9-22-2023

THE COLLECTIVE VIOLATION TALK SHOW: HOW DO WORKGROUPS ACCOUNT FOR CYBERDEVIANCE?

Gabriela Labres Mallmann
University of Jyväskylä, gabriela.l.labresmallmann@jyu.fi

Wael Soliman
University of Agder, wael.soliman@uia.no

THE COLLECTIVE VIOLATION TALK SHOW: HOW DO WORKGROUPS ACCOUNT FOR CYBERDEVIANCE?

Research Paper

Mallmann, Gabriela Labres, University of Jyväskylä, Jyväskylä, Finland, gabriela.l.labresmallmann@jyu.fi

Soliman, Wael, University of Agder, Kristiansand, Norway, wael.soliman@uia.no

Abstract

Cyberdeviance within workgroups is one of the most challenging cybersecurity problems facing modern organizations. Cyberdeviance is an intentional form of security policy violation, reflecting the outcome of a justification process deeming the violation acceptable for the violator. The collective nature of cyberdeviance within groups increases the challenge because group context can steer members to act in accordance with the group's decisions, even when it violates organizational directives. Despite these challenges, we know very little about how workgroups justify cyberdeviance. We ask: How do workgroups create and validate accounts for cyberdeviance? Guided by the theoretical lens of accounts and based on insights from five deviant workgroups using unauthorized technologies (aka, shadow IT), our analysis points to three core findings. First, the group context is crucial to understanding the violation framing process. Second, at the discursive level, the groups use a unique set of verbalizations that deem cyberdeviance acceptable within the group. Third, we found that this set of verbalized accounts is instrumental to ensure group cohesion and belongingness. We discuss the theoretical and practical implications of these novel insights.

Keywords: Cyberdeviance; ISP violation; workgroups; accounts; neutralization; rationalization; justification, multilevel.

1 Introduction

Cyberdeviance within workgroups is one of the most challenging cybersecurity problems facing modern organizations for at least three reasons. First, by definition, cyberdeviance is an intentional form of information security policy (ISP) violation (Venkatraman *et al.*, 2018, p. 1065), and as such, it reflects the outcome of a justification process deeming the violation acceptable (at least, from the violator's perspective). Second, the collective nature of cyberdeviance within groups increases the challenge of addressing such behaviors because, at the collective-level, group dynamics can steer the group members to act in accordance with the group's routinized norms, even if this means violating the organizational directives. Third, we focus on nonmalicious cyberdeviance, that is, when the violator intends no harm to the organization (e.g., Guo *et al.*, 2011). This type of deviance has been recognized in the information systems security (ISS) literature as a serious and challenging behavior to address (Guo *et al.*, 2011; Siponen and Vance, 2014) because by denying the harmful intent (i.e., well-intended violation), employees can disguise the potential adverse consequences of the behavior and shape how employees talk about cyberdeviance (Siponen and Vance, 2010).

Research on deviant behavior in ISS has been performed under different terms, such as computer abuse (Straub and Nance, 1990), computer misuse (D'Arcy, Hovav and Galletta, 2009), unethical IT use (Chatterjee, Sarker and Valacich, 2015), and ISP violations (Siponen and Vance, 2010). In general, the IS security literature has investigated why people violate or comply with ISP in an attempt to explain or

predict employees' ISS behavior having as normative standard the corporate ISS policies (e.g., Bulgurcu, Cavusoglu and Benbasat, 2010; Moody, Siponen and Pahnila, 2018; Gwebu, Wang and Hu, 2020). Within this body of knowledge, ways of verbally justifying deviant behavior are regarded as an important element in predicting and explaining employee's noncompliance behavior with ISP (e.g., Bulgurcu et al., 2010; Siponen and Vance, 2010). Neutralization theory (Sykes and Matza, 1957), for instance, has emerged as one of the most popular frameworks to investigate how individuals use specific linguistic tactics (e.g., neutralization techniques) to justify or excuse unethical and/or illegal security violations and how these tactics influence employees' intentions to commit the deviant behavior in the future (e.g., Siponen and Vance, 2010; Khansa *et al.*, 2017; Barlow *et al.*, 2018; Siponen, Puhakainen and Vance, 2020). The prevailing level of analysis in those studies has focused exclusively on the individual; that is, by examining employees' perceptions, motivations, and ISS-related behaviors within organizations. This emphasis leaves underexplored the collective level of analysis (cf. Burton-Jones and Gallivan, 2007), such as how interactions among group members, their interdependence and need for cooperation within a workgroup setting influence groups' justifications for their cyberdeviance.

In contrast to methodological individualism (Sarker and Valacich, 2010), approaching this topic from the collective level provides additional illumination since it recognizes that individuals' actions are mutually influenced by the actions of others within a collective. Social systems are populated by individuals who are influenced by one another and by the surrounding context, and consequently, the possible range of actions for individual behavior is influenced by several situational or contextual elements (Morgeson and Hofmann, 1999). Furthermore, when it comes to accounting (or developing justifications) for deviant behavior, we cannot ignore the interdependency between the individual and the accommodating collective. For instance, the literature on accounting for deviant behavior (Scott and Lyman, 1968) emphasizes the social and interactive nature of the accounting process, suggesting that the creation and validation of accounts depend to a great extent on the social circle in which they are introduced. Despite the wide recognition of the difference between individuals and collectives regarding information processing, decision-making and acting (Searle, 1990; e.g., Jetten and Hornsey, 2014; Mcgloin and Thomas, 2016); we know very little about how workgroups justify and propagate cyberdeviance.

In this study, we explore this challenge by asking the question: How do workgroups create and validate accounts for cyberdeviance? We focus on features of 'talk' to understand how workgroups justify cyberdeviance through the theoretical lens of *accounts* (Scott and Lyman, 1968), where an account is understood as "a linguistic device employed … by a social actor to explain unanticipated behavior or untoward behavior—whether that behavior is his own or that of others, and whether the proximate cause of the statement arises from the actor himself of from someone else" (Scott and Lyman, 1968, p. 46). By adopting the collective level of analysis (cf., Burton-Jones and Gallivan, 2007), we aim to uncover the social and interactive elements of the accounting process within groups. A collective here reflects an interdependent and goal-directed group of individuals, such as a team or department (Morgeson and Hofmann, 1999). To this end, we conducted in depth interviews with members of five deviant workgroups who collectively engaged, in coordinated deviant behaviors, thus, intentionally violating their workplaces' IS security policies (e.g., Burton-Jones and Gallivan, 2007; Schabram, Robinson and Cruz, 2018).

With this in mind, the paper is structured as follows. The next section presents the theoretical lens of accounts, which provides the basis for our analytical framework. Next, we describe the research approach and give an overview of our data collection and analysis methods. We then present the findings on how workgroups account for cyberdeviance. Finally, we conclude by discussing the theoretical and practical implications of our findings, as well as limitations and future research directions.

2 Theoretical Foundation

The theoretical lens of accounts provides the basis for our analytical framework (Sykes and Matza, 1957; Scott and Lyman, 1968). As noted earlier, an account is defined as a linguistic tactic used by a social actor to justify or excuse an unacceptable, unethical, or untoward behavior in general, rending it

acceptable (Scott and Lyman, 1968). The body of literature on accounts points our attention to three core elements which we find relevant to our data analysis and interpretation (See Figure 1): *(a) accounts as verbalizations at the discursive level*; *(b) the accounts' function or purpose at the cognitive level*; and *(c) the account validation process*. We discuss each in turn next.

Accounts as verbalizations at the discursive level. From a discursive lens, accounts reflect talks, arguments, verbalizations, and vocabularies that vindicate the acceptability of the unacceptable (from a given perspective). Due to the crucial role of language in influencing how people think and act, much of the research on deviance explores the language of justification (i.e., focuses on the discursive level of the accounts themselves). One key objective of research at the discursive level is to identify the tactics (i.e., linguistic techniques) that deviant actors (criminals or otherwise) use to justify or excuse their violations. Sykes and Matza's (1957) work on the techniques of neutralization reveals five of the most common excuses and justifications that norm-breakers use to account for their violations. These five accounts are: 'denial of responsibility', 'denial of injury', 'denial of victim', 'condemnation of condemners', and 'appeal to higher loyalties'. In addition to these five classical accounts, subsequent research has further identified various other techniques, including the 'metaphor of the ledger' (Klockars, 1974), the 'defense of necessity' (Minor, 1981), the 'defense of ubiquity' (Cromwell and Thurman, 2003), the 'claim of relative acceptability' (Cromwell and Thurman, 2003), and the 'claim of entitlement' (McGregor, 2008). Due to space limitation, we present a brief overview of the five classical accounts with examples from the IS literature.

First, the denial of responsibility account liberates oneself from any sense control with respect to the situation at hand. A popular argument here is that the crime is "due to forces outside of the individual and beyond his control" (Sykes and Matza, 1957, p. 667) . In the context of violating Internet-use policy, some employees could use this account to argue that using the workplace Internet for personal purposes is excused if one is unsure whether the organization has an Internet-use policy or one does not understand it fully (Cheng *et al.*, 2014). *Second, the denial of injury* account provides an argument that downplays the violation's impact on the victim, stating, for example, that the act "does not really cause any great harm" (Sykes and Matza, 1957, p. 668). In the context of violating Internet-use policy, some employees could use this account to argue that using the access provided by the organization for non-work-related purposes is justified if no harm is done to the company (Khansa *et al.*, 2017).

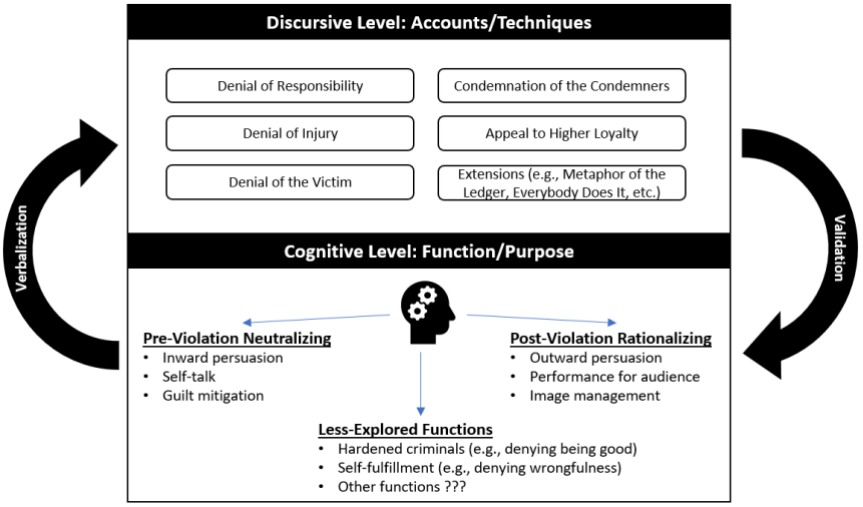

Figure 1. Accounts at the discursive level and their functions at the cognitive

Third, the denial of the victim account turns the victim into a wrongdoer and the offender into a rightful avenger. A wrongdoer could argue, for example, that the victim deserved what happened and "had it coming" (Sykes and Matza, 1957, p. 669). In the context of violating Internet-use policy, some employees could use this account to argue that using the Internet access provided by the organization for non-work-related purposes is justified when the manager is biased and does not treat the workers well (Cheng *et al.*, 2014). *Fourth, the condemnation of the condemners* account shifts the attention from the wrongdoer's own motives to those who disapprove, arguing, for example, that the police are

"corrupt, stupid, and brutal" (Sykes and Matza, 1957, p. 668). In the context of software piracy, this account could be used to argue that breaking software copyright agreements is justified when they are too restrictive (Siponen, Vance and Willison, 2012). *Fifth, the appeal to higher loyalties* account places the actor in a dilemmatic position between two forces, between the demands of a larger social group (e.g., society) and of a smaller social group to which he or she belongs (e.g., family and friends), thereby arguing that "I didn't do it for myself" (Sykes and Matza, 1957, p. 669). In the context of software piracy, this account could be used to argue that making unauthorized copies of software is justified if done, for instance, to assist a friend who does not have the means to purchase the software (Siponen, Vance and Willison, 2012).

Accounts' functions at the cognitive level. Whereas the discursive level is concerned with identifying and scrutinizing the use of language in the accounts themselves (Benson, 1985); the cognitive level shifts our attention to the importance of the underlying cognitive and motivational processes that invoke these accounts. In other words, what purpose do accounts serve in the norm-breaker's mind? Much of the research in this area delves into the motivational aspects of offenders when using accounts, and the main objective is to understand the role that accounts play in relation to norm violation. One central question often guides research at this level is: Does a norm breaker consider the account(s) as a form of pre-violation "self-talk" (Topalli, 2005); or as a form of post-violation "impression management" (van Dijk, 1992)? Whereas in pre-violation, the accounts' main function is to counteract or neutralize the self-regulative process of guilt or shame; the importance of post-violation accounting stems from their ability to "exaggerate actions they [deviants] believe others will view favorably …, while also concealing or minimizing socially undesirable actions or attitudes that may be detrimental to their identities or interactions" (Bryant *et al.*, 2018, p. 3).

Hence, a distinction is often made between two underlying cognitive processes: *pre-violation neutralizing* (Sykes and Matza, 1957), and *post-violation rationalizing* (Minor, 1981) . On the one hand, a norm-breaker may invoke a neutralizing account (say, denial of injury) prior to violation in order to "relieve themselves of the duty to behave according to the norms" (Benson, 1985, p. 587). Alternatively, a norm-breaker may utilize the same (or different) account to rationalize the violation after it has taken place in order to protect their social image (i.e., to save one's face, Scott and Lyman, 1968). This in effect means that the same account (at a discursive level) may be considered a pre-crime neutralization or post-crime rationalization (at a cognitive level) depending on what purpose this account serves in the norm-breaker's mind (Minor, 1981; Benson, 1985; Agnew, 1994). These two functions (neutralizing and rationalizing) are not the only ones. In fact, scholars acknowledge there are other less explored functions that warrant further investigation. For instance, (Topalli, 2005) found that hardcore criminals used various accounts – such as, denial of victim or denial of injury – for a unique and unconventional purpose. Neither to neutralize guilt from violating societal norms, nor to maintain the social image of a good citizen; but rather these accounts were used to project and maintain the image of being bad. To these hardcore criminals, the accounts were instrumental to assert their allegiance to the street code (Topalli, 2005). In a yet less-explored accounting function, Scott and Lyman (1968) point to norm-breakers who genuinely believe there is nothing unethical or wrong in their violations. For those norm-breakers, accounting served a *'self-fulfilling'* function, reflecting a desire to "enlighten what they [norm-breakers] considered to be unenlightened establishment" (Scott and Lyman, 1968, p. 52).

The account validation process. The third element we wish to highlight from the accounts lens is the role of validation in the accounting process. Accounts are not universal justifications independent of time and place; rather, they are based on a common background. That is, they are highly contextual and carefully curated arguments, and the extent to which they are honored (i.e., accepted) or not honored (i.e., rejected) depends on the violator's ability to convince the intended audience of the justness of the violation against the dominating norm or rule. Because of this, Scott and Lyman (1968) argued that a key "variable governing the honoring of an account is the character of the social circle in which it is introduced … [and that the] vocabularies of accounts are likely to be *routinized within cultures, subcultures, and groups*, and some are likely to be exclusive to the circle in which they are employed" (pp. 52-53, *emphasis added*). This, in effect, emphasizes the social and interactive nature of accounting, and that account-validation is a crucial component of the social learning process via which members of

a given 'social circle' develop an understanding of the effectiveness of different accounts in excusing or justifying deviance. For instance, members of a social system (e.g., a culture, a subculture, a group, etc.) need to learn the regulative framework of that system, which among several things, provides fundamental knowledge about (a) norms and rules that are non-negotiable, and therefore, no amount of accounting will justify violating them (within that social system); and (b) norms and rules that are negotiable coupled with the accounts that are known to justify breaking these norms and rules (within that social system). From a theoretical standpoint, these *'validated accounts'* are extremely important in preserving the cohesion of the social system. In fact, to Scott and Lyman (1968), it is this feature of 'talk' (i.e., the honoring of accounts) that makes the formation of society possible. That is, honored accounts are foundational to social systems due to "its ability to shore up the timbers of fractured sociation, its ability to throw bridges between the promised and the performed, its ability to repair the broken and restore the estranged" (p. 46).

3 Research approach

To better understand how cyberdeviance accounting occurs at the collective level, we conducted a narrative-based qualitative study. Narrative interviews have been recognized in both management and IS as a valuable source of insight into behavior and social elements in real-life contexts (e.g., Myers, 1997; Pentland, 1999). The unit of analysis in our work is the workgroup (known as *'speech community'* in the accounts literature). To Scott and Lyman (1968), the speech community is a unit of analysis "composed of human aggregates in frequent and regular interaction" (p. 61). More importantly, these speech communities "define for their members the appropriate lingual forms to be used amongst themselves … [and as a result,] the types of accounts appropriate to each speech community differ in form and in content" (pp. 61-62). With this mind, we use multilevel research guidelines to collect and analyze the data (Morgeson and Hofmann, 1999; Klein and Kozlowski, 2000; Burton-Jones and Gallivan, 2007). By multilevel analysis, we mean more than one level of conceptualization and analysis, such as, the role of individuals within a collective. In-depth interviews were conducted with 21 participants from five workgroups working in 4 different organizations located in southern Brazil.

We characterize the workgroups in our study as *deviant* because, at a collective level, each workgroup has its members engaged, in a coordinated manner, in the same cyberdeviance (Burton-Jones and Gallivan, 2007; Schabram, Robinson and Cruz, 2018). Table 1 presents a description of the five workgroups (G), the number of participants in each group, their organizational roles, as well as examples of cyberdeviance they were involved in collectively. The main instance of cyberdeviance in this study is the use of unauthorized technology to perform work tasks (Venkatraman *et al.*, 2018), also known as shadow IT (e.g., Silic, Barlow and Back, 2017), which is increasingly becoming a root-cause of many successful cyberattacks (Walters, 2022). By unauthorized we mean the deliberative use of information technology not officially sanctioned by the organization.

The interviewing process was guided by Myers and Newman's (2007) guidelines for qualitative interview in IS research. An interview protocol was developed and the interview questions were structured from general to specific (Myers and Newman, 2007). The interviewees were asked to provide a narrative as detailed as possible of the inception and spread of cyberdeviance within the workgroup, which was complemented with follow-up questions to capture specific details. Each interview lasted 1 hour on average, using video camera when the respondent agreed.

Considering our explicit interest in the collective level, we focus on the role of individuals in terms of the wider collective; that is, the individual as an informant of *collective* dynamics (Morgeson and Hofmann, 1999). Instead of isolated individuals, participants are treated as members of a group bounded by a context, as common in multilevel studies (e.g., Lapointe and Rivard, 2005). To this end, the interview questions focused on collective-level issues, such as, how did the use of unauthorized IT spread across the group's members? How are the relationships among the group members? And how do these relationships influence cyberdeviance at work? For instance, do they feel more influence from the group or from the organizational information security policy? Thus, multilevel guidelines were adopted to avoid methodological individualism by accounting for interrelationships among individuals, as well

as intra-group agreement (Klein and Kozlowski, 2000; Sarker and Valacich, 2010). The interviewees (as well as their organizations) were assured confidentiality and anonymity (Myers and Newman, 2007). To this end, all interviews were transcribed verbatim and were carefully anonymized. Data collection ended when we reached a sufficient level of saturation, that is, when no significant new information or insights emerged from the final interviews (Baker and Edwards, 2017).

G	Respondents	Group Cyberdeviance
G1	R1-R5G1 (5 employees) R6-R7G1 (2 superiors)	The sales department (SD) of a publishing group uses an unapproved CRM tool since 2014. The implementation has been done without consultation and support from the IT department.
G2	R1-R6G2 (6 employees)	Although the organization provides Skype for Business, a business unit for content creation in the same publishing group uses an unapproved instant messaging tool to collaborate at work for 5 years up to now.
G3	R1-R3G3 (3 employees)	An audit team of a multinational professional services firm uses several unapproved productivity tools (e.g., PDF Editing Software) to handle client documents to audit, which contain confidential information (e.g., financial data). To meet their own work demands, the employees search online for helpful tools and share them via USB flash drive among team members.
G4	R1-R2G1 (2 employees)	A team of communication and brand in the Public Relations (PR) department of a large communication group uses unapproved cloud services such as Dropbox and Google Drive to share content with internal colleagues in the PR department and external partners from advertisement agencies.
G5	R1G5 (superior) R2G5 (employee)	A team of store profitability in the operations and sales department of a large retail firm uses a variety of unapproved cloud services to communicate and share information with salespeople and regional managers located in the stores owned by the organization.

Table 1. Overview of the workgroups and their collective cyberdeviance

While our work is informed by the theoretical lens of accounting, the data analysis was mostly inductive. Considering our research question on how workgroups account for cyberdeviance, we followed a data-driven approach looking for how groups articulate cyberdeviance focusing on group dynamics, such as shared meanings, interdependency, interactions, and group context (Morgeson and Hofmann, 1999; Burton-Jones and Gallivan, 2007). Multilevel research posits that higher-level phenomena (e.g., collective) emerge from lower-level components (e.g., individuals, Morgeson and Hofmann, 1999). Therefore, individual-level data are critical for analyses of the collective, which require the demonstration of within-group consensus or consistency (Klein and Kozlowski, 2000). Accordingly, the data gathered from individual members of groups were aggregated to the collective level of analysis by focusing on within-group agreement to uncover shared team properties (Klein and Kozlowski, 2000), as suggested by multilevel guidelines (Burton-Jones and Gallivan, 2007). We used coding strategy (Myers, 1997; Pentland, 1999) following the guidelines of Strauss and Corbin (1990) because it offers a series of systematic and structured steps. The software Atlas for qualitative data analysis was used to support the coding process.

On the nature and role of theory in our study, the theory of accounts was used as a theoretical scaffolding to unfold our results (Sarker *et al.*, 2018). Therefore, we were inspired by the discursive and cognitive levels, as well as the importance of a common background, proposed by the theory to understand how groups create and validate accounts. We also compare our findings with existing literature related to accounts (e.g., neutralization techniques) to capture how group accounts may differ from individual-level ones.

4 Findings

The current section presents our findings, which are divided into three subsections following our analytic framework: 1) *contextual elements* that constitute the common background for groups' account

verbalization and validation, 2) *accounts* at the group discursive level, and 3) *accounts' function* at the cognitive level. Figure 2 depicts the general framework of our results on how workgroups create and validate cyberdeviance accounts in the workplace. The external layer shows the contextual elements that constitutes the common background for group members. The common background is behind the creation and validation of group accounts because it ensures that all members have a shared understanding regarding the cyberdeviance. Recognizing the contextual elements is essential because without context, accounts are rendered meaningless and their function useless (Scott and Lyman, 1968). The middle layer represents the group discursive level and reflects accounts that are created and validated by the group members. The most inner layer represents the cognitive level that emerges within the workgroup due to the common background and validated accounts. The two-directional arrows highlight that all the layers influence and reinforce each other during the creating and validation of group accounts. Next, we elaborate our findings.

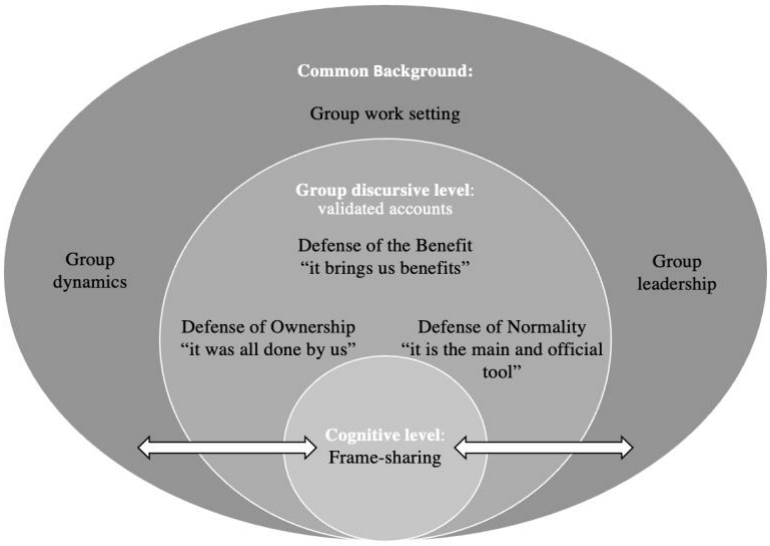

Figure 2. Framework on Group Accounts

4.1 Common background: contextual elements

The verbalization and validation of group accounts rely on elements or factors related to the workgroup context which constitute the common background shared by the members. Three contextual elements emerged as exceptionally salient from our analysis: (a) group work setting, (b) group dynamics, and (c) group leadership.

Group work setting. The first common background element reflects the group's shared experience related to execution of work, such as group tasks, technology, and processes. The group members tend to have common needs due to the interdependence of tasks, as well as common goals (e.g., productivity) that should be met by the group as a team or department. "One impacts the work of the other", says R1G1. For this reason, collaboration among members is valued by the group. For example, "when I need something, I … talk to some workmate, who maybe already had a similar situation" (R2G5). Their focus on exchanging and helping each other is driven by the achievement of performance to ensure the execution of tasks and the accomplishment of group goals. The interviews clearly demonstrate that the workgroups tend to have high task-interdependence, which demand coordination in terms of technology and processes to execute work. One interviewee sums it up eloquently:

> "I think the main factor is the time we have to perform the tasks. Sometimes we have really short deadlines, there is something to deliver, a goal to be achieved, so we seek the fastest and most agile way to do things … The great variable is this, performance. Although there are risks (referring to cyberdeviance), there is no doubt." (R1G5)

Group dynamics. The second common background element is the group's social environment and its importance stems from the realization that the group members constantly influence each other through formal and informal, as well as physical and virtual communication. Most of the problem-solving and work-related decisions rely on communication among members, mainly due to the common background of needs and goals discussed before. For instance, R1G3 notes that "once someone discovered that a tool is good, then when one needs, this person shared the tool via USB drive saying 'ah, I found a tool that can help you, you can download it too'. Because it is something (cyberdeviance) so common to everybody, it is easy to spread." Such perception that "everybody" in the group is engaged in cyberdeviance adds pressure on individuals to comply with the group's decisions. R6G2 further explains:

> "[T]here is a group influence (to use the unauthorized IT), it is like everybody uses it, you also need to. If you are not there, you do not know what is going on, not only related to the business but also social activities, like lunchtime ... Then, when you say it, you are forcing someone to (to use the unauthorized IT) to fit in the group." (R6G2)

Therefore, there is a pressure to adapt to group decisions to avoid negative reactions from the members and ensure social acceptance to maintain an amicable atmosphere, mainly because they consider their relationship as a form of camaraderie (not merely workplace colleagues). For instance, R2G3 reveals that "[t]here is friendship too. Most of us are also friends. Everybody is quite young. Including the senior. Sometimes we worked 60 hours per week, so we have to get along."

Group leadership. The third salient element is the group's leadership, and it represents the role of higher positions within the group (e.g., supervisors, managers, etc.). Leaders' role within the group is described as "the bigger force" (R1WG1) because they have double source of power, that is, leaders have formal power because of the organizational higher hierarchical position they possess, as well as informal power for being considered part of the group. This way, leaders play an intermediary role between the group and the organization, and can influence (and even mandate) decisions on group members. R5G1 notes that "[f]rom the group perspective, it (the unauthorized IT) is mandatory, totally!... mainly from the managers that use it to control performance. It is not about wanting or not; you have to use it". When the group superior endorsed somehow the deviant behavior, it can mislead or hide the deviant characteristics of the act. "For us, it was like a formal authorization. Although it was not formally authorized by the IT department, it comes from people that already have more responsibility (power) in the company hierarchy than us. It was like permission from a boss", explains R1G3. It is important to notice that the workgroup's leaders are not the ones responsible for developing and enforcing ISP, which is done by security teams. Thus, group leaders are also deviating from the official ISP by not discouraging (or even encouraging) cyberdeviance within the group. Also, we noticed that leaders on higher positions outside the group do not exert the same strong influence as the local leaders do because the latter are closer to the group members' daily work life, being responsible for their work and performance within the group.

In sum, the group context, reflected by these three main elements, serves as a common background for members verbalization and validation. For this reason, the common background drives the development of group accounts at the discursive level and, ultimately, at the cognitive level, as we explain below.

4.2 Group discursive level: validated accounts

Rooted in the common background presented above, the groups create accounts at the discursive level. That is, how the workgroup members talk about and present arguments (i.e., accounts) to justify cyberdeviance. These accounts are created and validated by workgroup members because they can easily make sense of each other's arguments once they share a common background. We identified three main group-level accounts, which we call (a) defense of ownership, (b) defense of the benefit, and (c) defense of normality. While these accounts bear some resemblance to the popular neutralization techniques at the individual level (Sykes and Matza, 1968; Siponen and Vance, 2010), the group-level accounts we discuss here are significantly different as we elaborate next.

Defense of ownership. The first group-level account represents the argument of cyberdeviance perceived as a group initiative, reflecting the argument that "[i]t is not an official tool. It was an initiative from our department" (R4G1), and that "[e]verybody were aware it was not a technology implemented by the IT department (R3G1)." The members talk about cyberdeviance as their initiative, which was created based on the groupwork needs and through their efforts. "We, as a department, saw the necessity of having an official tool", says R5G1, showing the perception of a lack of organizational solutions. "Since 2013, we created an account on (the unauthorized IT) way before the company had a formal process to use cloud services" (R3G4). Consequently, they act autonomously, mainly if the technical barriers are low, for instance, "if the tool is online (cloud service), so it does not impact the IT department… then we do everything by ourselves", explains R7G1. The group cyberdeviance is quickly shared among them, considering the common needs and goals of the group and the motivation to collaborate and help each other (group context and group dynamics). For example, "in our unit, yes, we search for technologies and share the findings with the colleagues", explains R2G4.

In a stark contrast with the typical excuse of denying responsibility (Sykes and Matza, 1957; Scott and Lyman, 1968; Siponen and Vance, 2010), our study participants consider the group cyberdeviance their responsibility, developing a sense of ownership towards it. For instance, "it was totally done by the department here" (R3G1), and "it was all our responsibility, we went after everything", says R1G2. Therefore, "it is a tool from our department that we have total control over it, we do not need to involve outsiders", complements R5G1.

Defense of the benefit. The second group-level account describes members' argumentation that cyberdeviance is beneficial to task execution. "The (unauthorized IT tool) has the goal of supporting us, our work, [and] do what we need.", reports R4G1. "It helped us a lot to perform the work … the company did not have an official tool for that", says R1G3. These excepts reveal that the group members compare the sanctioned organizational IT with the one of their choice and how the latter has become the *de facto* tool within the group. "Honestly, (the official organizational IT tool) misses some features we need. Many don't use (the official organizational IT tool), but all use (the unauthorized IT tool). Then, it facilitates the communication of having a common way" (R6G2).

The narratives also show how the accounts interrelate and complement each other. For example, "it (the unauthorized IT tool) was our initiative and it evolved very fast in the department. It came only to help us, we get benefits from it, so there was any bad perspective in relation to it" (R7G1). Thereby, the "our initiative" account is complemented by "we get benefits" because one reinforces the other, aiding in validating the accounts to the group members because, ultimately, their initiative brings positive outcomes to the group. For this reason, they also have no "bad perspective" of engaging in cyberdeviance, that is, no negative feelings (such as guilt or shame) are reported by the interviewees for violating the ISP. We will further explore this important finding in Section 4.3 (i.e., the accounting function at the cognitive level).

Defense of normality. The third group-level account describes how workgroups (re)frame the cyberdeviance as a group normal practice. "Nowadays the tool is more formalized, but still, it is completely managed by us… we can say there is a process of normalizing the tool" (R1G1). This narrative refers to a process of formalization for the unauthorized tool from the workgroup point of view, which is first introduced as a group initiative and then, disseminated among the group members based on the benefits. One interviewee explains:

> "The more people see the (cyberdeviance) is being useful to them to perform their daily tasks, the more they will engage. This is the key. We seek to engage people on tool usage, showing them how it is useful." (R6G1)

As a result, cyberdeviance is (re)framed within the workgroup based on the argument that "it is so normal, it is already settled in our process, in our routine", says R2G4. Consequently, cyberdeviance turns into the official and normal practice within the group. "It is not about wanting or not, you will use it. In this sense, to the group, it is very mandatory because it is the main and official tool" (R5G1), while it remains as cyberdeviance for the organization that, oftentimes, is unaware of the practice (e.g., G3 and G4).

It is important to highlight that those accounts are validated by the group members and are validated within the group due to their common background (group work setting, group dynamics, and leadership) as discussed earlier. Because of the common background, the verbalized group accounts can be understood by all the members and reproduced among them, leading to their validation. Accounting for cyberdeviance might vary according to the group of reference, thus many not be valid to outsiders who do not share the same background. For instance, it is not valid from the organizational perspective because the cyberdeviance still violates the ISP and represents a risk to information security, even when seen as normal by the workgroup members.

4.3 Group cognitive level: Beyond neutralizing and rationalizing

At the cognitive level, our empirical data point to the emergence of a yet unrecognized accounting function, which we call "frame-sharing". As noted earlier, the two most recognized accounting functions in the literature are *pre-deviance neutralizing* and *post-deviance rationalizing*, reflecting the two functions of guilt-avoidance and self-image-preservation respectively (Sykes and Matza, 1957; Scott and Lyman, 1968; Minor, 1981; Maruna and Copes, 2005). Careful analysis suggests that the accounts identified in our study (i.e., ownership, benefit, normality) have different functions/purposes that go beyond neutralizing and rationalizing cyberdeviance for the group members. In the following section, we elaborate how frame-sharing differs from the traditional functions of neutralizing and rationalizing and explain what novel function frame-sharing serves in the accounting process.

First, our analysis reveals that the group members did not experience the negative emotions of shame or guilt before engaging in the deviance, as is typically the case in pre-violation neutralizing (Sykes and Matza, 1957). For instance, when the interviewees were asked about the possibility of negative feelings, they replied: "no, I do not think so (referring to negative feelings). I think nobody feels this way. I have never felt bad for using it" (R4G2) … "because we did not see ourselves as doing anything wrong. It was necessary to perform our work" (R1G3). Interviewee R2G3 sums it up: "because of this [group] context, it never felt wrong or not permitted" (R2G3).

Second, our analysis also reveals that self-image preservation, as is typical of post-violation rationalizing (Minor, 1981), was unnecessary either among the studied groups. The majority of the respondents have reported never reflecting or considering negative repercussions of engaging in cyberdeviance, such as formal sanctions, risks, or negative outcomes in general. One interviewee notes: "No. I have never thought about it. Maybe because we did not see any risk of doing this (using an unauthorized IT tool), although we download the apps from another place [the Internet] without knowing the risks. But we did not feel this fear of being penalized." (R3G3).

By contrast, with frame-sharing (Orlikowski and Gash, 1994), individuals communicate taken-for-granted assumptions among the group, and these assumption (e.g., mental models) are responsible for making sense of (and giving sense to) lived experiences among a collective. As Orlikowski and Gash (1994) explain, "individuals can be said to share a frame if some core cognitive elements (assumptions, knowledge, and expectations) are similar" (p. 177). Our findings suggest that in the studied groups, the ultimate function of frame-sharing is to demonstrate group cohesion and ensure belongingness, which we discuss next.

Demonstrating group cohesion. In terms of group cohesion, one of the main findings, aside from the absence of notions of guilt-neutralizing and/or image-preserving, is the near-unanimous and unquestionable agreement in the studied groups that the cyberdeviance is described as: *"this is how it is done here!"* From the group's viewpoint, cyberdeviance is the *de facto* practice, which, to them, is well-justified since (a) it is a group initiative (defense of ownership), (b) it brings positive work outcomes (defense of benefits), and (c) it is normalized within the group (defense of normality). Therefore, cyberdeviance at that stage can be seen as part of the group's socially constructed reality and they account for it on that basis; a matter of *"stating the obvious"*. Interviewee R2G4 explains: "It (the unauthorized IT tool) was already rooted in our day-to-day work life, and we did not think if it was risky or not." The data also reveals that the group members seem confident in the way they conceive cyberdeviance, which reinforces the view that no negative feeling or connotation is related to the deviant

act. We further note that the group members need not defend their image in relation to others once they all share the perspective that they are not doing anything wrong. Thus, from the group's framing, cyberdeviance is permitted since it aims at maintaining things as they think is better for the group, for their work, and for the amicable atmosphere they value.

Ensuring belongingness to the group. When engaging in cyberdeviance within the group context, members are conforming to group decisions, which confer their acceptability and validation of their image by other members. "It was shared with every professional there, then it looks normal and part of the routine. So, we felt supported by them (group)", reports R3G3. Therefore, "it was not like 'let's study the IT rules', no! it was 'do what everybody does'", sums up R2G3. Another indication of that is the informal punishment from the members to those who might resist or refuse to engage in cyberdeviance. R7G1 eloquently describes in this analogy: "the uniform is red, and you come wearing blue? The person will receive feedback [i.e., retaliation] ... I think the group would not even see this person [i.e., ignore or ostracize them]." Therefore, one has no need to manage social image of following group conventions because it guarantees social rewards, such as positive image and acceptability.

5 Discussion

Guided by the theoretical lens of accounts and based on insights from five deviant workgroups, we investigated how workgroups create and validate accounts for cyberdeviance. Our analysis point to three core findings. First, the group context is crucial to understanding the violation framing process. Second, at the discursive level, the groups use a unique set of verbalizations that deem cyberdeviance acceptable within the group. Third, we found that this set of verbalized accounts are instrumental to ensuring group cohesion and belongingness. In this section, we discuss the theoretical and practical implications of these novel insights, as well as limitations and future research directions.

5.1 Theoretical implications

Introducing collective level explanation. Most behavioral ISS research to date adopt methodological individualist assumptions (e.g., Bulgurcu et al., 2010; Siponen and Vance, 2010), which potentially overlook elements that emerge from the collective (e.g., interrelations among members and group context) and influence employees' ISS behaviors at work (see also, Sarker and Valacich, 2010). In contrast, our work highlights the importance of looking at how security violations are accounted for at the collective level which differ significantly from the violation-justification process at the individual level. The main difference is that at the collective level, accounts are developed based on common background and are validated by members within a social group (i.e., the 'speech community', Scott and Lyman, 1968), which, ultimately, turns into a socially constructed reality for the group. For this reason, an individual may have a different governing system when acting alone compared to when acting as a member of a speech community (such as a workgroup). At the collective level, the individual member is part of a functional group, where they interact on a daily basis, share interdependent tasks and goals, and act in coordination with other members to achieve them. This group setting is above the individual because it constitutes a set of elements created and enforced over time by the group members. Therefore, being part of a collective, individuals tend to follow group conventions that may prevail over individual aspirations. Our study brings contributions to the literature on ISP violations at the collective level by showing how the workgroup context influences the discursive and cognitive level of accounting for cyberdeviance.

Proposing a novel accounting function. Our findings point to a novel accounting function beyond guilt-neutralizing (Siponen and Vance, 2010; Barlow *et al.*, 2018) and image-management-rationalizing (Benson, 1985; van Dijk, 1992). Our findings suggest that the newly identified accounts (namely, *defense of ownership, defense of the benefit, and defense of normality*) are instrumental to ensure group cohesion and belongingness. At the cognitive level, these verbalizations act as a shared framing by the group members, and, as such, these accounts are not meant to cater for the conventional purposes of guilt avoidance or image management. Our study reveals that not all cyberdeviance accounts given by employees are intended to neutralize guilt (or save image, for that matter). Since we acknowledge that

the same account may be used for different purposes, there are some key pointers that differentiate the account's function in our case. First, the workgroup members do not report any kind of negative feeling, such as shame or guilt, before engaging in the deviance, which is the key defining characteristic for pre-violation neutralizing (Sykes and Matza, 1957). In fact, without feelings of guilt or shame, there is nothing to neutralize (Cromwell and Thurman, 2003). Second, there is no need for managing social image after engaging in cyberdeviance, as is the case of post-violation rationalizing (Minor, 1981) because, within the group context, the management of one's social image is done by following group decisions which guarantees social rewards, such as acceptance and positive image (Jetten and Hornsey, 2014; Mcgloin and Thomas, 2016). In contrast, accounting in the form of frame-sharing resonates with the essence of what Scott and Lyman (1968) recognized as "self-fulfillment" (p. 52). As noted earlier, a key defining feature of this accounting function is it reflects a genuine belief in the correctness of the behavior (i.e., there is nothing unethical or wrong about it). Often times, those who utilize this accounting format consider themselves as pioneers (e.g., ahead of the normative curve) whose norm-breaking behavior will eventually become the new norm. In Scott and Lyman's (1968) words, these norm-breakers have a desire to "enlighten what they considered to be unenlightened establishment" (Scott and Lyman, 1968, p. 52). In organizational context, it is plausible to argue that workgroups who use accounts rooted in the frame-sharing function believe that, over time, their cyberdeviance (e.g., using Dropbox) will eventually be accepted by the prohibiting authority (e.g., the IS security team) to become the new norm.

Underscoring the role of common background in the account validation process. In the original formulation of the accounting lens, Scott and Lyman (1968) emphasized the criticality of the accounts' validation process and hinted to the importance of understanding the "background expectations" (p. 61) within a speech community which is ultimately responsible for deeming an accounts honored/accepted in the face of violation. Our study shows that members of the workgroup share preferences and opinions, as well as develop their own within-group rules that are created and reinforced by the group members. This is possible because they share a common background for being part of the same group, which allows them to have a similar understanding in relation to group matters. Therefore, within the group context, accounts are verbalized and validated by its members. This finding brings important insights to understand the accounting process by workgroups and some of its consequences for cyberdeviance. First, the consideration of validated accounts is important because they are harder to challenge and change due to the social support members provide to each other. Second, we provide an explanation for how the accounts get routinized in a workgroup by uncovering contextual elements of workgroups that are the basis for the verbalization and validation of accounts. Third, validated accounts can, over time, serve as a foundation for establishing new rules. This is important for addressing ISP violations because existing validated accounts that disguise cyberdeviance as a normal group practice can serve as support for further cyberdeviance within the group, continuing the cycle of verbalization and validation based on the group's common background.

5.2 Practical implications

Our study also brings important implications to practice, most notably, by showing that different accounts and functions might indicate different problem formulations, as well as different remedies and solutions for cyberdeviance within groups. Based on our findings, we highlight three suggestions for ISS managers when coping with cyberdeviance among workgroups. First, our study shows how the collective can influence individual behavior in verbalizing cyberdeviance. Therefore, measures to ensure ISS in the workplace should be designed to target the group as a whole, not only individual-level measures. For example, training to increase awareness on ISP where employees will be evaluated together in their teams or departments. The main idea is to propagate recommended behaviors to keep ISS, which can be targeted as a task to the whole workgroup, not to an individual employee only.

Second, the workgroup context offers important guidelines for developing initiatives to address cyberdeviance that is being perpetuated based on a validated account. The process of verbalizing and validating accounts is based on the workgroup context, which has the same importance when the goal

is to challenge an already honored account. For example, group leadership is part of the workgroup context because a group leader influences how members verbalize cyberdeviance. In being a leader and hierarchically superior position within the group, the manager can aid in validating or challenging the existing accounts. Thus, organizations can develop ISS initiatives that involve the group leader, such as leadership training programs that aim to instruct the group leader to better communicate and enforce ISP among group members.

Third, organizations also can benefit from understanding the function of 'accounting'. The function or purpose of group accounts indicates members' shared motivation in perpetuating the accounts. Organizations can use this knowledge as a guide to develop initiatives that aim to challenge the validated accounts for cyberdeviance within the group. Because validated accounts have the social support of members, such initiative might demand some time to be executed and be effective. ISS managers might also face conflicts in trying to challenge accounts that are already routinized by the group. Providing a space for dialogue between ISS teams and group members, taking advantage of the group leaders as a strategic role to mitigate conflicts, is important because the new intended measure (the ones that challenge the account in use) needs to be aligned with the group as a collective for social support.

5.3 Limitations and future research direction

Our work comes with a number of limitations that should be acknowledged. First, the study is geographically limited because the data was collected in Brazil, which may represent a tendency in the findings because of cultural reasons. This limitation calls for further investigations to test our findings in different cultural settings considering that the accounting process may vary based on the group or culture under study. Second, we focused on nonmalicious types of ISP deviance. Thus, researchers should be cautious before applying our conclusions more generally to other instances of ISP violations, which can imply a different set of accounts. Third, we did not consider the impact of group size on the accounting for cyberdeviance in our analysis. We acknowledge that some researchers argue that the number of people engaged in a deviant act can influence one's own deviant behavior (e.g., Mcgloin and Thomas, 2016). Thus, future research may consider how cyberdeviance (and the accounting thereof) are affected when the group is larger or smaller in terms of members.

In terms of future research, our results point out the emergence of a novel account's function at the cognitive level. However, emergence and change within collectives tend to be gradual since it requires coordination among members as the change diffuses across the group (Burton-Jones and Gallivan, 2007). Thus, it would be fruitful for future research to investigate how the accounts emerge over time at the collective level, considering the changes over time that result in the new cognitive function. It is reasonable to argue that group members use the accounts for neutralizing and/or rationalizing purposes at different stages of the normalizing process before reaching the stage of collective (normalized) cyberdeviance. A stage model approach could aid in this regard to uncover the development of accounts within groups, bringing clarity on how they emerge over time at the discursive and cognitive levels.

6 Conclusion

In this article, we sought to understand how workgroups create and validate accounts for cyberdeviance. Considering the scarcity of scholarly efforts addressing this challenge, our objective in this study was to answer the question: How do workgroups create and validate accounts for cyberdeviance? To this end, we focused on cyberdeviance at the collective level of analysis, that is, members of groups collectively engaging in coordinated violation of ISP in the workplace. Thus, workgroups were our unit of analysis. Guided by the theoretical lens of accounts and based on insights from five deviant workgroups, our analysis points to three central findings. First, common background elements are crucial to understanding the violation framing process. These common background elements reflect the group work setting, group dynamics, and group leadership. Second, we find that, at the discursive level, the groups use a unique set of accounts that deem their violations acceptable within the group. In particular, these accounts are defense of ownership, defense of the benefit, and defense of normality. Finally, we find that these salient accounts are instrumental to demonstrating group cohesion within,

and belongingness to, the group, thus pointing to a novel accounting function – beyond neutralizing and rationalizing – hitherto unrecognized. Despite some limitations, we believe our study is an initial step towards understanding the accounting processes within workgroups and increasing clarity on ISP violations by employees at the collective level of analysis.

References

Agnew, R. (1994) 'The Techniques of Neutralization and Violence', *Criminology*, 32(4), pp. 555–580.

Baker, S. and Edwards, R. (2017) 'How many qualitative interviews is enough? Expert voices and early career reflections on sampling and cases in qualitative research', *National Centre for Research Methods Review Paper* [Preprint].

Barlow, J. *et al.* (2018) 'Don't Even Think About It! The Effects of Antineutralization, Informational, and Normative Communication on Information Security Compliance', *Journal of the Association for Information Systems*, 19, pp. 689–715.

Benson, M.L. (1985) 'Denying the Guilty Mind: Accounting for Involvement in a White-Collar Crime*', *Criminology*, 23(4), pp. 583–607.

Bryant, E. *et al.* (2018) 'Techniques of Neutralization and Identity Work Among Accused Genocide Perpetrators', *Social Problems*, 65(4), pp. 584–602.

Bulgurcu, B., Cavusoglu, H. and Benbasat, I. (2010) 'Information Security Policy Compliance: An Empirical Study of Rationality-Based Beliefs and Information Security Awareness', *MIS Quarterly*, 34(3), p. 523.

Burton-Jones, A. and Gallivan, M.J. (2007) 'Toward a Deeper Understanding of System Usage in Organizations: A Multilevel Perspective', *MIS Quarterly*, 31(4), p. 657.

Chatterjee, S., Sarker, S. and Valacich, J.S. (2015) 'The Behavioral Roots of Information Systems Security: Exploring Key Factors Related to Unethical IT Use', *Journal of Management Information Systems*, 31(4), pp. 49–87.

Cheng, L. *et al.* (2014) 'Understanding personal use of the internet at work: An integrated model of neutralization techniques and general deterrence theory', *Computers in Human Behavior*, 38, pp. 220–228.

Cromwell, P. and Thurman, Q. (2003) 'the devil made me do it: use of neutralizations by shoplifters', *Deviant Behavior*, 24(6), pp. 535–550.

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.

van Dijk, T.A. (1992) 'Discourse and the Denial of Racism', *Discourse & Society*, 3(1), pp. 87–118.

Guo, K.H. *et al.* (2011) 'Understanding Nonmalicious Security Violations in the Workplace: A Composite Behavior Model', *Journal of Management Information Systems*, 28(2), pp. 203–236.

Gwebu, K.L., Wang, J. and Hu, M.Y. (2020) 'Information security policy noncompliance: An integrative social influence model', *Information Systems Journal*, 30(2), pp. 220–269.

Jetten, J. and Hornsey, M.J. (2014) 'Deviance and Dissent in Groups', *Annual Review of Psychology*, 65(1), pp. 461–485.

Khansa, L. *et al.* (2017) 'To Cyberloaf or Not to Cyberloaf: The Impact of the Announcement of Formal Organizational Controls', *Journal of Management Information Systems*, 34(1), pp. 141–176.

Klein, K.J. and Kozlowski, S.W.J. (2000) 'From Micro to Meso: Critical Steps in Conceptualizing and Conducting Multilevel Research', *Organizational Research Methods*, 3(3), pp. 211–236.

Klockars, C.B. (1974) *The professional fence | Office of Justice Programs*. New York: Free Press. Available at: https://www.ojp.gov/ncjrs/virtual-library/abstracts/professional-fence (Accessed: 17 November 2022).

Lapointe, L. and Rivard, S. (2005) 'A Multilevel Model of Resistance to Information Technology Implementation', *MIS Quarterly*, 29(3), pp. 461–491.

Maruna, S. and Copes, H. (2005) 'What Have We Learned from Five Decades of Neutralization Research?', *Crime and Justice*, 32, pp. 221–320.

Mcgloin, J.M. and Thomas, K.J. (2016) 'Incentives for collective deviance: Group size and changes in perceived risk, cost, and reward', *Criminology*, 54(3), pp. 459–486.
McGregor, S.L.T. (2008) 'Conceptualizing Immoral and Unethical Consumption Using Neutralization Theory', *Family and Consumer Sciences Research Journal*, 36(3), pp. 261–276.
Minor, W.W. (1981) 'Techniques of Neutralization: a Reconceptualization and Empirical Examination', *Journal of Research in Crime and Delinquency*, 18(2), pp. 295–318.
Moody, G.D., Siponen, M. and Pahnila, S. (2018) 'Toward a Unified Model of Information Security Policy Compliance', *MIS Quarterly*, 42(1), pp. 285–311.
Morgeson, F.P. and Hofmann, D.A. (1999) 'The Structure and Function of Collective Constructs: Implications for Multilevel Research and Theory Development', *The Academy of Management Review*, 24(2), pp. 249–265.
Myers, M.D. (1997) 'Qualitative Research in Information Systems', *MIS Quarterly*, 21(2), p. 19.
Myers, M.D. and Newman, M. (2007) 'The qualitative interview in IS research: Examining the craft', *Information and Organization*, 17(1), pp. 2–26.
Orlikowski, W.J. and Gash, D.C. (1994) 'Technological frames: making sense of information technology in organizations', *ACM Transactions on Information Systems*, 12(2), pp. 174–207.
Pentland, B.T. (1999) 'Building Process Theory with Narrative: From Description to Explanation', *The Academy of Management Review*, 24(4), pp. 711–724.
Sarker, S. *et al.* (2018) 'Learning from First-Generation Qualitative Approaches in the IS Discipline: An Evolutionary View and Some Implications for Authors and Evaluators', 19(8), pp. 752–774.
Sarker, S. and Valacich, J.S. (2010) 'An Alternative to Methodological Individualism: A Non-Reductionist Approach to Studying Technology Adoption by Groups', *MIS Quarterly*, 34(4), pp. 779–808.
Schabram, K., Robinson, S.L. and Cruz, K.S. (2018) 'Honor among thieves: The interaction of team and member deviance on trust in the team.', *Journal of Applied Psychology*, 103(9), pp. 1057–1066.
Scott, M.B. and Lyman, S.M. (1968) 'Accounts', *American Sociological Review*, 33(1), pp. 46–62.
Searle, J.R. (1990) 'Collective Intentions and Actions', *Intentions in communication*, 401, p. 23.
Silic, M., Barlow, J.B. and Back, A. (2017) 'A new perspective on neutralization and deterrence: Predicting shadow IT usage', *Information & Management*, 54(8), pp. 1023–1037.
Siponen, M., Puhakainen, P. and Vance, A. (2020) 'Can individuals' neutralization techniques be overcome? A field experiment on password policy', *Computers & Security*, 88, p. 101617.
Siponen, M. and Vance, A. (2010) 'Neutralization: New Insights into the Problem of Employee Information Systems Security Policy Violations', *MIS Quarterly*, 34(3), p. 487.
Siponen, M. and Vance, A. (2014) 'Guidelines for improving the contextual relevance of field surveys: the case of information security policy violations', *European Journal of Information Systems*, 23(3), pp. 289–305.
Siponen, M., Vance, A. and Willison, R. (2012) 'New insights into the problem of software piracy: The effects of neutralization, shame, and moral beliefs', *Information & Management*, 49(7), pp. 334–341.
Straub, D.W. and Nance, W.D. (1990) 'Discovering and Disciplining Computer Abuse in Organizations: A Field Study', *MIS Quarterly*, 14(1), pp. 45–60.
Strauss, A. and Corbin, J.M. (1990) *Basics of qualitative research: Grounded theory procedures and techniques*. Thousand Oaks, CA, US: Sage Publications, Inc (Basics of qualitative research: Grounded theory procedures and techniques), p. 270.
Sykes, G.M. and Matza, D. (1957) 'Techniques of Neutralization: A Theory of Delinquency', *American Sociological Review*, 22(6), pp. 664–670.
Topalli, V. (2005) 'When Being Good Is Bad: An Expansion of Neutralization Theory*', *Criminology*, 43(3), pp. 797–836.
Venkatraman, S. *et al.* (2018) 'The "Darth" Side of Technology Use: An Inductively Derived Typology of Cyberdeviance', *Journal of Management Information Systems*, 35(4), pp. 1060–1091.
Walters, M. (2022) *Four Practical Steps To Eliminate Shadow IT Permanently*, *Forbes*. Available at: https://www.forbes.com/sites/forbestechcouncil/2022/02/25/four-practical-steps-to-eliminate-shadow-it-permanently/ (Accessed: 6 March 2023).