of information technology resources: Testing a contemporary deterrence model. *Decis. Sci.* **2012**, *43*, 1091–1124. [CrossRef]

86. Grance, T.; Kent, K.; Kim, B. Computer security incident handling guide. *Natl. Inst. Stand. Technol.* **2012**, *800*, 1–147.
87. Yang, C.L.; Yuan, B.J.C.; Huang, C.Y. Key determinant derivations for information technology disaster recovery site selection by the multi-criterion decision making method. *Sustainability* **2015**, *7*, 6149–6188. [CrossRef]
88. Hassan, S.; Wright, B.E.; Yukl, G. Does ethical leadership matter in government? Effects on organizational commitment, absenteeism, and willingness to report ethical problems. *Public Adm. Rev.* **2014**, *74*, 333–343. [CrossRef]
89. Chin, W.W. Issues and opinion on structural equation modeling. *MIS Q.* **1998**, *22*, vii–xvi.
90. Hair, J.F.; Anderson, R.E.; Tatham, R.L.; Black, W.C. *Multivariate Data Analysis*; Prentice-Hall International: Upper Saddle River, NJ, USA, 1998.
91. Gefen, D.; Straub, D.; Boudreau, M.-C. Structural equation modeling and regression: Guidelines for research practice. *Commun. Assoc. Inf. Syst.* **2000**, *4*, 1–78. [CrossRef]
92. Fornell, C.; Larcker, D.F. Evaluating structural equation models with unobservable variables and measurement error. *J. Mark. Res.* **1981**, *18*, 39–50. [CrossRef]
93. Gefen, D.; Straub, D. A practical guide to factorial validity using PLSGraph: Tutorial and annotated example. *Commun. Assoc. Inf. Syst.* **2005**, *16*, 91–109.
94. Harrington, S.J. The effect codes of ethics and personal denial of responsibility on computer abuse judgments and intentions. *MIS Q.* **1996**, *20*, 257–278. [CrossRef]
95. Gopal, R.D.; Sanders, G.L. Preventive and deterrent controls for software piracy. *J. Manag. Inf. Syst.* **1997**, *13*, 29–47. [CrossRef]
96. Chang, S.J.; van Witteloostuijn, A.; Eden, L. From the editors: Common method variance in international business research. *J. Int. Bus. Stud.* **2010**, *41*, 178–184. [CrossRef]
97. Malhotra, N.K.; Kim, S.S.; Patil, A. Common method variance in IS research: A comparison of alternative approaches and a reanalysis of past research. *Manag. Sci.* **2006**, *52*, 1865–1883. [CrossRef]
98. Ones, D.S.; Viswesvaran, C.; Schmidt, F.L. Comprehensive meta-analysis of integrity test validities: Findings and implications for personnel selection and theories of job performance. *J. Appl. Psychol.* **1993**, *78*, 679–703. [CrossRef]
99. Podsakoff, P.M.; MacKenzie, S.B.; Podsakoff, N.P. Sources of method bias in social science research and recommendations on how to control it. *Ann. Rev. Psychol.* **2012**, *63*, 539–569. [CrossRef]
100. Simmering, M.J.; Fuller, C.M.; Richardson, H.A.; Ocal, Y.; Atinc, G.M. Marker variable choice, reporting, and interpretation in the detection of common method variance: A review and demonstration. *Organ. Res. Methods* **2015**, *18*, 473–511. [CrossRef]
101. Chu, A.M.Y.; So, M.K.P.; Chung, R.S.W. Applying the randomized response technique in business ethics research: The misuse of information systems resources in the workplace. *J. Bus. Eth.* **2018**, *151*, 195–212. [CrossRef]
102. Chong, A.C.Y.; Chu, A.M.Y.; So, M.K.P.; Chung, R.S.W. Asking sensitive questions using the randomized response approach in public health research: An empirical study on the factors of illegal waste disposal. *Int. J. Environ. Res. Public Health* **2019**, *16*, 970. [CrossRef] [PubMed]
103. Chung, R.S.W.; Chu, A.M.Y.; So, M.K.P. Bayesian randomized response technique with multiple sensitive attributes: The case of information systems resource misuse. *Ann. Appl. Stat.* **2018**, *12*, 1969–1992. [CrossRef]
104. Straub, D.W., Jr. Effective IS security: An empirical study. *Inf. Syst. Res.* **1990**, *1*, 255–276. [CrossRef]
105. Lowry, P.B.; Moody, G.D.; Galletta, D.F.; Vance, A. The drivers in the use of online whistle-blowing reporting systems. *J. Manag. Inf. Syst.* **2013**, *30*, 153–190. [CrossRef]
106. Straub, D.W., Jr.; Nance, W.D. Discovering and disciplining computer abuse in organizations: A field study. *MIS Q.* **1990**, *14*, 45–60. [CrossRef]
107. Hovav, A.; D'Arcy, J. Applying an extended model of deterrence across cultures: An investigation of information systems misuse in the U.S. and South Korea. *Inf. Manag.* **2012**, *49*, 99–110. [CrossRef]
108. Liao, Q.; Luo, X.; Gurung, A.; Li, L. Workplace management and employee misuse: Does punishment matter? *J. Comput. Inf. Syst.* **2009**, *50*, 49–59.
109. Guo, K.H.; Yuan, Y. The effects of multilevel sanctions on information security violations: A mediating model. *Inf. Manag.* **2012**, *49*, 320–326. [CrossRef]

110. Guo, K.H.; Yuan, Y.; Archer, N.P.; Connelly, C.E. Understanding nonmalicious security violations in the workplace: A composite behavior model. *J. Manag. Inf. Syst.* **2011**, *28*, 203–236. [CrossRef]
111. Chu, A.M.Y.; Chau, P.Y.K.; So, M.K.P. Explaining the misuse of information systems resources in the workplace: A dual-process apprach. *J. Bus. Eth.* **2015**, *131*, 209–225. [CrossRef]
112. Vitak, J.; Crouse, J.; LaRose, R. Personal internet use at work: Understanding cyberslacking. *Comput. Hum. Behav.* **2011**, *27*, 1751–1759. [CrossRef]
113. Arnesen, D.W.; Weis, W.L. Developing an effective company policy for employee internet and e-mail use. *J. Organ. Cult. Commun. Confl.* **2007**, *11*, 53–65.
114. Siponen, M.; Vance, A. Neutralization: New insights into the problem of employee information systems security policy violations. *MIS Q.* **2000**, *34*, 487–502. [CrossRef]
115. Vance, A.; Siponen, M. IS security policy violations: A rational choice perspective. *J. Organ. En117d User Comput.* **2012**, *24*, 21–41. [CrossRef]
116. Hu, Q.; Xu, Z.; Dinev, T.; Ling, H. Does deterrence work in reducing information security policy abuse by employees? *Commun. ACM* **2011**, *54*, 54–60. [CrossRef]
117. Johnston, A.C.; Warkentin, M.; McBride, M.; Carter, L. Dispositional and situational factors: Influences on information security policy violations. *Eur. J. Inf. Syst.* **2016**, *25*, 231–251. [CrossRef]
118. Stanton, J.M.; Stam, K.R.; Mastrangelo, P.; Jolton, J. Analysis of end user security behavior. *Comput. Secur.* **2005**, *24*, 124–133. [CrossRef]