Compliant or Not-Compliant? A Taxonomy for Types of Information Security Policy Deviance

Completed Research Paper

Introduction

In the last few years, the importance of information technology (IT) has increased throughout the private and business environment (Yoo et al. 2012), while information systems (IS) and IT have evolved from a purely supportive function to a more empowering and leading function (Bharadwaj et al. 2013; Gannon 2013) in the field. With increasing digitalization, the use of IS in the professional sector and the amount of distributed data is also increasing, resulting in a transformation of the working environment (Colbert et al. 2016; Tilson et al. 2010). On the other hand, IT's influence on the business environment leads to higher efficiency and an easier performance of operational tasks, while subsequently unveiling the potential for criminal acts and their resulting damages associated with its increase (Charlier et al. 2017; Wu et al. 2015). Therefore, companies have defined IT security policies for employees to directly follow in order to ensure responsible use of IT at the workplace, as has been done without IT in the past (Höne and Eloff 2002; Sohrabi Safa et al. 2016). A related topic to this phenomenon in IS research is the deviation of Information Security Policies (ISP), defined as the deviation of individuals in a professional context from an accumulation of information security activities, of which employees must adhere for ensuring information security in accordance with those policies provided (Padayachee 2012).

In the current research, important progress has been made in the analysis of ISP deviance. Several studies have analyzed different aspects of ISP to explain the various types of associated deviancies and are therein based on theories of deviant behavior at the workplace or other related research areas such as criminology. Looking at the existing ISP deviance literature, there is a noticeably wide variety of approaches considered towards the clarification of behavior and its analysis. There are studies analyzing the user's awareness of security countermeasures and its impact on ISP deviance using deterrence theory (D'Arcy et al. 2009). Other studies concentrate on the effect of ISP on conformal behavior, also based on theories out of the field of criminology as social learning or deterrence theory (Lembcke et al. 2018; Trang 2018). Gua and Yuan (2012) consider the impact of punishment on employee compliance based on their individual motivation. Posey et al. (2011) address the non-compliant behavior of employees with the purpose of protecting organizational goods, such as information or information systems based on protection-motivated behaviors. Furthermore, Banerjee et al. (1998) analyze employees' behavior against the ISP out of an ethical perspective. All these results give important insights into employee's behavior from various perspectives with regard to ISP deviance or in other related research fields such as criminology or work deviance research, of all which cope with the ISP related faults of employees. Looking at the different perspectives on ISP deviance research, there is no clear taxonomic distinction between them, since it is important to gain an overview of existing gaps in research and which theories can be applied in which contexts. This need can be illustrated by Willison and Warkentin (2013) or Willison et al. (2018), who argue that the use of behavioral research-oriented theories in ISP deviance research, such as deterrence theory, cannot be applied and analyzed in every context which would create a need for demarcation. A taxonomy offers an initial starting point for this.

However, what is dually noticeable when inspecting these articles is on the one hand, numerous studies exist applying many different points of views for the description of ISP deviance behavior. So far, however, they have only been considered useful to a limited extent in an overall context, as in a taxonomy. Some examples of taxonomies in ISP deviance research include the definition of costs and benefits of ISP compliance (Bulgurcu et al. 2010) and its overall function, an individual's awareness about incompliant actions (Cheng et al. 2013), or the classification of offenses against individuals or organizations with minor or more serious consequences and the classification of technologically required knowledge for such offenses (Venkatraman et al. 2018). Padayachee (2012) additionally addresses the motivation for ISP deviance. On the other hand, the existing ISP deviance typologies have so far only been based on a purely inductive or deductive approach, or also have been developed ad hoc and refer only partially to existing dimensions of

ISP deviance or related research areas such as criminology or work deviance research (Venkatraman et al. 2018; Venter et al. 2007).

Since there is a multitude of distributed approaches for the explanation of ISP deviance behavior, along with a recognizable connection to work deviance research and criminology, the combination of these approaches within a holistic taxonomy is an important tool to summarize the existing state of research in a structured and clear manner. Therefore, a holistic procedure is needed. This includes the review of existing ISP deviance, as well as work deviance and criminology literature, in addition to the application of empirical methods instead of a unilateral approach, of which are not mutually exclusive and collectively exhaustive.

Accordingly, we identify a gap in the current literature of a holistic and deductively as well as empirical developed ISP taxonomy.

To address this gap in the current literature, this paper applies a conceptual and empirically driven taxonomy development as suggested in Nickerson et al. (2013) and meets the necessities of mutually exclusivity and collectively exhaustivity. Drawing on the workplace deviance and criminology taxonomy literature as well as existing studies for the description of behavior in the ISP deviation context, we develop an initial approach for our ISP deviance taxonomy, followed by interviews with employees from different organizations to extend the given dimension and characteristics derived from literature. The interviews were evaluated using structured content analysis. With this approach, we can aggregate the existing literature on ISP deviation and provide an effective and complete overview, as well as transfer further aspects from work deviance research and criminology into the context of IS research, identifying approaches for their ensuing application. In its practical application, such a taxonomy can be employed to identify types of violations or to derive countermeasures, designing more behaviorally-oriented IT security training.

The remaining part of this article is structured as follows: Following the introduction, taxonomies in general and the aforementioned related research fields, as well as that of ISP deviation are described. Subsequently, the method and procedure for taxonomy creation, including the method for data collection and analysis, will be presented, followed by the created taxonomy's description and concurrent discussion. The paper concludes with implications for research and practice, as well as limitations of the paper and actions for future research.

Theoretical Background

Taxonomies in Research

In the literature, the development of taxonomy is often described as a tool for classifying objects and information in different subject areas in order to illustrate complex facts (Glass and Vessey 1995). This enables their viewers, whether from the practical environment or from research, to gain an appropriate overview of a particular subject (Bailey 2003; Nickerson et al. 2010; Webster and Watson 2002). As Nickerson et al. (2013) describe, however, the concept and methodology of taxonomy are broadly defined, resulting in different applications with different terms within the chosen taxonomy. Nickerson et al. (2013) compare the approaches used by other authors for the development and use of taxonomy and summarize them in the following definition:

$T = \{D_i, i = 1, ..., n \mid D_i = \{C_{ij}, j = 1, ..., k_i, k_i \geq 2\}$

T describes the taxonomy, while D_i denotes the dimensions to be developed, whereby at least one and at most n dimensions must be contained. The dimensions consist of characteristics C_{ij}, which exclude each other, whereby no object has only one characteristic of a respective characteristic while at least one characteristic for each object must exist. In total, at least $k_i \geq 2$ characteristics per dimension should exist. Since this taxonomy definition in IS research provides an established approach for the methodological development of taxonomies (Siering et al. 2017; Walsh et al. 2016), it is enabled via the context of this paper and described in further detail in the following section.

Taxonomies are used in various subject areas to structure and abstractly reproduce an unclear subject area (Nickerson et al. 2013). Typologies have also been used to describe human behavior in behavioral research, such as criminology and work deviance research. Within these taxonomies, different types of deviant behavior, either deviating from the law or deviating from work policies, were identified and typecasted. As already stated in the introduction, a relationship can be identified between behavioral research from the fields of criminology and work deviance to ISP deviance (Hsu et al. 2015; Hu et al. 2011; Moody et al. 2018). In order to form a stable literature basis for the taxonomy to be developed in this work, existing taxonomies from these areas will be considered as well.

Taxonomies in work deviance research and criminology

In order to get an adequate overview of taxonomies and dimensions of criminology and work deviance, it is necessary to characterize them separately and subsequently combine them. In the work deviance literature inspected by Warren (2003), recurrent positive and negative deviations from rules were identified and discussed on. Thus, in her work, she defines that deviating actions from work instructions can have both a positive, constructive effect on the organization, in addition to a negative, deconstructive one. The research approach applied in her research was based on that of a deductive procedure. Additionally, Vadera et al. (2013) take up the construct of constructive deviation by specifying it into different sub-areas and therein testing it empirically against the background of intrinsic motivation and psychological empowerment (Vadera et al. 2013). Similarly, Dahling and Guthworth (2017) identify in an empirical approach normative conflicts and organizational identity to have a positive influence on constructive deviance (Dahling and Gutworth 2017). That being acknowledged, deconstructive deviance has not yet been considered in an empirical approach.

As a matter of significant foundation, Robinson and Bennet (1995) developed a typology for deviating workplace behavior using multidimensional scaling techniques. They explain that deviant behavior in the workplace varies from minor and serious aspects to interpersonal and organizational aspects. Based on these two factors, the deviation of employees seems to be classifiable into the categories of production deviation, ownership deviation, political deviation, and personal aggression. Bennet and Robinson (2000) goes beyond this approach and identifies how the target object of a thread can be either the organization itself, an individual person, or a group within an organization. Therefore, empirical methods were used in the application for the research. Diefendorff and Mehta (2007) address the relationship between motivational characteristics and workplace deviance through another lens, making a fundamental distinction between the targets of an offense. On the one hand, individuals can be defined as target objects, while on the other hand, organizations can be defined as targets. They also address the motivation or desired added value of a person who violates workplace policies, such as seeking competitive excellence or averting corporate damage. Huang et al. (2017) analyzed why and when employees have the opportunity to respond to job insecurity by misbehaving in the workplace, by defining the trade of personal and corporate moral in relation to misconduct at the workplace.

Equivalently in criminology, approaches can be found for explaining misbehavior against given policies as well. Farr and Gibbons (1990) also use a classification scheme to classify types of crime and behavior. This taxonomy includes the type of crime, or place where the crime was committed, such as at the workplace or on the street. Targets are also referred to as an individual or an organization. Further aspects of the typology are the scope of the crime and the legitimation of the perpetrator. McDevitt et al. (2002) investigated in the field of criminology via the motives for committing hate crimes, placing the aspects thrill, defensive, and mission in the foreground. The table below summarizes the literature considered from Work Deviance and Criminology, which with the help of typologies, empirically or deductively, form a basis for classifying deviant behavior from given rules.

Author	Dimension	Derivation type of the taxonomy
(Dahling and Gutworth 2017; Vadera et al. 2013; Warren 2003)	Constructiveness	Deductive/Empirical
(Robinson and Bennet 1995)	Interpersonal and Organizational Deviance; Personal and Political Deviance	Empirical
(Bennet and Robinson 2000)	Target Object	Empirical
(Diefendorff and Mehta 2007)	Added Value; Target Object	Empirical
(Huang et al. 2017)	Motivation/Moral	Empirical
(McDevitt et al. 2002)	Motivation for crime/Moral	Empirical
(Farr and Gibbons 1990)	Interpersonal and Organizational Crime; Motivation/Moral	Deductive

Table 1: Existing Dimensions of Work Deviance and criminology

Information Security Policy Deviance

As mentioned, there exist previous studies which describe behavior contradictory to a certain norm in the workplace and in society. Similarly, typologies have already been developed in these areas to provide an abstract overview of varying behavior types. Since IT has become a widespread application throughout companies and related policies (ISP), have been equally established, IS research strives to more closely inspect this topic in turn. The ISP deviance research is already dealing with the explanation of deviant behavior in relation to given IS policies as well. Banerjee et al. (1998) for example, discusses the different types of motivation that affect employees when acting against the policies or raising moral standards when they think about committing an indiscretion. They distinguish between an intrinsic motivation emanating from a person and a motivation or related values emanating from an organization, which in turn influence an employee's actions. Guo and Yuan (2012) also address personal motivation, which according to them can impact committing or not committing an IT security breach. A survey conducted in both studies and an empirical derivation of their respective dimensions are provided.

As Venkatraman et al. (2018) achieve in their study, an overview is arranged with types of cyber deviance activities which focus on the dimensions of the target object as a person or organization and the severity of the offense (minor or serious), while at the same time referring to work deviance literature as well. The technical skills required for the offense were likewise included in the analysis too. Other aspects of the ISP deviance or work deviance literature, such as the intrinsic motivation of a person, the expected added value or demarcation between constructive and deconstructive deviance, are omitted. For their typology, the method of multidimensional scaling was applied, which is purely inductive and empirical, and ultimately already recognized from the work deviance literature (Robinson and Bennett 1995).

Padayachee (2012) also addresses the motivation of employees who commit a breach of IT security policies. He goes one step further though than the previously mentioned authors, describing in his taxonomy that the awareness of whether a violation of the guidelines is present or not can also have an influence on the correct classification of ISP deviance. The taxonomy was carried out ad hoc based on existing literature. In a similar manner, Vance and Siponen (2012) identified the suggestion for organizations to focus on activities related to the IS security awareness of their employees that address moral beliefs and perceived benefits of non-compliance inclinations.

Furthermore, Chu and Chau (2014) refer in their study to existing workplace deviance dimensions and transfer them using an empirical study consisting of several statistical methods to the ISP deviance context. They also assume a division in offenses against individuals and the organization, dividing these into political offenses, such as spreading rumors about other colleagues or using IS for private purposes at work. In contrast to this, direct and aggressive offenses are mentioned, such as the injury of persons or the misuse of company property. The procedure is empirical, whereby the constructs used are based on a literature review. Their results can be summarized in a dimension about types of violation.

The motivation is also reflected in the motive of a perpetrator, whereby research was also carried out into their expected added value. For example, Vance et al. (2013) consider that an ongoing problem in information security is the threat posed by members of a company which have access to important internal information and misuse it for their own purposes. Countermeasures are often designed to protect against attackers from outside an organization and most time disregard internal crimes. Therefore, according to their argumentation, because of a violation of the ISPs, an added value can have an informative added value itself. Vance et al. (2012) add in this aspect as there can also be added monetary value inherent in a crime or an ISP violation.

Posey et al. (2013) focus on protection-motivated behaviors in their developed taxonomy in relation to the misusage of computer related information systems. They use qualitative as well as quantitative approaches to develop their taxonomy. Table 2 below summarizes the determined dimensions of ISP deviance including their reference and their type of derivation.

Author	**Dimension**	**Derivation type of the Taxonomy**
(Banerjee et al. 1998)	Motivation/Moral	Empirical
(Guo and Yuan 2012)	Motivation/Moral	Empirical
(Venkatraman et al. 2018)	Target Object; Technical requirements; Severity of the offense	Empirical
(Padayachee 2012)	Awareness; Motivation/Moral	Deductive
(Vance and Siponen 2012)	Awareness	Empirical
(Chu and Chau 2014)	Type of violation	Deductive/Empirical
(Vance et al. 2013)	Added Value	Empirical
(Vance et al. 2012)	Added Value	Empirical
(Posey et al. 2013)	Motivation/Moral	Deductive/Empirical

Table 2: Existing Dimensions of ISP Deviance.

A closer look at the analyzed articles shows the either strongly deductive or empirically based derivation of existing dimensions of classification approaches in the field of ISP deviance research. Furthermore, overlap in some dimensions of other related topics can be identified from differing perspectives. We can recognize taxonomies from different angles on ISP deviance with different deviation types for the taxonomy development. A holistic view, based on a conceptual and empirical approach, is missing so far. Based on these findings, it seems necessary to take a uniform look at this state of current research with the help of the previously introduced procedure, in order to present the results of previous research in a summarized and clear manner, and if necessary, to expand them empirically.

Methodological Approach for Taxonomy Development

According to Nickerson et al. (2013), a taxonomy must fulfill five criteria in order to ensure high usability and quality. First, the number of dimensions and characteristics should be limited in order to make a concise use of the taxonomy possible. Second, there should be enough dimensions and characteristics so they can be clearly distinguished from one another and thus lead to a robust taxonomy. Third, the completeness of the taxonomy, means that a taxonomy with its dimensions can describe all considered objects, be they predefined from an empirical or conceptual approach. Fourth, a taxonomy should be extendable by dimensions and characteristics, whereas it becomes necessary with the consideration of new objects. Lastly, a taxonomy should be descriptive and thus describe the objects with their characteristics of the individual dimensions in such a way that a proper overview of their properties is conducted and provided therein (Nickerson et al., 2013). Furthermore, a certain process is to be pursued during development. As an initial step after the approach of Nickerson et al. (2013), the Meta criterion shall be determined. Meta-characteristics can be developed from the purpose of the taxonomy and reflect the general objective of the taxonomy. The user group of the taxonomy should likewise be considered when determining it, as these can have an impact on the content of the taxonomy with their needs for different information. This may happen explicitly, based on derivations from the users of the objects considered, and implicitly, based on the researcher's assumptions (David Geiger et al. 2011). The Meta criterion for this article can thus be defined as the determination of a meaningful classification of ISP deviation in a professional context.

As a subsequent step in taxonomy development, Nickerson et al. (2013) list the determination of final conditions in which case the iterative development of the taxonomy will be terminated, and its iterations will be considered complete. These criteria can be both objective and subjective. On the one hand, the taxonomy must meet the five quality criteria mentioned above, which can be defined as a subjective condition. On the other hand, objective conditions can be rightly defined. Objective final conditions can be defined according to the approach and needs of the respective user. A list of objective final conditions frequently used in IS research is provided in the subsequent chapters (Sowa and Zachman, 1992). In the subsequent steps of the approach, according to Nickerson et al. (2013), a deductive and an empirical inductive approach alternate. For each iteration, it must be defined in advance whether one of the two approaches are to be chosen.

In the deductive approach, the dimensions and characteristics of the taxonomy are defined and grouped first based on existing literature. Proceeding from this, the objects to be considered are then assigned to the characteristics of the dimensions. The empirical, inductive approach conversely proceeds vice versa. First, the objects to be analyzed are considered and new dimensions and characteristics are formed and grouped based on the results of their analysis. After each iteration, it is verified whether the previously selected final conditions are fulfilled. If this is not the case, a further iteration is carried out until the final conditions are fulfilled. Finally, the taxonomy is then considered as the relative development process is terminated. (Bailey 2003; Nickerson et al. 2013).

The process for developing the taxonomy in this study is illustrated in the figure below. The first iteration follows a conceptual approach. For the definition of dimensions and characteristics the existing ISP deviance, work deviance and criminology literature were used. The second iteration is based on an empirical approach. Within these, 25 interviews were conducted and 135 cases (objects) of ISP deviance were recorded. These objects were then analyzed and assigned to the existing dimensions and characteristics. If necessary, existing components of the taxonomy were modified, deleted or new ones added. For the third iteration, another 15 interviews were conducted, and additional 165 objects were recorded. In the third iteration, the existing taxonomy was verified an adjusted, if necessary.

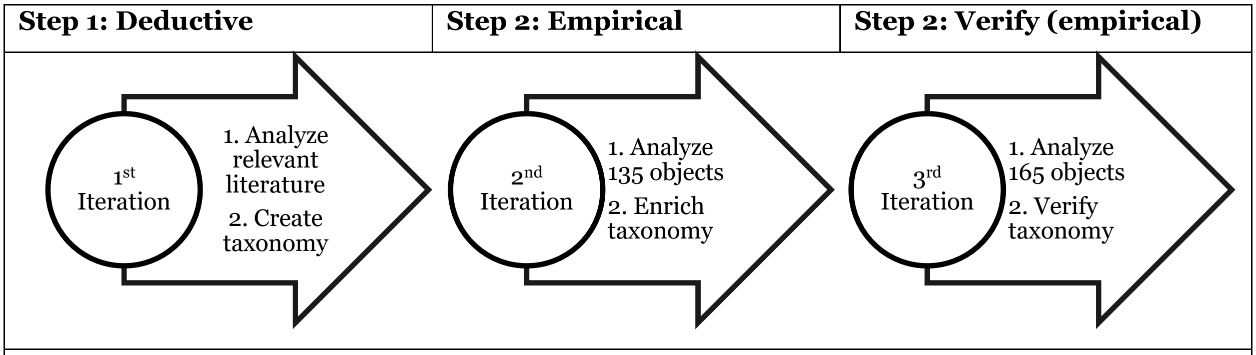

Figure 1: Process for Taxonomy Development.

In contrast to the other taxonomies or classification schemes in ISP deviance research, this approach combines a conceptual and empirical approach instead of concentration on solely one technique, thus combining the advantages of both approaches. This results in a holistic interpretation of the existing ISP deviance, work deviance and criminology literature while meeting the necessities of mutually exclusivity and collectively exhaustivity. Due to the empirical part of the approach, new, previously unknown aspects of ISP deviance can additionally be taken up and integrated into the scheme.

Taxonomy Development

Data Set Description

In addition to the analyzed literature, data has been collected for the empirical part of this study. A total of 300 cases (objects) of ISP deviance were recorded during 40 performed interviews and integrated for the taxonomy development. The data for the development of the taxonomy are collected as follows: The first iteration consists of dimensions and characteristics based on existing ISP deviance literature according to the deductive approach of taxonomy development and reflecting the current state of research in this area, including existing typologies of related research fields mentioned previously. During the second iteration, 25 interviews were conducted which extended or changed those dimensions and characteristics derived from the literature out of the first iteration. In a third iteration, 15 further interviews were conducted, with 35% of the interviewees being female and 65% being male. A large proportion of the respondents worked in the manufacturing industry (23%), the financial sector (20%) and chemical industry (14%), while other sectors included mining, the public sector, the food industry, humanities and transport services. All respondents were aware of their company's IT policies, with the average age of the respondents being 32 years old. During the second iteration, the objects resulting from the first 25 interviews were used to extend the existing, deductively developed dimensions and characteristics. The resulting intermediate results were then verified and finalized by the remaining objects resulting from the other 15 interviews in a third iteration, according to Nickerson et al.'s (2013) rules for creating a valid taxonomy.

1st Iteration

The first iteration followed a conceptual approach in which the dimensions and characteristics shown below were derived from existing literature. Literature from the field of workplace deviance, criminology, as well as from ISP deviance research was accounted. The six derived dimensions, including their characteristics, are illustrated below and form the first basis of the taxonomy. The articles previously presented in the literature review and their dimensions were both merged into the first draft of the taxonomy. In addition to the dimensions, the characteristics contained therein, the literature references and their original thematic field can also be found in the table below.

Dimension D_i	**Characteristics C_{ij}**	**Source**	**Research Field**
D_1 Constructiveness	C_{11} constructive, C_{12} deconstructive	(Dahling and Gutworth 2017; Vadera et al. 2013; Warren 2003)	work deviance
D_2 Moral	C_{21} Individual, C_{22} Organizational	(Banerjee et al. 1998; Farr and Gibbons 1990; Huang et al. 2017)	work deviance / ISP deviance
D_3 Target Object	C_{31} Person, C_{32} Organization	(Diefendorff and Mehta 2007; Venkatraman et al. 2018)	cyber deviance / ISP deviance; criminology; work deviance
D_4 Type of Violation	C_{41} Personal-Aggressive, C_{42} Personal-Political, C_{43} Organizational-Physical, C_{44} Organizational-Immaterial	(Chu and Chau 2014)	ISP deviance; work deviance
D_5 Awareness	C_{51} Conscious, C_{52} Not Conscious	(Padayachee 2012; Vance and Siponen 2012)	ISP deviance
D_6 Added Value	C_{61} Informative, C_{62} Monetary	(Vance et al. 2012; Vance et al. 2013)	ISP deviance; criminology

Table 3: Conceptual derived Taxonomy for ISP deviance after 1st. Iteration.

Constructiveness describes whether a violation of the work or IT guidelines brings added value (C_{11} constructive) for the company or a disadvantage (C_{12} Deconstructive) and was derived from the existing work deviance literature (Dahling and Gutworth 2017; Vadera et al. 2013; Warren 2003). The moral recalled by a person into his memory forms the basis for the second dimension. The individual (C_{21}

Individual) and organizational (C_{22} Organizational) morals for work deviation according to Huang et al. (2017) are used as the basis for the derived characteristics (Banerjee et al. 1998; Farr and Gibbons 1990). The target object describes the third dimension, where Diefendorff and Mehta (2007) distinguishes between persons (C_{31} Person) and companies in a work deviance and Venkatraman et al. (2018) in a cyber deviance context (C_{32} Organization). The type of violation underlies the fourth dimension of this taxonomy. Chu and Chau (2014), which was adopted for the definition of the dimensions and characteristics depicted, distinguishes between personal and corporate misdemeanors. Poverty can be more aggressive (C_{41} Personal-Aggressive) or more political (C_{42} Personal-Political), while Entrepreneurial misdemeanors can be physical (C_{43} Organizational-Physical) or immaterial (C_{44} Organizational-Immaterial). The consciousness of the person violating the ISP is embodied in the fifth dimension. Also, the person may or may not be conscious (C_{51} Conscious, C_{52} Not Conscious) of his or her actions (Padayachee 2012). Furthermore, the sixth dimension describes the added value of the offense committed, which distinguishes between an informative (C_{61} Informative) or monetary (C_{62} Monetary) added value (Vance et al. 2012; Vance et al. 2013). Since no ending conditions for a robust taxonomy according to Nickerson et al. (2013) were met, a further Iteration was needed.

2nd Iteration

An inductive approach was chosen for the second iteration. In the course of 25 interviews, 135 examples of ISP deviance were documented and classified into the existing taxonomy. No new dimensions were added to the taxonomy, but changes in the individual characteristics of the dimensions were noted. Regarding constructiveness, it was found that certain offenses were neither strongly deconstructive nor constructive. Therefore, the characteristic C_{13} Neutral was included. The nature of the offense also changed in the inherent characteristic. The characteristics previously identified in the literature differ between personal attacks and attacks on the company itself. However, this already takes place within the framework of the third dimension of the target object, so that the characteristics of the fourth dimension have been summarized to physical and immaterial, which makes a classification of ISP offenses clearer. Due to this, C_{41} Personal-Aggressive, C_{42} Personal-Political, C_{43} Organizational-Physical, C_{44} Organizational-immaterial were summarized in C_{41} Physical and C_{42} Immaterial.

Additionally, within the framework of the 6th dimension, three further characteristics were added. In the attempt to classify several ISP infringements into the existing taxonomy, a feeling towards the lack of a characteristic arose, containing an added value in terms of the perpetrator's personal status. This type of added value is reflected in the characteristic C_{63} status. Other unclassifiable offenses were those were ISP offenses were committed for amusement. Those objects were combined in the characteristic C_{64} Amusement. Additionally, several cases have been documented in which people have not adhered to the ISP out of convenience. Such objects were also assigned to the characteristic C_{65} Convenience. Finally, there were cases where there was no added value for a person so that None was present as a characteristic named C_{66} None. For the dimensions Moral, Target Object and Awareness no new characteristics were added, nor existing ones removed or changed. Since in the second iteration changes were made to the characteristics of the taxonomy, a third iteration were necessary.

3rd Iteration

During the third iteration, 15 further interviews were conducted for the further development of the taxonomy and 165 further objects of ISP deviation were documented and analyzed. Due to the completion of the taxonomy, the objective and subjective final criteria according to Nickerson et al. (2013) were considered to be fulfilled. There are no doublings within the dimensions and characteristics, with each cell and each character in every dimension is assigned to at least one analyzed object, while no changes were made. It can also be concluded that enough objects were analyzed so that the subjective final criteria are considered fulfilled. To illustrate the need for each iteration, the table below summarizes the three iterations and shows the extent to which each contributes to meeting the required end conditions.

1st. Iteration	**2. Iteration**	**3. Iteration**	**Objective Ending Conditions**
Conceptual	Empirical	Empirical	
	(135)	(165) X	All objects or a representative number of objects were considered
X	X	X	No object was assigned to a similar object in the last iteration or divided into several objects
		X	At least one object is assigned to each characteristic of each dimension
		X	During the last iteration, no new dimensions and characteristics were added
		X	No new dimensions and characteristics were split or assigned during the last iteration
X	X	X	Each dimension is unique and has not been repeated - No duplicates exist
	X	X	Each characteristic is unique in its dimension - no duplicates exist
		X	Each cell of the taxonomy is unique and has not been repeated - No duplicates exist
Subjective Ending Conditions			
	X	X	Limitation of dimensions and characteristics
	X	X	Robustness of the taxonomy
	X	X	Full scope of the taxonomy
X	X	X	Extensibility of the Taxonomy
	X	X	Describability of the taxonomy

Table 4: Summary of iterations and ending conditions.

Since no more changes were made to the taxonomy after a third run and analysis of further objects and all ending conditions were met, the taxonomy is regarded as finished and is represented below.

Dimension D_i	**Theoretically derived Characteristics C_{ij}**	**Empirical developed Characteristics C_{ij}**
D_1 Constructiveness	C_{11} constructive, C_{12} deconstructive	C_{13} None
D_2 Moral	C_{21} Individual, C_{22} Organizational	
D_3 Target Object	C_{31} Person, C_{32} Organization	
D_4 Type of Violation	C_{41}, Physical, C_{42} Immaterial	
D_5 Awareness	C_{51} Conscious, C_{52} Not Conscious	
D_6 Added Value	C_{61} Informative, C_{62} Monetary	C_{63} Status, C_{64} Amusement, C_{65} Convenience, C_{66} None

Table 5: Conceptual and Empirical derived Taxonomy for ISP deviance after 3rd Iteration.

Discussion

This study addresses the need for a holistic, conceptual and empirical developed overview of the different perspectives of ISP deviance research. The approach taken in this study made it possible to meet this need piecemeal by first using the existing literature for taxonomy development and then expanding and reviewing it with the help of empirical data in the form of ISP deviance cases which were analyzed in relation to the taxonomy. After the final classification of all objects, the dimensions and characteristics previously determined from the literature have lightly changed and merely been extended. This may indicate that results and frameworks from criminology and work deviance are also relevant in ISP deviance research as has already been demonstrated in a few previous studies (Venkatraman et al. 2018; Willison and Warkentin 2013). The different dimensions and characteristics of the taxonomy are illustrated in the table listed below and explained by an example for each characteristic.

Dimension D_i	**Characteristics C_{ij}**	**Example**
D_1 Constructiveness	C_{11} constructive	Send work documents unencrypted to colleagues so that work to can be completed
	C_{12} deconstructive	Pass on information to third parties in order to harm the company
	C_{13} None	Using the employee card to give another colleague access to employee parking
D_2 Moral	C_{21} Individual	Abuse system access to steal money from the company for their own benefit
	C_{22} Organizational	Passing on information to third parties in order to prevent major entrepreneurial damage
D_3 Target Object	C_{31} Person	Ignore e-mails from a specific person
	C_{32} Organization	Order private objects using the company system.
D_4 Type of Violation	C_{41}, Physical	Printing of private documents at company expense
	C_{42} Immaterial	Sending private e-mails from the company's e-mail address during working hours
D_5 Awareness	C_{51} Conscious	Withdrawal of IT usage rights from another person due to personal differences
	C_{52} Not Conscious	Not classifying documents for archiving because it was not communicated by the organization
D_6 Added Value	C_{61} Informative	Misuse of IS access rights in order to achieve secret information for a personal purpose
	C_{62} Monetary	Ordering office supplies for private purposes at company's expense
	C_{63} Status	Data of other persons as own misuse, in order to provide a personal advantage
	C_{64} Amusement	Manipulating the computer desktop of an employee who has forgotten to lock it
	C_{65} Convenience	Online shopping at work to avoid having to do it at home
	C_{66} None	Forgetting to archive unimportant e-mails, which had no impact on the company or the person themselves

Table 6: Explanation of Dimensions and Characteristics.

If we consider the characteristics of the individual dimensions separately, their relation to ISP deviance can be emphasized more precisely, as can the transfer of aspects from areas of criminology and work deviance to ISP deviance research. The dimension of constructiveness (D_1), including its characteristics, has so far only been considered in work deviance research and has received no attention in ISP deviance research. However, the results of the taxonomy deduce that this dimension, including its characteristics, is also valid in the ISP context. There are approaches in ISP deviance research in a similar field of interest, such as the subdivision into malicious or beneficial intentions, but no direct reference to constructiveness (Stanton et al. 2005; Vadera et al. 2013; Walsh et al. 2016). A substantiating example out of the empirical part of the taxonomy development for constructive behavior (C_{11}) was *violating the ISP to send work documents to colleagues so that work to can be completed*. Deconstructive (C_{12}), on the other hand, was a case in which the *ISPs were carried out by non-compliant disclosure of information to third parties and the company was harmed*. None (C_{13}) was used when a rule was violated that had no effect, such as *using the employee card to give another colleague access to employee parking*.

The results of the taxonomy also show that the dimension moral (D_2) is an important point in the ISP deviance context as well, whereby previously used literature for the conceptual derivation of this dimension is based on work deviance as well as on ISP deviance. Huang et al. (2017) discuss the influence of moral on work deviance, although, within the ISP deviance literature, the motivation of a person is in the foreground, which can have an influence on the moral of a person (Diefendorff and Mehta 2007; Posey et al. 2013).

According to results of the empirical part of the taxonomy development, the moral or motivation of a person in an ISP deviance context expressed itself as follows: Underlying personal moral (C_{21}) in a committed offense was that *a person of personal interest used the employer's IT systems to gain a monetary advantage over others*. An ISP violation where organizational moral (C_{22}) was acted out is a case *where information was to a third party in order to prevent major entrepreneurial damage.*

The division of the target object (D_3) for a violation of the ISP was addressed both in the ISP and in the work deviance research and could be identified within this taxonomy as helpful for the classification of ISP deviance (Bennett and Robinson 2000; Venkatraman et al. 2018), with one case being a Person (C_{31}) who was a target object in a case where *e-mails of an employee were deliberately ignored*. A case with an organization (C_{32}) as a target would be the example in which *an employee used internal IT systems to order office supplies for a private purpose*.

Regarding the type of violation (D_4), a more abstract level was chosen within this taxonomy than in existing ISP deviance research. The dimensions of Chu and Chau (2014) were initially adopted for the taxonomy development and later divided into two areas, physical and immaterial offenses. Cases with a physical type of misdemeanor relate directly to personal or material damage. An example of physical damage (C_{41}) in the ISP context is the *printing of private documents at company expense*, whereas an immaterial violation (C_{42}) is shown by the example of sending private e-mails from the company's e-mail address during working hours. More detailed assumptions of types of these offenses, such as criminal profiles developed in criminology, could not be identified in the context of an ISP deviance taxonomy development (Clinard et al. 2014).

Awareness (D_5) as a dimension is also considered as helpful for classification of ISP deviance in the context of taxonomy and is based on the literature of the same subject area. A closer look at this aspect is also worthwhile, as conscious dealing with IS and a strong awareness of the ISP are an important aspect for conformal acting (Padayachee 2012; Puhakainen and Siponen 2010; Vance and Siponen 2012). Conscious (C_{51}) acting is reflected, for example, *withdrawing of IT usage rights from another person due to personal differences,* while Not conscious (C_{52}) acting can be *not classifying documents for archiving because it was not communicated by the organization*.

The added value (D_6) as a dimension was most empirically extended. At this point, it is worth taking a closer look at the empirically derived characteristics of status (C_{63}), amusement (C_{64}), convenience (C_{65}) and None (C_{66}) for further research, in order to examine their relevance in ISP deviation research more closely. Status (C_{63}) was used as a character when, for example, the *usage of data of other persons as own misuse, in order to provide a personal advantage*. This could possibly refer to Huang et al.'s (2017) definition of competitional excellence and should be considered in more detail in future research. Examples of amusement (C_{64}) as an added value can be *manipulating the computer desktop of an employee who has forgotten to lock it* and was not mentioned in the literature thus far. Convenience (C_{65}) describes cases where ISPs have been violated in order to create more personal comfort. An example of this is *online shopping at work to avoid having to do it at home*. None (C_{66}) received cases as a characteristic where no added value for a person was apparent, such as *unconscious forgetting to archive unimportant e-mails, which had no impact on the company or the person themselves*. About existing characteristics in the literature, it has also been shown that they are valid within the sixth dimension of the ISP deviance taxonomy created here (Vance et al. 2012; Vance et al. 2013). For example, *ordering office supplies for private purposes at company's expense* can be used as an example of monetary (C_{62}) added value, and an Informative (C_{61}) added value is, for example, *the misuse of IS access rights in order to achieve a personal added value through secret information*.

Implications for Research

From the preparation of the taxonomy for ISP deviance, important implications for research could be successfully derived. In general, a taxonomy with both conceptual and empirical elements offers a holistic overview of ISP deviance research. On the basis of existing literature from the underlying field of research, but also from related fields, it was possible to use this as a basis, therein presenting it in a holistic, compact and descriptive way which is mutually exclusive and collectively exhaustive. Such an indication provides a solid basis for further research in the direction of Willison and Warketin's (2013) call for a clear demarcation of sub-areas of ISP deviance including applied theories. On the one hand, researchers can use this taxonomy to get an overview of existing dimensions and characteristics of this subject area where has not been intensive research so far. It could likewise be pointed out that especially in the empirically derived aspects such as added value, there are still open points with regard to ISP deviation research.

Based on the fact that literature from work deviance research and literature from criminology were also used, new fields of research open up through the transfer of constructs from related disciplines to ISP deviance research. It has been shown that dimensions and characteristics of other disciplines have their usefulness and have already been partially adapted in ISP deviance research, such as for the purposes of moral or motivational aspects, or additionally the target object of an action (Banerjee et al. 1998; Padayachee 2012). It was also possible to show where literature from other subject areas has been used for taxonomy creation and where none at all exists from one's own subject area. For example, the dimensions of constructiveness and added value were derived from the work deviance literature (Dahling and Gutworth 2017; Diefendorff and Mehta 2007) or strongly empirically expanded upon. Further potentials of the ISP deviance can be seen in the investigation of these areas. Likewise, a smaller proportion of literature could be identified in relation to the dimension of motivation and moral.

Implications for Practice

In addition to the implications for research, practical benefits can also be derived from the results of this work. Such a classification provides managers or IT security experts with a keen overview, along with the added incentive for the characterization and classification of IT security breaches in their company. Based on an existing classification, it is also possible to derive measures for a more compliant behavior of employees or to prevent this. This can also be observed, among other things, in the confirmation of previous recommendations from the literature, whereby it can be argued this study demonstrates the way in which misdemeanors are indeed caused by unconsciousness. In opposition to this possibility, Puhakainen and Siponen (2010) point out that, for example, targeted IT security training strengthens awareness of compliant behavior. The different dimensions and characteristics also help to better understand the behavior of employees, especially with regard to their expected added value through an act’s execution. The topic of constructiveness can also be taken up in practice in order to attempt to generate controlled added value for the company through such actions.

Limitations

Besides the presented results, this work also assumes some limitations. In general, it can be said that the taxonomy is not based on data collected from a specific industry, but rather provides a cross-sector view of the classification of ISP deviation. Sector specifics could therefore not be accounted for, of which could exist, for example, in very IT-heavy sectors such as software development. It can also be noted that another group of industries can display different results.

In addition, limitations with regard to the taxonomy and its creation in itself can be mentioned. First, it should be noted that taxonomies are based on the subjective assumptions of the researcher creating the taxonomy. Another researcher might, therefore, have different opinions about the classification of objects and the creation and modification of dimensions and characteristics. This is also related to the selected dimensions and characteristics. Yet, there exist other taxonomies in the ISP deviation which focus on other areas of research, leading to different dimensions and characteristics, such as Venkatraman et al. (2018) or other studies, who also classify their consequences or prerequisites in addition to the reasons for an offense (D'Arcy and Hovav 2007).

Based on the literature used and the objects analyzed, a consideration of external ISP violations were not considerable enough, detailing potential for future research. Likewise, only 40 persons could be interviewed, which entails the disregard for ISP deviation examples of other potential interview partners. In addition, the sample size did not allow a meaningful differentiation between individual job positions in connection with the developed taxonomy.

Future Research

The developed taxonomy for ISP deviance forms a basis for further research on ISP deviance with addressing the gap of the current literature of a holistic and deductively as well as empirical developed ISP taxonomy. In principle, it can be shown that the individual dimensions and characteristics of the taxonomy form sub-areas of the ISP deviance, where in fact a detailed investigation of the individual areas could be worthwhile. This is especially thought-provoking, since it could be shown at some points, e.g. the dimension of constructiveness, as an applicable aspect for ISP deviance, but only so far as has been considered in the ISP deviance literature. An analysis of applied theories and methods in the individual dimensions would be interesting for future studies because for the most part this point could not be considered in detail via the literature review of this study. Based on recurring examples during the interviews, a closer examination of the objects should be performed based on the taxonomy, as well as deriving suitable archetypes for ISP deviation, which both offer deeper insights into behavior patterns of non-compliant employees. Additionally, a more detailed investigation of the identified dimensions of ISP deviance can be carried out, whereby due to the importance of a context-related theory application (Willison et al. 2018) in the ISP environment, the attention can be concentrated on phenomena and theories considered so far in the different subsections of ISP deviance research.

In addition, it is worth considering the given dimensions and characteristics from a different perspective, e.g. with a focus on IT security attacks from outside on an organization. Another equally significant possibility would be the inclusion of other aspects, such as prerequisites for a violation or the evaluation of the associated consequences, which Venkatraman et al. (2018) have recently introduced. It is also worth considering other dimensions and characteristics from work deviance literature and criminology. The results of this study principally show many parallels between the ISP deviance research and the two research fields mentioned above, even if further elaboration is required.

Conclusion

ISP deviance is a growing topic in IS research and practice. It is becoming more and more important for companies to be able to understand IT abuse correctly and to derive corresponding countermeasures. The taxonomy we developed enables on the one hand to have a holistic overview of the different perspectives on ISP deviance combined in a taxonomy which was previously remarked as a gap in current ISP deviance research. In a broader sense, it provides a basis to investigate these different sub-areas in more detail, e.g. by using archetypes for each dimension of the taxonomy or by considering previously applied theories in the different areas. On the other hand, there were also parallels to other research areas such as criminology and work deviance identified as relevant in ISP deviance which helps to spread an idea about other factors influencing deviant behavior in an ISP context and opens a broad field of currently not considered theoretical concepts to be analyzed in further research.

References

Bailey, K. D. 2003. *Typologies and taxonomies: An introduction to classification techniques*, Thousand Oaks, Calif.: Sage Publ.

Banerjee, D., Cronan, T. P., and Jones, T. W. 1998. "Modeling IT Ethics: A Study in Situational Ethics," *MIS Quarterly* (22:1), pp. 31–60.

Bennett, R. J., and Robinson, S. L. 2000. "Development of a Measure of Workplace Deviance," *Journal of Applied Psychology* (85:3), pp. 349–360.

Bharadwaj, A., El Sawy, O. A., Pavlou, P. A., and Venkatraman, N. 2013. "Digital Business Strategy: Toward a Next Generation of Insights," *MIS Quarterly* (37:2), pp. 471–482.

Bulgurcu, Cavusoglu, and Benbasat 2010. "Information Security Policy Compliance: An Empirical Study of Rationality-Based Beliefs and Information Security Awareness," *MIS Quarterly* (34:3), pp. 523–548.

Charlier, S. d., Giumetti, G. W., Reeves, C. J., and Greco, L. M. 2017. "Workplace Cyberdeviance," in *The Wiley Blackwell handbook of the psychology of the Internet at work*, G. Hertel (ed.), Hoboken, NJ: John Wiley et Sons, Ltd, pp. 131–156.

Cheng, L., Li, Y., Li, W., Holm, E., and Zhai, Q. 2013. "Understanding the violation of IS security policy in organizations: An integrated model based on social control and deterrence theory," *Computers & Security* (39), pp. 447–459.

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

Clinard, M. R., Quinney, R., and Wildeman, J. 2014. *Criminal behavior systems: A typology:* Routledge.

Colbert, A., Yee, N., and George, G. 2016. "The Digital Workforce and the Workplace of the Future," *Academy of Management Journal* (59:3), pp. 731–739.

Dahling, J. J., and Gutworth, M. B. 2017. "Loyal rebels? A test of the normative conflict model of constructive deviance," *Journal of Organizational Behavior* (38:8), pp. 1167–1182.

D'Arcy, J., and Hovav, A. 2007. "Deterring internal information systems misuse," *Communications of the ACM* (50:10), pp. 113–117.

D'Arcy, J., Hovav, A., and Galletta, D. 2009. "User Awareness of Security Countermeasures and Its Impact on Information Systems Misuse: A Deterrence Approach," *Information Systems Research* (20:1), pp. 79–98.

David Geiger, Stefan Seedorf, Thimo Schulze, Robert C. Nickerson, and Martin Schader 2011. "Managing the Crowd: Towards a Taxonomy of Crowdsourcing Processes," in *AMCIS*.

Diefendorff, J. M., and Mehta, K. 2007. "The Relations of Motivational Traits With Workplace Deviance," *Journal of Applied Psychology* (92:4), pp. 967–977.

Farr, K. A., and Gibbons, D. C. 1990. "Observations on the Development of Crime Categories," *International Journal of Offender Therapy and Comparative Criminology* (34:3), pp. 223–237.

Gannon, B. 2013. "Outsiders: An Exploratory History of IS in Corporations," *Journal of Information Technology* (28:1), pp. 50–62.

Glass, R. L., and Vessey, I. 1995. "Contemporary application-domain taxonomies," *IEEE Software* (12:4), pp. 63–76.

Guo, K. H., and Yuan, Y. 2012. "The effects of multilevel sanctions on information security violations: A mediating model," *Information & Management* (49:6), pp. 320–326.

Höne, K., and Eloff, J.H.P. 2002. "Information security policy — what do international information security standards say?" *Computers & Security* (21:5), pp. 402–409.

Hsu, J. S.-C., Shih, S.-P., Hung, Y. W., and Lowry, P. B. 2015. "The Role of Extra-Role Behaviors and Social Controls in Information Security Policy Effectiveness," *Information Systems Research* (26:2), pp. 282–300.

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

Huang, G.-H., Wellman, N., Ashford, S. J., Lee, C., and Wang, L. 2017. "Deviance and exit: The organizational costs of job insecurity and moral disengagement," *Journal of Applied Psychology* (102:1), pp. 26–42.

Lembcke, B., Hengstler, S., Plics, P., Pamuk, M., and Trang, S. 2018. *Information Security Behavior: Comparing the Predictive Power of Social Learning Theory and Deterrence Theory*, Göttingen.

McDevitt, J., Levin, J., and Bennett, S. 2002. "Hate Crime Offenders: An Expanded Typology," *Journal of Social Issues* (58:2), pp. 303–317.

Moody, G. D., Siponen, M., and Pahnila, S. 2018. "Toward a Unified Model of Information Security Policy Compliance," *MIS Quarterly* (42:1), 285 - A22.

Nickerson, R., Muntermann, J., and Varshney, U. 2010. "Taxonomy Development in Information Systems: A Literature Survey and Problem Statement," *AMCIS 2010 Proceedings*.

Nickerson, R. C., Varshney, U., and Muntermann, J. 2013. "A method for taxonomy development and its application in information systems," *European Journal of Information Systems* (22:3), pp. 336–359.

Padayachee, K. 2012. "Taxonomy of compliant information security behavior," *Computers & Security* (31:5), pp. 673–680.

Posey, C., Roberts, T. L., Lowry, P. B., Bennett, R. J., and 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), pp. 1189–1210.

Puhakainen, and Siponen 2010. "Improving Employees' Compliance Through Information Systems Security Training: An Action Research Study," *MIS Quarterly* (34:4), pp. 757–778.

Robinson, S. L., and Bennett, R. J. 1995. "A Typology of Deviant Workplace Behaviors: A Multidimensional Scaling Study," *Academy of Management Journal* (38:2), pp. 555–572.

Siering, M., Clapham, B., Engel, O., and Gomber, P. 2017. "A Taxonomy of Financial Market Manipulations: Establishing Trust and Market Integrity in the Financialized Economy through Automated Fraud Detection," *Journal of Information Technology* (32:3), pp. 251–269.

Sohrabi Safa, N., Solms, R. von, and Furnell, S. 2016. "Information security policy compliance model in organizations," *Computers & Security* (56), pp. 70–82.

Stanton, J. M., Stam, K. R., Mastrangelo, P., and Jolton, J. 2005. "Analysis of end user security behaviors," *Computers & Security* (24:2), pp. 124–133.

Tilson, D., Lyytinen, K., and Sørensen, C. 2010. "Research Commentary —Digital Infrastructures: The Missing IS Research Agenda," *Information Systems Research* (21:4), pp. 748–759.

Trang, S. 2018. "When Does Deterrence Work? A Moderation Meta-analysis of Employees' Information Security Policy Behavior," in *Proceedings of the Thirty ninth international conference on information systems 2018*.

Vadera, A. K., Pratt, M. G., and Mishra, P. 2013. "Constructive Deviance in Organizations," *Journal of Management* (39:5), pp. 1221–1276.

Vance, A., Lowry, P. B., and Eggett, D. 2013. "Using Accountability to Reduce Access Policy Violations in Information Systems," *Journal of Management Information Systems* (29:4), pp. 263–290.

Vance, A., Siponen, M., and Pahnila, S. 2012. "Motivating IS security compliance: Insights from Habit and Protection Motivation Theory," *Information & Management* (49:3-4), pp. 190–198.

Vance, A., and Siponen, M. T. 2012. "IS Security Policy Violations," *Journal of Organizational and End User Computing* (24:1), pp. 21–41.

Venkatraman, S., M. K. Cheung, C., Lee, Z. W. Y., D. Davis, F., and Venkatesh, V. 2018. "The "Darth" Side of Technology Use: An Inductively Derived Typology of Cyberdeviance," *Journal of Management Information Systems* (35:4), pp. 1060–1091.

Venter, H., Eloff, M., Labuschagne, L., Eloff, J., and Solms, R. von (eds.) 2007. *New Approaches for Security, Privacy and Trust in Complex Environments,* Boston, MA: Springer US.

Walsh, I., Gettler-Summa, M., and Kalika, M. 2016. "Expectable use: An important facet of IT usage," *The Journal of Strategic Information Systems* (25:3), pp. 177–210.

Warren, D. E. 2003. "Constructive and Destructive Deviance tn Organizations," *Academy of Management Review* (28:4), pp. 622–632.

Webster, J., and Watson, R. T. 2002. "Analyzing the Past to Prepare for the Future: Writing a Literature Review," *MIS Quarterly* (26:2), pp. xiii–xxiii.

Willison, R., and Warkentin, M. 2013. "Beyond Deterrence: An Expanded Views of Employee Computer Abuse," *MIS Quarterly*