Towards a Taxonomy of Information Security Policy Non-Compliance Behavior

Sebastian Hengstler
Chair of Information Security and Compliance, University of Goettingen, Germany
s.hengstler@stud.uni-goettingen.de

Robert C. Nickerson
San Francisco State University
rnick@sfsu.edu

Simon Trang
Chair of Information Security and Compliance, University of Goettingen, Germany
simon.trang@wiwi.uni-goettingen.de

Abstract

Due to the increasing digitalization of our society, IT security professionals must implement even more effective security measures to meet the growing information security requirements of their organizations. To target and effectively deploy these measures in the best possible way, they must consider different types of behaviors that might lead to information security threats. Regarding this issue, current research offers little for clarity to security professionals when it comes to understanding and differentiating the various types of behavior. Therefore, this research aims to develop a taxonomy to classify different types of information security policy non-compliance behavior. Our results present a taxonomy with five dimensions, each containing mutually exclusive and collectively exhaustive characteristics. Our results provide a basis for a more specific analysis of different types of information security policy non-compliance behavior and can be used for more comprehensive development and analysis of appropriate security measures.

1. Introduction

Over the last two decades, ensuring information security has become one of the most important tasks in organizations [1]. However, accomplishing this task is rather challenging. Research and practice agree that to achieve a high level of information security within an organization, it is crucial to implement technical measures and some appropriate methods to prevent non-compliant behavior of employees regarding information security policies (ISP) [2]. ISPs can be described as "a set of formalized procedures, policies, roles and responsibilities that employees must follow in order to protect and properly use their organizations' information and technology resources" and are used to derive security measures for different types of security threats [3]. On the one hand, an information security expert is faced with the challenge that there are many different types of non-compliant behaviors. Keeping them straight is a prerequisite to selecting appropriately effective measures that positively influence employee's ISP non-compliance behavior [4]. On the other hand, the information security researcher is faced with the complex task of characterizing and purposefully structuring these various types of ISP non-compliance behavior to develop security measures against it [5].

Considering the fact that employees' non-compliant behavior is one of the leading causes of security breaches in an organization [6], it is mandatory to have a closer examination of the variety of types of ISP non-compliant behaviors to understand better the different aspects which lead to a certain information security threat [1]. However, current research about ISP non-compliance behavior uses the construct of ISP non-compliance behavior in various ways. While some approaches by, e.g., Lembke et al. (2018), focus on behavior in a specific context (e.g., information distribution between organizations), other research approaches aim to provide unified models to explain ISP compliance behavior [6, 7]. Nonetheless, the usage of context-specific or generalized results becomes complicated when the underlying contexts of non-compliance behavior change. For example, the findings of Trang and Brendel (2019) illustrate that theoretical constructs (e.g., sanctions) can have different effects, depending on a certain type of behavior, such as maliciousness or non-maliciousness [8]. Aurigemma and Mattson (2019) show that there is substantial behavioral variability in ISP mandated actions and that a distinction between different types of ISP-related behaviors is important since the effectiveness of theoretical constructs differs in terms

URI: https://hdl.handle.net/10125/79925
978-0-9981331-5-7

of its measurement [9]. This discussion underlines that the different types of behavior need to be defined and systematized [10].

One possible way to define this variety of types of ISP non-compliant behavior is to use a taxonomy. Taxonomies are implemented in various research areas to reduce complexity by identifying and abstractly representing the commonalities and differences among objects of interest within the domain [11]. The organization of objects into different dimensions and characteristics can help create structure in a complex subject area and is also seen, among other things, as a form of theory building or basic design principle that can serve as a foundation for further research [12]. As we will show in the course of this paper, classification of security threats exists in research, although little has been done to define different dimensions and characteristics for types of ISP non-compliant behavior. While there are approaches to describe various factors of non-compliant behavior, these do not meet the definition of taxonomy and can only be used to a limited extent as a theory- or design basis in our research area [13]. Accordingly, this paper applies a conceptual and empirically driven taxonomy development, as Nickerson et al. (2013) suggested.

Drawing on existing research, we first develop a conceptual approach for our taxonomy, followed by interviews with employees from different organizations to extend the taxonomy. The interviews were evaluated using structured content analysis [14]. Our taxonomy is designed to help information security researchers to identify the different types of ISP non-compliant behavior for other behavior-specific research. Information security practitioners can use our taxonomy to distinguish better the different reasons for a security threat and develop measures that effectively address the actual reason and not just the non-compliant behavior.

The rest of this paper is structured as follows: after the introduction, the construct of taxonomies is described together with an overview of information security policy compliance behavior. Next, the method and procedure for taxonomy development, including the method for our data collection and analysis, are presented. Afterward, we explain how the taxonomy was created and discuss our outcome. The paper concludes with implications for research and practice, as well as limitations of the paper and actions for future research.

2. Background

2.1. Information security policy compliance behavior

Recently, there has been a growing stream of research on the human perspective of information security, which focuses on the different types of employee' behavior regarding the ISPs of their organization. The focus of this research stream is predominantly on identifying theoretical mechanisms, which help achieve ISP compliance behavior. Existing research shows that different factors contribute to the compliance behavior of employees, such as sanctions or rewards, or that social factors can have an influence on ISP compliance behavior [6]. It also shows that contextual differences are important in the use of these factors [9]. For example, research indicates that the effectiveness of several mechanisms that positively influence ISP compliance behavior are culturally dependent [15]. For example, the current state of research indicates that sanctions are more effective for malicious ISP violations [16]. Venkatraman et al. (2018) also show that different types of offenses can have a smaller or bigger impact on an organization [13]. Therefore, we follow previous research findings and their conclusions that a precise understanding and separable distinction of behaviors (which, e.g., drive employees to adhere to roles and responsibilities defined in ISPs) play a central role in developing effective security measures.

Considering existing research results on how information security behavior can be described and distinguished in classification schemes, such as a taxonomy, several approaches can be identified. Venkatraman et al. (2018), e.g., show that a schematic distinction of cyber deviance is important to define effective security measures. However, in their empirically developed typology, they focus firstly on descriptive factors of behavior, secondly, more on characteristics that constitute ISP offenses in an organization, and thirdly, what behavior has led to these different offenses. They list dimensions such as: which technical skills are needed, the target group (an individual or the organization), the impact of the offense (minor or major), and list different behaviors as typical examples for these types of security threats. They focus less on the nature and different components of the behavior itself, ultimately becoming an ISP offense [13].

Padayachee (2012) developed a taxonomy for compliant information security behavior related to the motivation factor. Based on the self-determination theory, the three factors of intrinsic, extrinsic, or amotivation are presented as decisive motivating

factors for compliance behavior in a hierarchical taxonomy. We suggest taking a closer look at those three factors. Intrinsic motivation refers to performing an activity because it is inherently interesting, while extrinsic motivation means performing an activity because it could lead to an expected outcome [4]. Amotivation is defined as a 'state of lacking an intention to act and not feeling competent enough to perform a certain activity [17].

Das et al. (2019) specify these motivational factors and argue that there are different types of triggers for information security non-compliance behavior. They distinguish between self-motivation, which relates to intrinsic motivation, and forced or social triggers, which refer to extrinsic motivation. A forced motivational trigger describes an influencing factor, which is not caused by an external source around an employee, while a social trigger suggests a source located in an employee's social environment, e.g., their team or close friends [17, 18].

Ahmad et al. (2016) distinguish between two dimensions in their typology for employees' information security behavior. Their typology indicates that information security behavior differs with respect to whether an employee is aware of the non-compliance of their behavior or not [19]. Guo et al. (2011) also distinguish between different behavioral concepts and state that behavior can be malicious or non-malicious [20]. They describe malicious behavior as an attitude intending to harm another person or their organization with a particular act. Non-malicious behavior refers to behavior that is intended to help oneself, e.g., by saving time and effort, without directly harming another person or the organization [20]. Vance et al. (2020) closely relate moral belief to behavioral intention and argue that individuals can have various moral beliefs, which influence the way they behave. Moral beliefs are the subjective opinions of what employees regard as morally right or wrong and are mostly based on ethics, religion, cultural differences or the social environment [21].

Overall, different elements can be identified in existing research that describes types of ISP non-compliance behavior, such as awareness, different motives, or moral beliefs [4, 19, 20]. However, existing research currently does not fulfill the need for a holistic approach to differentiate between different types of ISP non-compliance behavior systematically. When considering the importance of contextual relevance in ISPCB research, it is necessary to gain an overview to understand better which specific types of behavior can be influenced by which types of theoretical models [9]. Therefore, we conceptually and empirically developed a taxonomy to fulfill this need and form a theoretical basis for more specific ISP compliance behavior research [11].

2.2. Taxonomies in research

In existing research, the use of taxonomies various objectives and under different premises can be identified. Before the actual development of the taxonomy, we need to present what exactly a taxonomy is. A taxonomy is often described as a tool for classifying objects and information to illustrate complex fields of interest [22]. Thus, it is a useful method to explore a less-analyzed or very heterogeneous area, where many different research approaches with different focuses exist. Besides the numerous uses of taxonomies in other fields, such as biology [23], there is a lack of usage of this methodology in information systems research. Thus, Gregor (2006) notes that there is a need for the development of typologies (definition often used synonymously with a taxonomy) to structure constructs and relationships of complex research strands and thereby provide a solid foundation for further study [11, 12]. From the practical environment or the research field, this enables their viewers to gain an appropriate overview of a particular subject [24, 25. In IS research, and in research in other domains, there are different approaches to the development of taxonomies [13]. In addition to taxonomy development using ad hoc methods, some methods perform an empirical derivation of a taxonomy or methods with a predominantly conceptual or mixed approach [23].

We use the definition of a taxonomy given by Nickerson et al. (2013) since their definition finds application in various research areas, including IS research. A taxonomy can be described as a set of dimensions, where each dimension consists of mutually exclusive and collectively exhaustive characteristics. The characteristics form a particular expression of the respective feature (dimension) [11]. The respective characteristics must not occur twice or interfere with each other. Likewise, each dimension must contain at least one characteristic so that the taxonomy is descriptive and there are sufficiently enough details of the analyzed objects. A taxonomy based on these criteria is called a flat taxonomy, where there are usually no dependencies between the expressions of characteristics of different dimensions at a categorized object. Hierarchical taxonomies are classification schemes in which characteristics of a dimension are themselves a dimension for other characteristics. However, a facet taxonomy allows a characteristic to be assigned to multiple dimensions, which allows the classification to be ordered in

multiple ways rather than in a single, predetermined constellation of dimensions and characteristics (as in a flat or hierarchical taxonomy) [26]. Facet taxonomies are often used to create, e.g., system architectures and are rather unsuitable for our objective of the structured classification of objects [27]. This research focuses on the creation of a flat taxonomy. The methodology for its creation was adapted from Nickerson et al. (2013) [11].

3. Methodological approach for taxonomy development

We used a multistep, iterative method based on Nickerson et al. (2013) to create our taxonomy for information ISP non-compliance behavior [11]. This approach was applied because this method focuses on (but is not limited to) the development of taxonomies in the IS domain and better organizes our results in the research stream [25]. In addition, this methodology provides a clear framework (meta-characteristic) for taxonomy development, to which all inferred dimensions and characteristics relate, making the taxonomy more focused. Apart from that, the methodology defines subjective and objective end conditions as measures to progressively finalize an iterative taxonomy development in empirical and/or conceptual steps. Moreover, detailed steps are introduced to ensure that all features in the dimension are mutually exclusive and that there are no duplications or ambiguities. The approach thus combines advantages from purely empirical and purely conceptual approaches to taxonomy development [11].

According to Nickerson et al. (2013), a taxonomy must fulfill five criteria to ensure high usability and quality. First, the number of dimensions and characteristics should be limited in order to make a concise possible use of the taxonomy. Second, there should be enough dimensions and characteristics to 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, whether they predefined from an empirical or conceptual approach. Fourth, a taxonomy should be extendable by dimensions and characteristics, whereas it becomes necessary to consider new objects, and fifth, a taxonomy should be descriptive [11].

Our used methodical approach for taxonomy development is shown in Figure 1 and can be described as followed. As an initial step, the meta-characteristic, which reflects the most general characteristic of the taxonomy from which all other characteristics follow, should be determined. The user group of the taxonomy should be considered when determining the meta- characteristic, as they have an impact on the content of the taxonomy. This process can be done explicitly, based on derivations from the users, or implicitly, based on the researcher's assumptions [28]. The meta-characteristic for this article can be defined as determining elements describing different types of ISP non-compliance behavior in a professional context. Information security researchers can use our results to understand the phenomenon of ISP non-compliance behavior with different degrees of orientation and organization and apply the taxonomy as a theoretical basis for more specific research, such as a specific type of behavior. Professionals can use our taxonomy to develop targeted measures for different behaviors to ensure information security in their organization. As a subsequent step in taxonomy development, the ending conditions need to be defined, in which case the iterative development of the taxonomy will be terminated, and the taxonomy will be considered complete. These criteria can be both objective and subjective. Subjective ending conditions are reflected in the mentioned quality criteria above. Objective ending conditions can be defined according to the approach and needs of the respective user. We adapted the ending conditions of Sowa and Zachman (1992) [29]. In the subsequent steps of the approach, users of the method can choose again between either a deductive or an empirical approach.

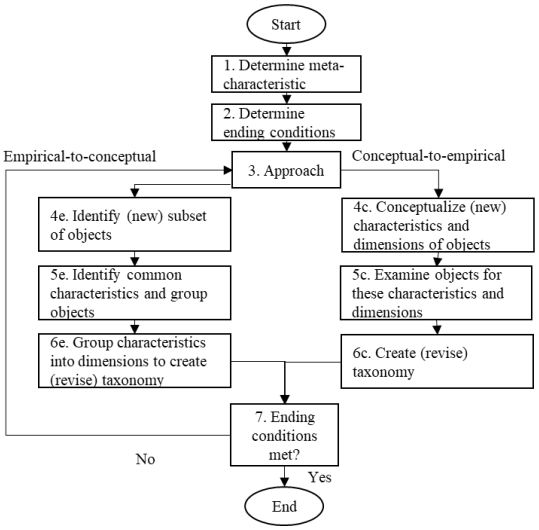

Figure 1. Process of taxonomy development [11].

Each iteration must be defined in advance whether one of the two approaches is to be chosen. In the deductive approach, the dimensions and characteristics of the taxonomy are defined and

arranged firstly 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. In the first place, the objects to be analyzed are considered, and new dimensions and characteristics are formed and organized 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. If the existing taxonomy fulfills all defined ending conditions, the taxonomy is considered complete, and the development process ends [11, 23].

4. Results

4.1. Taxonomy development process and descriptive statistics

The process for developing the taxonomy in this study is illustrated in figure 2. In total, we conducted three iterations in which we developed the taxonomy using both conceptual and empirical approaches.

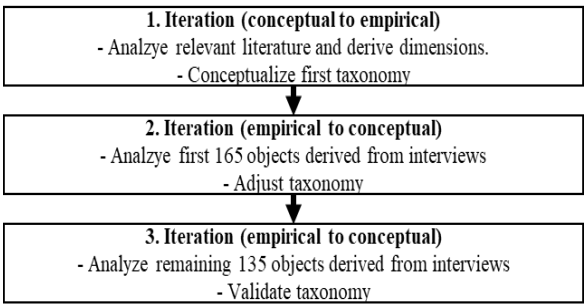

Figure 2. The number of iterations for the taxonomy development.

Our first iteration followed a conceptual-to-empirical approach. We analyzed existing literature describing elements that could be used to classify ISP non-compliance behavior. We apply constructs of existing research to define our first set of dimensions and characteristics. The second iteration is based on an empirical-to-conceptual approach. We conducted 58 interviews with professionals working in an organization with information security policies. Our interview partners were asked to explain different situations in which they felt to behave non-compliant or where they might have observed information security non-compliance behavior of other employees in their organization. Our method was a semi-structured interview approach. The interviews were recorded and documented. The conducted data were analyzed using a structured content analysis approach based on Mayring (2010) [14]. The descriptive statistics for our data sample are shown in Table 1. The average age of our subjects was 31 years old. 60% of the subjects were male, and 40% were female. The majority of subjects work in large corporations with more than 10000 employees (57%), 26% work in medium-sized companies (>250-9999 employees), and 17% work in small companies with fewer than 250 employees. The departments represented vary.

Table 1. Descriptive statistics of the conducted interviews.

Department	Amount	Industry	Amount
IT	16%	Manufacturing	38%
Sales	16%	Biotechnology	16%
Administration	14%	Finance industry	14%
Process mgmt.	10%	Food industry	10%
Marketing	9%	Event mgmt.	6%
Production	9%	Legal	4%
Research & development	9%	Insurances	4%
Purchasing	5%	Music industry	2%
Finance	4%	Mechanical engineering	2%
Human resources	3%	Mining industry	2%
Legal department	3%	Consulting	2%
Quality	2%		

We were able to identify 300 situations of our interview partners in which they intended to behave non- compliantly according to the ISPs of their organization. We used their experience in these situations as objects and classified them with our conceptual-to-empirical derived taxonomy from the first iteration.

During the analysis of the objects, we were able to identify new dimensions and characteristics. After 165 objects were analyzed, we reached a certain level of maturity and could not derive any additional dimensions or characteristics from the analyzed objects. Therefore, we decided to stop the second iteration. In the third iteration, an empirical-to-conceptual approach was chosen again to classify the remaining 135 objects using the taxonomy from the second iteration. No new dimensions or characteristics were identified during this analysis. After the third iteration, we additionally had to check whether the ending conditions defined at the beginning were fulfilled. We analyzed a representative number of objects for our analysis because we were able to show

that at least one object is assigned to each characteristic of each dimension, and after a certain number of assigned objects, no new dimensions or characteristics could be identified. No new dimensions and characteristics were added during the last iteration, and no new dimensions and characteristics were split or assigned during the last iteration. Each dimension and characteristic is unique and has not been repeated, meaning duplicates do not exist, and each cell of the taxonomy is unique and has not been repeated. We conducted an independent review of five information security research experts to test our subjective ending conditions. The experts confirmed the describability, robustness, extensibility, and completeness of the taxonomy [29].

4.2. A taxonomy for information security policy non-compliance behavior

In total, our taxonomy consists of five dimensions and 16 characteristics which follows the suggestion of Nickerson et al. (2103) [11]. Table 2 shows our final taxonomy, including a description of the dimensions and characteristics. We further show whether the dimensions and characteristics were derived from existing literature or an outcome of our structured content analysis.

Table 2. Final taxonomy for information security policy non-compliance behavior (C = conceptual, E = empirical).

Moral Beliefs [21] (C)	
Characteristics	**Description**
Personal Moral (C)	Personal moral beliefs describe the view that what an individual thinks is morally right or wrong and thus influences their intention and behavior.
Organizational Moral (C)	Organizational moral beliefs describe the view that what an employee thinks is morally right or wrong when acting as a representative of it's organization andthus influences their intention and behavior.
Awareness [5] (C)	
Conscious (C)	The characteristic "conscious" describes the behavioral state in which an employee is aware of its non-compliant behavior regarding information securitypolicies.
Not Conscious (C)	The characteristic "not conscious" describes the behavioral state in which an employee is not aware of its non-compliant behavior regarding information security policies.
Motive [20] (C)	
Beneficial (E)	A motive is classified as "beneficial" when an employee with a violation of the ISP intends to effect something positive toward another person or their organization.
Malicious (C)	The motive is classified as "malicious" when it is apparent from an employee's behavior that they intend to harm another person or their organization withan ISP security threat.
Not Malicious (C)	Motive is classified as "not malicious" when it is apparent from an employee's behavior that they do not intend to harm another person or their organizationwith an ISP security breach.
Expected Outcome (E)	
Informative (E)	The expected outcome of a particular behavior is classified as "informative" if anemployee hopes to gain informative value from non-compliant behavior.
Monetary (E)	The expected outcome of a particular behavior is classified as "monetary" if an employee hopes to get a monetary reward when not complying with ISP's.
Status (E)	The characteristic "status" describes the expected outcome of non-compliance behavior, from which an employee hopes to improve their reputation.
Amusement (E)	The characteristic "amusement" refers to behavior in which an ISP threat is being performed to amuse the performer of the threat.
Convenience (E)	The expected outcome of a particular behavior is classified as "convenience" if anemployee seeks to benefit, such as saving to or effort from non-complying with the ISP of their organization.
None (E)	If no specific outcome is expected through information security non-compliancebehavior, the behavior is classified with the characteristic "none."
MotivationalTrigger [4, 18] (C)	
Extrinsic (social) (E)	Extrinsic (social) motivational trigger refers to an external influence on an employee from its social environment, which leads to ISP non-compliance behavior.
Extrinsic (forced) (C)	Extrinsic (forced) motivational trigger refers to an external influence on an employee, pushing pressure on them and leading to information security non-compliance behavior.
Intrinsic (proactive) (C)	The intrinsic (proactive) motivational triggers refer to behavior, which is only motivated by an employee's motives and not directly shaped by its external environment.

The dimension “Moral Beliefs” was derived with its characteristics of personal and organizational morals considering empirical iteration from the concepts according to Vance et al. 2020 [21]. The results of our interviews show that information security non-compliance behavior can differ in terms of moral belief in personal or organizational morality [30]. Behaviors with personal morality often refer to situations in which employees acted from their perspective, e.g., to generate added value for themselves. Organizational morality can be seen in behaviors where employees commit a security breach to provide added value to the organization, such as finishing work outside working hours and using private hardware.

The dimension “Awareness” with its characteristics was derived from existing literature [5]. The characteristic “Not Conscious” could be identified in behaviors where an employee did not immediately know when committing the violation that it was a violation of the ISP. However, the characteristic “Conscious” was used to classify behaviors in which the interviewees were aware, that their behavior violated their organization's ISP.

The “Motive” can be divided into a total of three different characteristics, where malicious and non-malicious refer to the constructs according to Guo et al. (2011), and the characteristic “Beneficial” is a result of the structured content analysis of the empirical-conceptual, second iteration and was derived from the objects we analyzed [20]. Types of behavior that provide added value to the organization were characterized as beneficial. An example of such behavior is, e.g., that an employee sent company information to the private e-mail address to complete work on private hardware and thought that they were doing something good for the organization. Malicious behavior can be classified as when employees actively intended to harm their target with their violation, such as using system privileges to steal information from other employees for their own added value. Non-malicious behavior represents the opposite of malicious behavior, where an employee had no malicious intent in their behavior, such as browsing away work time.

The “Expected outcome” is a dimension that we defined from the results of the structured content analysis during the second iteration. It consists of six different characteristics. The characteristic “Informative” was used to classify types of behavior in which the committing person obtained additional, needed information that he or she would not have obtained without the act. For example, one interview person used a system access to view team members' salaries and have a better bargaining point for the next salary negotiation. The expected outcome, “Monetary” was used to classify behaviors where the expected added value was for improving the financial situation of the committing person, such as stealing information for sale to third parties. Another expected added value is improving status, where employees expected their behavior to increase their reputation. The characteristic “Amusement” was used to classify behaviors that were done solely for the amusement of the perpetrators, such as changing the background images of other employees because they did not lock their PC screens and left the workplace for a short time. Other objects could be classified in this dimension by ”Convenience.” We were able to identify behaviors that have their added value in convenience or, for example, saving time. We were able to identify the characteristics of online shopping during working hours or the use of company hardware for private purposes, such as network printers. When employees reported types of behavior where no direct added value could be attributed to them, the characteristic “None” was used. An example of this is the use of digital company discounts for third parties.

The dimension “Motivational trigger” is divided into three different characteristics. These are based on the constructs identified by Padayachee (2012) and Das et al. (2019) [4, 18]. We were able to assign to the social (extrinsic) characteristic types of behavior in which an individual reported that he or she chooses to violate information security policies for social reasons. For example, one individual reported that they obtained information in a non-compliant manner and disclosed it to the legal system to prevent socially non-compliant organizational behavior (cheating). Under the characteristic forced (extrinsic), behaviors were classified in which employees were forced to behave in a certain way by external influences. For example, a person was forced by their manager to pass on unencrypted company information to others via unauthorized distribution channels. The third characteristic, intrinsic (proactive), was used to classify behaviors in which individuals committed an ISP offense out of their own motivation, such as using company software to avoid buying it themselves or saving time. Table 3 shows examples for classified objects to determine different types of ISP non-compliance behavior according to our taxonomy.

Table 3. Classified ISP non-compliance behavior using the taxonomy.

Exemplary non-compliant behavior	Taxonomy classification
Using private hardware to finish work at home: "I once sent a corporate presentation to my private mail address to finish my work at home because there was no time to finish it in the office. I know that we are actually not allowed to do it, but I wanted to finish my work to hold the deadlines for this task."	**Moral Beliefs**: Organizational Moral **Awareness**: Conscious **Motive**: Beneficial **Expected Outcome**: status **Motivational Trigger**: Intrinsic (proactive)
Online shopping during work time: "Sometimes I do online shopping during work when I have not much to do. I know it is not allowed, but I think if I have the time to do it during work, I don't have to it at home."	**Moral Beliefs**: Organizational Moral **Awareness**: Conscious **Motive**: Beneficial **Expected Outcome**: status **Motivational Trigger**: Intrinsic (proactive)
Inviting external people to online company meetings: "It happened from time to time that colleagues asked me to invite people from outside of the organizations to participate in our corporate meeting, like a conference. I did not know that this was a security threat until someone told me."	**Moral Beliefs**: Personal Moral **Awareness**: Not Conscious **Motive**: Not malicious **Expected Outcome**: None **Motivational Trigger**: Extrinsic (forced)
Stealing software: "Once I used a software license key for private purposes. My organization did not control the license usages, so I just installed the software on my private device to save money".	**Moral Beliefs**: Personal Moral **Awareness**: Conscious **Motive**: malicious **Expected Outcome**: Monetary **Motivational Trigger**: Intrinsic (proactive)
Unauthorized installation of software: "I really had to finish work, but my organization was not able to provide me the software I needed. So I just bypassed the administration rights and installed it on my own to go forward in my project".	**Moral Beliefs**: Organizational Moral **Awareness**: Conscious **Motive**: Beneficial **Expected Outcome**: Informative **Motivational Trigger**: Intrinsic (proactive)
Forward confidential information to not involved colleagues: "I have shared confidential information with other colleagues to alert them of problems in their organization, even though I was not allowed to share the information."	**Moral Beliefs**: Organizational Moral **Awareness**: Conscious **Motive**: Not malicious **Expected Outcome**: None **Motivational Trigger**: Extrinsic (social)
Using corporate hardware for private purposes: "I used my corporate laptop for private purposes because I did not know that it is forbidden. It helped me to save time because I did not have to switch the devices all the time."	**Moral Beliefs**: Personal Moral **Awareness**: Not Conscious **Motive**: Not malicious **Expected Outcome**: Convenience **Motivational Trigger**: Intrinsic (proactive)

5. Discussion

By reviewing existing literature, conducting expert interviews, and structuring our findings in the form of a taxonomy using a method from Nickerson et al. (2013), we developed a taxonomy for types of ISP non-compliance behavior in this paper. It is an important milestone for structuring different behaviors regarding information security [11]. This paper makes several theoretical contributions. In the first place, it provides a comprehensive overview of how ISP non-compliance behavior can be classified. This allows researchers to distinguish the different behaviors from each other and analyze what mechanisms positively influence the different types of behaviors. It makes it possible for researchers in the future to respond to different contextual differences, such as types of offenses and to understand the origin of these more precisely, and analyze them specifically. Also, our taxonomy provides characteristics for differentiating behaviors that allow us to design specific awareness measures for the different behaviors. Design science research in the security awareness domain can use our taxonomy as a basis for designing specific security measures.

In addition to our theoretical contribution, we can furthermore present practical benefits of our work. Our taxonomy provides a keen overview for IT managers or IT security experts about the different aspects they have to consider when designing and using different information security measures. Based on our classification scheme, it is possible to derive measures for specific types of behavior, such as targeted awareness programs, based on behaviors where employees were not aware of their offenses or specific measures against the different types of expected added values. Further possibilities would be, e.g., the use of behavior with organizational moral or beneficial intention to achieve a positive effect on information security, e.g., promoting an information security culture [32].

Besides the presented results, this work also has some limitations. Our taxonomy is not based on data collected from a specific industry but rather provides a cross-sector view of the classification of types of ISP non-compliance behavior. Therefore, sector specifics could not be explicitly considered as in, e.g., strong

regulated sectors, such as the airspace or military industry. Additionally, 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. In addition, the sample size does not allow a meaningful differentiation between individual job positions in connection with the developed taxonomy. Moreover, a broader range of interviews might reveal other dimensions or characteristics useful for the taxonomy. For example, contextual differences such as different occupations or demographic dependencies could not be taken into account. This also applies to the different effects of the identified elements of our taxonomy on ISP non-compliance behavior. The dimensions and characteristics may depend on other factors that influence their mode of action but are too complex to be represented in a taxonomy. For example, it can be seen that moral beliefs or behavioral intention can be influenced by factors such as culture but could not be included in our taxonomy due to their complexity. Future studies based on our taxonomy must take these influencing factors into account.

However, our results show potentials for further research on information security behavior with addressing the gap in existing research of a holistically and analytically as well as empirically developed taxonomy. Essentially, it becomes clear that the individual dimensions and characteristics of the taxonomy form sub-areas of ISP non-compliance behavior. In addition to that, a detailed investigation of the individual areas could be beneficial. This is especially thought-provoking since it could be shown at some points, e.g., the relation between behavior and a certain expected outcome of a security threat has been less considered in research so far. An analysis of applied theories and methods in the individual dimensions would be interesting for future studies to understand better which theoretical mechanisms work for specific behavior types. Based on recurring examples during the interviews, a closer examination of the different behaviors should be carried out, based on the taxonomy, as well as deriving suitable archetypes for ISP non-compliance behavior. Both approaches could offer deeper insights into ISP non-compliance behavior patterns. Additionally, a more detailed investigation of the identified dimensions of our taxonomy can be carried out, considering further context-relevant aspects such as culture or demographic differences [31]. Furthermore, possible dependencies in our taxonomy must not be ignored. Thus, future research should analyze whether certain manifestations of the characteristics often occur together and whether archetypes of behavior can be derived from them.

6. Conclusion

Information security compliance behavior is a growing topic in IS research and practice. It is becoming increasingly important for companies to understand the causes of non-compliance behavior and derive appropriate countermeasures correctly. Based on our identified dimensions and characteristics of our taxonomy, information security researchers can identify different types of ISP non-compliant behavior for their research and analyze specific types of behavior more closely. Information security practitioners can use our taxonomy to better distinguish the different reasons for a security threat and develop measures that effectively address the actual reason and not just non-compliant behavior. Furthermore, the taxonomy provides a holistic overview of the different descriptive elements of types of ISP non-compliance behavior and is a theoretical basis for future research, e.g., by defining archetypes for each dimension of the taxonomy or by considering already applied theories in the different types of behavior. Future studies can consider our results for a more specific analysis of the individual elements of describing the different types of behavior.

7. References

[1] W.A. Cram, J. D'Arcy, and J.G. Proudfoot, “Seeing the Forest and the Trees: A Meta-Analysis of the Antecedents to Information Security Policy Compliance”, MIS Quarterly 43(2), 2019, pp. 525-554.

[2] S. Hina, and P.D.D. Dominic, “Information security policies’ compliance: a perspective for higher education institutions”, Journal of Computer Information Systems 60(3), 2020, pp. 201-211.

[3] R. Willison, P.B. Lowry, and R. Paternoster, “A Tale of Two Deterrents: Considering the Role of Absolute and Restrictive Deterrence to Inspire New Directions in Behavioral and Organizational Security Research”, Journal of the Association for Information Systems 19(12), 2018, pp. 1187-1216.

[4] K. Padayachee, “Taxonomy of compliant information security behavior”, Computers & Security 31(5), 2012, pp. 673-680.

[5] B. Bulgurcu, H. Cavusoglu, and I. Benbasat, “Information security policy compliance: an empirical study of rationality-based beliefs and information security awareness”, MIS Quarterly 34(3), 2010, pp. 523-548.

[6] G.D. Moody, M. Siponen, and S. Pahnila, “Toward a Unified Model of Information Security Policy Compliance”, MIS Quarterly 42(1), 2018, pp. 285-311.

[7] T.B. Lembcke, K. Masuch, S. Trang, S. Hengstler, P. Plics, M. Pamuk, “Fostering Information Security Compliance: Comparing the Predictive Power of Social Learning Theory and Deterrence Theory”, Proceedings of Americas Conference on Information Systems (AMCIS), 2019, Mexico.

[8] S. Trang, B. Brendel, “A Meta-Analysis of Deterrence Theory in Information Security Policy Compliance Research”, Information Systems Frontiers 21(6), 2019, pp. 1265-1284.

[9] S. Aurigemma, and T. Mattson, “Generally Speaking, Context Matters: Making the Case for a Change from Universal to Particular ISP Research”, Journal of the Association for Information Systems 20(12), 2019, pp. 1700-1742.

[10] A. Farooq, S.R.U. Kakakhel, S. Virtanen, and J. Isoaho, “A taxonomy of perceived information security and privacy threats among IT security students”, in 10th International Conference for Internet Technology and Secured Transactions (ICITST), 2015, pp. 280-286.

[11] R.C. Nickerson, U. Varshney, and J. Muntermann, “A method for taxonomy development and its application in information systems”, European Journal of Information Systems 22(3), 2013, pp. 336-359.

[12] S. Gregor, “The Nature of Theory in Information Systems”, MIS Quarterly 30(3), 2006, p. 611.

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

[14] P. Mayring, Qualitative Inhaltsanalyse: Grundlagen und Techniken, 2010, s.l.: Beltz Verlagsgruppe.

[15] A. Hovav, and J. D’Arcy, “Applying an extended model of deterrence across cultures: An investigation of information systems misuse in the U.S. and South Korea”, Information & Management 49(2), 2012, pp. 99-110.

[16] J. Shropshire, M. Warkentin, and S. Sharma, “Personality, attitudes, and intentions: Predicting initial adoption of information security behavior”, Computers & Security (49), 2015, pp. 177-191.

[17] P. Menard, J.B. Gregory, and R.E. Crossler, "User motivations in protecting information security: Protection motivation theory versus self-determination theory", Journal of Management Information Systems 34(4), 2017, pp. 1203-1230.

[18] S. Das, L. Dabbish, and J. Hong, "A typology of perceived triggers for end-user security and privacy behaviors", Fifteenth Symposium on Usable Privacy and Security, 2019, pp. 1-11.

[19] Z. Ahmad, M. Norhashim, O.T. Song, and L.T. Hui, “A typology of employees' information security behaviour”, in 4th International Conference on Information and Communication Technology (ICoICT), 2016, pp. 1-4.

[20] K.H. Guo, Y. Yuan, N.P. Archer, and C.E. Connelly, “Understanding Nonmalicious Security Violations in the Workplace: A Composite Behavior Model”, Journal of Management Information Systems 28(2), 2012, pp. 203-236.

[21] A. Vance, M.T. Siponen, and D.W. Straub, “Effects of sanctions, moral beliefs, and neutralization on information security policy violations across cultures”, Information & Management 57(4), 2020, p. 103212.

[22] R.L. Glass, and I. Vessey, “Contemporary application-domain taxonomies”, IEEE Software 12(4), 1995, pp. 63-76.

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

[24] J. Webster, and R.T. Watson, “Analyzing the Past to Prepare for the Future: Writing a Literature Review”, MIS Quarterly 26(2), 2002, pp. 13-23.

[25] R.C. Nickerson, J. Muntermann, and U. Varshney, “Taxonomy Development in Information Systems: A Literature Survey and Problem Statement”, in AMCIS proceedings, 2010, pp. 125-132.

[26] V. Broughton, “The need for a faceted classification as the basis of all methods of information retrieval”, Aslib Proceedings 58(1), 2006, pp. 49-72.

[27] M. Ruzza, B. Tiozzo, C. Mantovani, F. D’Este, and L. Ravarotto, “Designing the information architecture of a complex website: A strategy based on news content and faceted classification”, International Journal of Information Management, 37(3), 2017, pp. 166-176.

[28] R.T. Nakatsu, E.B. Grossman, and C.L Iacovou, “A taxonomy of crowdsourcing based on task complexity”, Journal of Information Science 40(6), 2014 pp. 823-834.

[29] J.F. Sowa, and J.A. Zachman “Extending and formalizing the framework for information systems architecture”, IBM Systems Journal 31(3), 1992 pp. 590-616.

[30] K.L. Thomson, R. von Solms, and L. Louw, “Cultivating an organizational information security culture”, Computer Fraud & Security 2006(10), 2006, pp. 7-11.

[31] R. Willison, M. Warkentin, and A.C. Johnston, “Examining employee computer abuse intentions: insights from justice, deterrence and neutralization perspectives”, Information Systems Journal 28(2), 2018, pp. 266-293.

[32] T. Mashiane, and E. Kritzinger, “Cybersecurity Behaviour: A Conceptual Taxonomy”, in IFIP International Conference on Information Security Theory and Practice, 2019, pp. 147-156.