New Insights into the Justifiability of Organizational Information Security Policy Noncompliance: A Case Study

Wael Soliman
University of Jyvaskyla
wael.soliman@jyu.fi

Hojat Mohammadnazar
University of Jyvaskyla
hojat.h.mohammadnazar@jyu.fi

Abstract

Information security policies as apparatus for communicating security principles with employees are the cornerstone of organizational information security. Resultantly, extant literature has looked at different theories to better understand the noncompliance problem. Neutralization theory is emerging as one of the most popular approaches, not only as an explanation but also as a solution. In this in-depth qualitative study, we ask the question 'how do employees justify violating the ISP'? Our findings reveal nine rationalizing techniques, three of which have not been recognized in previous research. We label them 'I follow my own rules', 'matter of mere legality' and 'defense of uniqueness'. But more importantly, our in-depth insights point to the danger of taking these rationalizations out of context, since without context, it becomes impossible to judge whether the behavior or the rule, needs correcting, reflecting a dilemma recognized in the original writing of neutralization theory, which has since been forgotten.

1. Introduction

With increasing reliance of organizations on cyber environments for managing their daily operations, protection of information assets in such environments becomes ever more crucial. Various threat classifications have been introduced [1], of which threats emanating from employees (i.e. insider threat) is considered "the greatest threat to information security" [2]. Indeed, it is widely acknowledged among scholars of information systems security (hereafter, ISS) that information security policy (hereafter, ISP) and its enforcement constitute the foundation of an organization's information security [3], [4]. In most behavioral ISS research, ISP reflects low-level policies which contains "normative lists of actions that the employees should (or should not) perform" [3]. Formally, these normative lists of actions, or rules, are the ultimate authoritative voice against which employees are held accountable. Considering the critical role that ISPs could play in ensuring the security of organizational information assets, many ISS scholars have emphasized that policy enforcement should be non-negotiable, and that "an unenforced policy is not worth the paper it is written on" [5]. It would be safe to argue that solving the ISP noncompliance problem has become the mantra of mainstream ISS research. Neutralization theory [6] is emerging as a popular lens in ISS research [7]–[9], especially that it has the capacity to double both as an explanation and solution to the noncompliance problem. As an explanation, neutralization theory is used to demonstrate that employees apply various rationalizations (aka neutralization techniques) in order to liberate themselves from normative restrictions, thereby making policy violations easier to justify [4]. Current ISS research provides evidence in line with this argument [10]–[12]. As a solution, neutralization theory is used to devise training programs tailored to the specific techniques with the aim of de-neutralizing them [13], [14].

Despite these extremely important insights into employees' use of neutralizations and the proposed solutions, it is surprising to find that very little has been done to hear the employees' voices regarding the justifiability of ISP violations committed in the specific context of their work environment. Furthermore, as of yet, there is little evidence to suggest that ISS researchers have considered the possibility that ISP, rather than employees' neutralizations, needs correcting. After all, research in criminology has recognized that 'not all neutralizations are bad' [15, p. 228]. If this is the case in the ISS context as well, then we might be missing crucial insights if all employees' insights are dismissed as (bad) neutralizations.

Lack of understanding of the context of violation may lead to the adoption of 'no-justification-allowed' approach, which would be problematic in situations where even justifiable reasons for violating an ISP rule would be reported as 'making excuses' [16], when the correct course of action would have been a modification in the security measure and its corresponding policy. Research of this nature is inherently qualitative, which is currently lacking and much needed [17], [18]. Given this research gap, in this article we report our findings from an in-depth qualitative study [19], [20]. In conducting this study, not only have we gained insights

URI: https://hdl.handle.net/10125/80163
978-0-9981331-5-7

that extends neutralization theory through the identification of novel techniques, but also, we demonstrate that employees' justifications for policy violation are context-dependent and in some cases may point our attention to flaws in the rules, rather than in the behavior.

2. Theoretical background

Information security policy (ISP) is recognized as the foundation of organizational information security since it communicates to the employees what they can and cannot do with the organization's assets [3]. Therefore, understanding of employees' ISP (non)compliance behavior has become one of the major concerns for information security researchers [4], [13], [14], [21]. In this domain, neutralization theory [6], [22] is emerging as a popular lens to examine how employees justify violating workplace ISPs. Neutralization theory [6] was introduced to explain how delinquents, especially those in the early stages of their criminal career, deploy various techniques that enable them to drift between the worlds of the law-abiding citizen, and that of a delinquent. Sykes and Matza [6] identified five such techniques and called them neutralizations techniques. These are, 'denial of responsibility', 'denial of injury', 'denial of victim', 'condemnation of condemners', and 'appeal to higher loyalties'.

Each of these techniques provides a counterargument (hence the name, neutralization) to rationalize or justify the deviant behavior from the offender's point-of-view. The 'denial of responsibility' technique is used to liberate oneself from any sense of accountability and control with respect to the situation at hand, by arguing, for example, that "I didn't mean it" [6, p. 669]. 'Denial of injury' provides a rationalization that diminishes the impact of the act, whereby the offender would claim, for example, that "I didn't really hurt anybody" [ibid]. The 'denial of the victim' technique involves a confrontational argument denying the existence of a victim in the first place, suggesting that the victim deserved what happened and that "they had it coming" [ibid]. The 'condemnation of the condemners' is a technique by which the offender turns the spotlight on those who disapprove of the activity to undermine them usually by arguing that "everybody is picking on me" [ibid]. Lastly, the offender might 'appeal to higher loyalties' and argue that engaging in the offense is out of loyalty to groups such as family or friends and it is not due to lack of respect for norms of the society at large, for example, "I didn't do it for myself" [ibid]. Later research in criminology has unearthed further techniques that offenders could deploy to neutralize anti-social behavior. 'Metaphor of the ledger' [23], 'defense of necessity' [24], 'claim of individuality' [25] 'justification by comparison', 'justification by postponement' [26], 'claim of entitlement' [27], 'everybody does it' [27], and 'claim of relative acceptability' [25] are among the techniques that have been developed in addition to the initial five techniques.

In the ISS field, neutralization theory has been used to explain deviance in two main research themes. The first theme covers workplace deviance committed by employees. Under the workplace deviance theme, two distinct topics have dominated this area of research: one explores the justifiability of crimes committed by employees, such as hacking and stealing [28], [29]; and the other explores non-criminal violations of organizational policy, such as, cyberloafing [12], [30] and shadow IT use [11], [31]. The second research theme, in turn, covers deviant behavior outside of organizational context, which explores the justifiability of software and music piracy [32]–[34]. To date, however, neutralization-based ISS research design has been predominantly confirmatory in nature, aiming to test the extent to which one or more neutralization techniques is significantly associated with a given violation. In this regard, multiple studies provide evidence that neutralization techniques could increase one's intention to engage in ISP violation in general [8], [35]–[37], commit computer abuse [29], [38], use the workplace Internet for personal purposes [30], [39], [40] as well as engage in shadow IT use [11]. Furthermore, some studies suggest that deploying neutralization techniques may discourage employees from complying with ISP [10], [41], [42]. While these studies generally focus on testing the extent to which neutralization is significantly associated with a given violation; more recent research has started devising neutralization theory-based solutions to ISP violations. One such solution is communicating anti-neutralization messages [13], [14]. For instance, a message targeting 'denial of injury' would stress that "there is always the possibility for harm" [13]. Results from two studies that examined the mitigating effect of anti-neutralization messages showed that users who received such messages were more likely to be discouraged from ISP violation compared to those who did not receive any communication messages [13], [16]. Another solution that has been investigated for neutralization prevention is anti-neutralization training [14]. After conducting a training program targeting users' neutralization of password policy violation, Siponen et al. [14] reported that overall the training programs based on cognitive dissonance reduced neutralization even though training might have been ineffective for specific techniques such as, 'claim of entitlement', 'claim of relative acceptability' and 'Justification by comparison'.

Despite the very important insights we gain from these studies, it is surprising to find that we lack context-specific and data-driven (i.e., inductive) research [43]–[45] that aims to understand how employees, in their own words, rationalize and justify ISP violations committed in their workplace. The only exception is Lim and Teo [46] whose work on cyberloafing recognized the importance of the 'shifting work home' phenomenon. Beyond this single effort, no attempt has been made to probe the violator's worldview. Such explorative approach, not only does it offer evidence of the applicability (or lack thereof) of neutralization theory in different contexts, but also it offers a unique opportunity to discover new neutralization techniques specific to ISP violations.

3. Research approach

The study reported here is based on a qualitative inquiry [19], [20] conducted between 2016 and 2018, with the general aim of understanding the employees' perspective regarding the role ISP plays in guiding their everyday work routines, in the context of a large research-oriented Nordic university. Several calls have been made to conduct such research in the ISS field to complement the dominant functional view, which generally favors "normative logic and predictive capacity" [47], at the expense of understanding what employees actually do in real life settings [17], [18]. In balance, in this research we explore how the neutralization theory lens could help us better understand the employees' information security noncompliance behavior. Hence, our approach emphasizes the examination of a phenomenon in its naturalistic context, with the purpose of confronting theory with the empirical world [48], [49]. Not only does our research approach support the understanding of a phenomenon in its natural setting, but also it advocates adopting neutralization theory as a sensitizing device to ensure that we enter the research setting with an 'open'–rather than 'empty'–mind [50]. Research based on neutralization theory acknowledges the subjective interpretive nature of neutralizations, and that there can be multiple interpretations for the same event and the justifications used within. Maruna and Copes [15] notes: "Every event is subject to multiple interpretations … [O]ne person's rational explanation is another's rationalization. If neutralizations are to carry any psychological weight, they must, at least partially, be believed by the person using them" [15, p. 230]. With this emphasis, we wish to highlight that in our analysis and identification of the neutralization techniques, we do not treat them as 'lies' or 'deceptions'; rather as mere justifications.

In terms of data collection, this study builds on multiple data sources including formal interviews, informal discussions, official documents (e.g., the official information security policy), as well as personal observation. Regarding the interviews, scheduled interviews were conducted with eighteen participants between October 2016 and September 2018. The participants were all on the payroll, and held various positions in the organization, including, administration staff, teacher, doctoral candidate, post-doctoral researcher, and professor. All interviews were conducted face-to-face, and on average, each lasted for one hour. All interviews were recorded, and the interviewees were promised anonymity, so they will be referred to in this study as "Interviewee # …". All recorded interviews were treated with utmost care, and to ensure anonymity they were transcribed and anonymized by the first author alone. Then the transcribed text was shared with the second author for further analysis. Interviews were semi-structured [51], and the main themes revolved around each participant's perception of and attitude towards the workplace ISP, to gain an in-depth understanding of its role in shaping their personal day-to-day computer use behavior. As such, the interview protocol was designed to elicit insights about the employees' perception of ISPs in general, as well as about specific security behaviors [52]. General perceptions about ISP reflected questions such as to what extent they were aware of the official ISP, what it meant to them in the workplace, and how they felt ISP impacted their daily routines at work. Specific questions, on the other hand, focused more on discussing the participant's views of specific rules as stated in the ISP (e.g., password change rule and personal IT use rule), to what extent they comply or violate these specific rules, and in the case of violation what they considered the best course of action to fix the situation. During each interview, the official ISP (either a printout or onscreen) was used to facilitate the discussion.

All interview transcripts were coded using both first- and second-order themes [53] Specifically, first-order codes are more reflective of the empirical data and represent as close as possible the narratives as generated by the participants themselves. By contrast, second-order codes are more analytic in nature as they reflect the analysts' interpretation of these concepts, which in our case, are influenced by the theoretical lens of neutralization. For instance, we consider the code 'ISP_is_Stupid' to be first-order code since it reflects the participant's utterance. Subsequently, we code the same utterance using the second-order code 'Condemnation_of_the_Condemners', which is consistent with neutralization theory. This process allowed categorizing the violation justifications according to known neutralization techniques, as well as identifying new justifications. The two authors discussed all resultant techniques in various meetings until a final agreement was achieved.

4. Findings

This section reports the main findings regarding the research question: '*how do employees justify violating the ISP*'? Due to space limitation we decided to report only our findings regarding neutralization techniques that are used by at least one-third of the participants. With this in mind, our analysis reveals the prevalence of nine neutralization techniques used by our participants to justify their ISP violations. Three of these techniques are classical and are well-known in the literature since they originate in Sykes and Matza's [6] work. Namely, 'denial of responsibility', 'condemnation of the condemners', and 'denial of injury'. Three technique have been further developed by criminologists and are somewhat known in various ISS writings. Namely, 'defense of necessity', 'justification by comparison', and the 'everybody does it' claim. Finally, we introduce three novel techniques specific to ISP violations that are not recognized in previous work. Namely, 'matter of mere legality', 'defense of uniqueness', and 'I follow my own rules'. We discuss each of these categories in turn.

1. Denial of responsibility. The 'denial of responsibility' technique is the most applied technique for policy violation in our study. Sykes and Matza [6] explain that 'denial of responsibility' allows delinquents to liberate themselves from normative restrictions by negating personal accountability. In this sense, employees who use the 'denial of responsibility' technique could argue that they were not in control of the situation, rather, they were acted upon by other responsible actors [26]. Fourteen participants used this technique. The use of this neutralization technique among our interviewees came to light when they were introduced with a copy of the official policy, at which point many of them realized that they had not seen it before or did not remember its content. Moreover, some went further to argue that no one stopped them from violating the policy and therefore they were not to be blamed. Meanwhile, others wished that someone else would take the burden of understanding and summarizing the ISP on their behalf. In general, the prevalence of this technique suggests that the interviewees see that it is not their responsibility to exert an effort on searching for the organization's ISP and study its content. One interviewee sums up the use of this technique: *"I think the main responsibility lies in the upper persons working in their office. I think it's the ones who make the policy should make sure everybody knows about it and knows about the different steps. I think if, for example, you start working for the university, people should tell you how to do, and you should not try to find things yourself, because there are millions of things that you have to learn about. Then I wouldn't put the responsibility on the employee, it's the responsibility of the employer to tell their employees that this is the policy to follow. So, I think the responsibility somewhere higher than on the average worker here."* [Interviewee #11].

2. Condemnation of the condemners. The 'condemnation of the condemners' neutralization technique enables an offender to shift the blame from oneself to those who disapprove of the action [6]. When deploying this technique an offender may claim that those who disapprove of the action are hypocrites who themselves commit the offense [6]. In criminal research, deploying this neutralization technique suggests that the offender views the enforcer as corrupt [26]. In ISS context, this technique often reflects disapproval of the ISP as being unreasonable [8], or that those who enforce IT policy may themselves engage in similar behavior [31]. In line with the common interpretation in ISS research, we find that thirteen participants used this technique. We observed the 'condemnation of the condemners' neutralization technique clearly reflected a criticism towards the ISP itself as being 'outdated', 'lame', 'ridiculous' and even 'stupid'. For instance, one participant believes that the policy section related to personal IT use "*doesn't make too much sense, because all the things that I do on daily basis are somewhat related to private use"* [Interviewee #16]. Similarly, others would think that this rule is "*kind of old fashion*" and it could have made more sense if it was introduced "*five or ten years back"* [Interviewee #6]. In addition to condemning the rules within the policy, some have also criticized those responsible for introducing those impractical rules in the policy in the first place. For instance, Interviewee #15 criticized the management style and what managers do with their time when the outcome is a policy such as this one. They note: "*But these are the issues that I never understood. Maybe we're having too many bosses. Too many high salary people who do not have anything better to do. Yeah. But that's the way it is."* [Interviewee #15].

3. Denial of injury. Using the 'denial of injury' technique allows an offender to render their action as harmless [6]. Since there is no harm, the offender could argue that the behavior is not blame-worthy. In criminology, the 'denial of injury' neutralization technique reflects the common argument that, for instance, a shoplifter could argue that big stores make a lot of money so 'they don't miss the little bit I get' [26]. Similarly, In ISS context, employees may deploy 'denial of injury' by justifying that their security violation is a minor issue and does not hurt anyone [16]. In the study at hand, thirteen interviewees used this technique. The use of ‘denial of injury’ neutralization technique was evident when interviewees directly noted that their policy violations were harmless. Generally, many interviewees regarded the role of ISP to be suggestive at best, and that violating it is acceptable as long as no harm is done. *“... somehow the policies are drawing the boundary, so as long as people, kind of, within the boundary, or somehow a little beyond the boundary but, it doesn't really harm the security of those IT resources, or it doesn't really dramatically create negative impact on job performance, then I think it's somehow ok”* [Interviewee #5]. When interviewees were asked to elaborate their views further using the specific example of the personal IT use rule, some took a productivity perspective and clarified that violating it is acceptable since “*there's no harm except the work time lost that I can make up by working a bit later, or working at home when the kids are in bed.” [Interviewee #17].* Others, however, took a purely financial perspective and justified rule breaking on the basis of the economic impact of the violation: *“unless there's something I don't know about, I mean, it doesn't cost any more money, does it? ... Is there a loss of money to the university for me looking at a holiday website in my lunch break?”* [Interviewee #10].

4. Defense of necessity. The ‘defense of necessity’ neutralization technique holds that an offense is necessary to achieve a crucial outcome (Coleman, 1987). Consequently, since the offense is necessary and the offender has no other choice, there is no need for feeling guilty or ashamed [24], [26]. In criminal research, thieves for example would use the ‘defense of necessity’ technique to argue that stealing was the only way to feed the family [26]. In ISS context, employees may deploy this technique by arguing that due to time constraints, violation of the ISP is necessary for completing their tasks [8]. In the current study, half of the interviewees appealed to this technique. The ‘defense of necessity’ was evident in arguments whereby compliance with the ISP was framed as an obstacle to efficiency, or a secondary priority in the face of the pressing demands of work requirements. Talking about the ISP in general, several interviewees advanced arguments similar to this one: “So, *security and complying with the policy is secondary in priorities compared to the primary things that needs to be done; what I'm here to do.”* [Interviewee #11]. When asked to elaborate their rationale, one interviewee gives further explanation: *“I mean it is like, if you follow this 100% [pointing to the personal IT use rule], you couldn't visit any webpage with your work computer, for example, that are not 100% related to work. Then you would all the time have to carry 2 computers with you. And then if you have a browser open in one computer, then you would have to open the other one and open a browser there just to visit, for example, one page. So, it would be a lot of hassle, a lot of extra work, and in the end, I think it would also be detrimental to your work effectiveness.”* [Interviewee #11].

5. Justification by comparison. The idea behind the ‘justification by comparison’ technique is quite simple, by arguing that the violation in question is much better than a much worse violation. When deploying this technique, an offender acknowledges that they are engaging in a wrongdoing but justifies their action by arguing that they could have done worse. In criminal research, shoplifters for instance would argue that stealing from a shop is nothing compared to robbing people or breaking in houses [26]. In ISS research, ‘justification by comparison’ has received little research attention, however, a user can utilize this technique by arguing that an ISP violation, such as violating password policy, is not as bad as wasting the whole day on non-productive work [14]. Nearly half of our participants (eight interviewees) used this technique, when comparing their own (little) ISP violations with what would be considered (truly) serious violations, such as *“downloading movies”* [Interviewee #12], *“watching pornography”* [Interviewee #9], or even *“bitcoin mining”* [Interviewee #17]. Interestingly, there seems to be a general agreement on comparing ISP violations against what would be clearly interpreted as a harmful or illegal, to justify own violations. One interviewee elaborates their perspective: *“if students were running peer-to-peer networking at [online service]. So, that's a clear violation. It's illegal activity. So, that goes beyond the threshold. At that point, yellow card. But, obviously, using Facebook, e-commerce, online banking, doesn't go beyond the threshold of me to get a warning.”* [Interviewee #13].

6. Everybody does it. The ‘everybody does it’ technique involves a “transfer of responsibility from the offender to a large and often vaguely defined group to which he or she belongs” [54]. As such, this technique is commonly used when an offender tries to avoid self-blame by pointing out that others engage in the same activity and that the activity is commonplace and normal in a given context [26], [27]. ISS researchers adopting this technique in their studies have often referred to it with various names, such as ‘defense of ubiquity’ [42] or ‘normalization’ [46]. The main point here is that using this technique often reflects the argument or rationalization that the ISP violation in question is commonplace. In the current study, one-third of the interviewees used this technique to argue that their violation of the ISP was commonly acceptable and normal. When discussing rules in general, it was emphasized that social acceptability can be more important than what the policy dictates. For instance, one interviewee explains *"I'm sure there are a lot of things that I disagree with [in the policy] because of the fact that I don't think socially anybody is complying with it."* [Interviewee #18]. When pressed to clarify their rationale further, some would use the personal IT use rule to point out: "*If you consider basic rule #1 presented there, I think ... that most people around here are not aware of such rule, and I also think that if the policy has rules that you would think by commonsense that 95% of the people are violating–... of course I can't say for sure–but I think that everyone here is violating basic rule #1 at some time during their work"* [Interviewee #11].

7. Matter of mere legality. The 'matter of mere legality' justification is a previously unknown technique of neutralization identified in this study. Nearly half of the study participants (eight participant) used this technique to justify their ISP violation. Using this technique, rule violators argue that a workplace policy is merely a matter of contractual agreement and need not be followed strictly. The employee may assert this position by noting that workplace policies are designed for 'worst case scenarios' in order to protect the organization from legal liabilities in extreme cases, or to provide legal grounds for further action against rogue employees. In deploying this technique, in addition to pointing out the legal qualities of the ISP, participants have also noted that the ISP is not a document to communicate information security measures and guidelines but a legal document that is reserved for gross violation or difficult individuals. But for as long as the employee is generally careful about not causing any harm (see 'denial of injury'), and doing a generally good job (see 'metaphor of the ledger'), then these ISP rules belong only 'in the drawer'. Surprisingly, this is an assumption several interviewees share even without knowing what the content of the policy is. One participant notes: *"I explained I haven't read that [pointing to ISP], ... and I think without reading that–I might be wrong, of course–I think this manual is 10 pages that liberate the [employer] or whoever wrote that, from the, hmm, let's say, the legal side of things, if someone does something wrong on purpose. It wasn't written for the employee ... hmm, the purpose of that document is not to help the employees to do stuff, like, in secure way; it's just something that's required legally".* [Interviewee #2]. Similarly, Interviewee #18 explains: "*If you are in a situation with an employee where the employee becomes difficult, you can always say: Okey, there's this policy, you're supposed to have read it"*, and then punitive action can be easily taken against the trouble-maker. More interestingly, the 'matter of mere legality' justification does not reflect disgruntlement against the policy; rather, it reflects a general understanding that this is how policies should be written, but for legal purposes only. Interviewee #10 expresses this idea well: *"Yeah. I understand why these have to be here. I really do. But, nowadays, and more specifically within this environment, it's really for the purposes of them being able to getting us legally. Because we roughly know what we're doing."* In fact, Interviewee #17 thought that if they were asked to write a policy, they would write it in that exact same way, but that does not mean that they would not violate it!

8. Defense of uniqueness. The 'defense of uniqueness' is a newly identified technique of neutralization in this study. Nearly half of the study participants (eight participant) used this technique to justify their ISP violation. Using this technique, a policy violator questions the contextual relevance of the policy and argues that certain policies are not applicable to the setting in which the violation occurs. In doing this, the violator raises the issue that the setting has unique qualities that make certain rules inapplicable in that setting while drawing comparison with other settings in which the rule applies. Although this technique involves a comparative process like the 'justification by comparison' technique; what we identified here is different. Specifically, whereas the 'justification by comparison' is violation-oriented (i.e., the violation in question is not as bad when compared with much worse ones); the 'defense of uniqueness' is context-oriented (i.e., the rule in question may be suitable to other contexts, but not ours). Participants in this study used this technique to differentiate between their line of work with others, either in the same organization or in other organizations. Furthermore, in some cases they directly argued that the ISP is not applicable to them due to the nature of their work. One interviewee explains their general view regarding the contextual relevance of rules: *"I've worked in a number of different organizations with different levels of education. You get a lot of a**holes out there who, hmm, who would do what they want, and take the f*ck what they want, and don't give a sh*t about the consequences. These are what these rules are there for. But [here], we're all generally a decent punch of people."* [Interviewee #10] When talking specifically about the personal IT use rule, another interviewee gives a more specific explanation for the violation: "*... I understand if I work in an organization that is very, like military, or something like that, I understand that I'm not allowed to do my personal stuff by my working computer, or through the network of that organization. But here, hmm, ... I don't do anything like that, hmm. So my work is not related to anything that should be so secure that I can't use my work computer to read my emails."* [Interviewee #14].

9. I follow my own rules. 'I follow my own rules' is the third newly identified technique which reflects the argument that a violator has enough knowledge and/or expertise to decide which rules to follow, and which to bypass. This also reflects an awareness that not all rules are equal; some are meant to be broken. Nearly half of the study participants (eight participant) used this technique to justify their ISP violation. By using this technique, the violator argues that they have developed their own set of rules, some of them will be compliant with the ISP, but some others may coincidentally violate it. Our participants used this technique when justifying their disregard for the official ISP, and that it is enough to follow their own rules. For instance, Interviewee #4 explains that it once crossed their mind to check the ISP, but eventually decided not to. When they were asked to explain why they think they did so, they replied: *"Why do I think I do that? ... Because I have my own judgment of what might be good and what might be bad, hahaha"* [Interviewee #4]. Interestingly, the 'I follow my own rules' seems to require proof of past success. That is, those rules that end up in the employee's own internalized 'rule-set' are the ones that have so far been effective in keeping them out of trouble. One interviewee points out: "*I'll follow my own habit, because I think it has been quite successful thus far*" [Interviewee #12]. When another was asked to elaborate on how they developed their own rules; they replied: *"It's taken maybe 15 years to come up with the standards that I have now. When it all started? I don't really know. Perhaps one of the aspects is like watching people do their stuff, and someone saying that 'you should have a strong password' or 'you shouldn't leave these computers open' ... to be blunt, those 10 pages I haven't read, like I said, but I think it's gonna be 10 pages of common-sense."* [Interviewee #2].

5. Discussion

In the previous section we presented our main findings regarding the neutralization techniques our study participants used to justify violating ISP in a Nordic university context. Next, we discuss the most salient theoretical and practical implications of these findings.

5.1. Theoretical implications

First, our findings contribute to the depth of knowledge on neutralization theory in activities related to information security. While there is a sizeable literature on neutralization theory in ISS research, much of this research has been conducted using a quantitative cross-sectional research design and little has been done to explore users' justification for real violations in real contexts. In fact, with a few exceptions [46], [55], we have not found any studies that examined employees' justifications in response to their workplace policy violations. This study steps up to this challenge and in doing so provides insights regarding the use of neutralization techniques in ISS context. Sykes and Matza [6] have acknowledge that neutralization techniques are context-specific, meaning that some techniques might be more (or less) relevant in certain contexts. Our findings lend support to the assertion that the techniques 'denial of responsibility', 'denial of injury' and 'condemnation of the condemners' are the most prevalent classical techniques. Meanwhile, some techniques such as 'denial of the victim' [6], though a classical technique, might be less relevant in similar contexts. In this regard, our findings are in line with Siponen and Vance's [8] contention that the 'denial of victim' neutralization technique might be irrelevant in ISP violation cases due to the difficulty of identifying victims. Our findings, therefore, highlight the need for further explorative studies in other ISS related activities such as computer abuse, shadow IT use and cyberloafing to determine which techniques may or may not be relevant to each activity.

Second, this study contributes to neutralization theory by identifying three previously unknown neutralization techniques, namely, 'matter of mere legality', 'I follow my own rules', and 'defense of uniqueness'. These newly identified techniques seem to be associated with distinctive qualities of ISPs. The 'matter of mere legality' technique highlights the juxtaposition of ISPs as legal documents as well as tools for communicating security do's and don'ts [56]. The 'defense of uniqueness' technique, on the other hand, addresses the context-specificity of the work environment. Since organizations have different needs and different working climates, an 'one-size-fits-all' approach to ISPs may not be ideal [57]. Lastly, the 'I follow my own rules' technique underscores the importance of recognizing individual competence and personal experience. ISPs may contain information that requires high competence and skill to implement [58]. The caveat, however, is that when an individual possesses such competence and experience, they may develop their own ways of handling information security and fall into a false sense of confidence regarding their own abilities hence rejecting ISPs as helpful communication tools. Alternatively, employees' own rules might be more attuned to the specificity of their situation, than the policy. In such situations, we are faced with a dilemma: what needs correction, the employee's behavior or the policy? Answering this question points to our third theoretical implication.

This dilemma carries within, a value judgement regarding the adequacy of the neutralizations. If the neutralization is adequate, then employees' behaviors need not be corrected, which means that our attention should be placed on changing the policy itself. So far, research based on neutralization theory has not addressed this question, which not only does it bear theoretical implications, but also practical implications (see, practical implications section). Sykes and Matza [6] were well aware of this dilemma and hinted to some direction for resolving it. Specifically, Sykes and Matza [6] contemplated the question "why men violate the laws in which they believe" [6, p. 666]. To answer this, they point to "the fact that social rules and norms … seldom if ever take the form of categorical imperatives" (ibid), and because of this contextual flexibility, they argue, any functioning legal system deliberates about the "defenses to crimes" before giving a verdict regarding a given act. Of course, in many situations, the justice system deems justifications inadequate, and corrective measures need to be taken. However, in some situations, even what is generally regarded as *mala in se*, or evil-by-nature crimes [59], [60], such as killing a human being, are acquitted because they were 'justified' (e.g., in self-defense). Yet, in other situations, certain rules had to be challenged and violated before any law itself needed to change. Interestingly, despite Matza and Sykes' [6] recognition of this assumption, it has not attracted scholarly attention, leading Maruna and Copes, half-a-century later, to remind us that "the treatment of neutralization techniques as automatically 'bad things' in criminology and corrections is an oversimplification of a complex and substantial body of literature" [15, p. 228]. In line with these insights, we suggest neutralizations should be regarded as provisional pleas until a verdict is made. The practical implications of this insight will be discussed in the next section.

5.2. Practical implications

There are two challenges related to the production of meaningful practical implications: (a) the degree of violation-specificity, and (b) the degree of context-specificity. Degree of violation-specificity regards one's perception of the ISP as a collection of rules and guidelines rather than a single entity. We learned early on that the participants did not perceive the ISP as a single entity guiding their security behavior. Nearly all our interviewees have been complying with some ISP rules but violating one or more other rules. For instance, one interviewee might be unyielding about password sharing (complying with password rule) but using the work computer to pay personal bills or read the news (violating the personal IT use rule). Practically speaking, when employees are asked general questions about the extent to which they comply with or violate ISP (in general), it is impossible to discern which neutralization techniques are relevant to which violation. So, we fear that using such generic questions will not produce meaningful insights to security professionals and consultants regarding what the employees are actually doing in the workplace. Consequently, we suggest that future explorations of ISP violations to be narrower in their scope to be more practice-relevant [61].

Second, regarding the degree of context-specificity, we realized a critical practical dilemma, even after narrowing the scope of violation-specificity to one specific rule. During the course of each interview after going through general discussions regarding the ISP, each participant was confronted with a rule from the ISP (such as basic rule #1). As noted earlier, this basic rule bars users from all non-work related use. Approaching and analyzing participants' responses to such rules without due consideration of context using the neutralization theory indicated clear use of various neutralization techniques from a 'context-less perspective'. Prohibiting all non-work related use of the organization resources is justified by countless writings on the threats of such violation. Not only does personal use of IT expose the organization to various security threat such as viruses, spam, and malware [62], but also introduces loss of productivity [12].

These concerns are legitimate, and therefore the obvious recommendation of a context-less perspective would be to curb the violations by developing counter-neutralization strategies tailored to the specific techniques we identified. Regarding the 'condemnation of the condemners' technique, a typical recommendation is to suggest anti-neutralization communication, and training aimed at correcting the employees' behavior by creating cognitive inconsistencies between what they do and the justifiability of their rationalizations [13], [14], [16]. Following this line of thought, a practical recommendation would be developing training and persuasive messages to teach the learners that criticizing the ISP is not acceptable (a generic approach), or that it is an immoral thing to do to use the organization resources for personal use (a more specific approach). Regarding the 'matter of mere legality' technique, a straightforward practical recommendation is the enforcement of monitoring and immediate sanctioning of violators to demonstrate the seriousness of the ISP [63]. Other technique-specific solutions are available, such as victim-offender mediation which is thought to be effective with the 'denial of injury' technique [8].

However, considering the specific nature of the studied context, one might see things differently. In this specific research-oriented environment where employees believe that creativity and openness are core values, and where the line between what they do at work and at home is thinning, there is good chance that the neutralizations identified in this research need not be deneutralized. There might be truth (i.e., adequacy) to the argument that strict adherence to the ISP regarding personal IT use would hinder, rather than improve, the functioning of this specific organization, especially that the security risk associated with personal IT use does not outweigh its benefits in the studied organization. In fact, the thinning line between work and home and the necessity of managerial attention to this issue before resorting to de-neutralization is recognized in previous literature [46]. Consequently, we suggest that practitioners observe employees justifications with diligence as utterances of employees may reflect their tacit knowledge of the work environment, task requirements, or deficiencies in the ISP; rather than (bad) neutralizations that help them evade accountability [15]. For instance, in our study, 'defense of uniqueness' and 'matter of mere legality' techniques were commonly used justifications. While these justifications could reflect of employees' neutralization of security misbehaviors, it might also reflect a deficiency in the design of the ISP with respect to its relevance and contextual fit. The ISP may in fact require correcting and updating. In this case, 'following own rules' might have been a good neutralization after all.

6. Conclusion

The objective of this study has been to explore the employees' perspective regarding their workplace ISP violation. The guiding research question has been '*how do employees justify violating the ISP*'? Our analysis reveals the prevalence of nine neutralization techniques used by our participants to justify their ISP violations. Three of these techniques were introduced in the original work neutralization theory, 'denial of injury', 'denial of responsibility', and 'condemnation of the condemners'. Three techniques were introduced by later research extensions, namely, 'defense of necessity', 'justification by comparison' and 'everybody does it'. In addition to these six previously recognized techniques, our analysis also revealed three novel and previously unreported neutralization techniques. We called them: 'matter of mere legality', 'defense of uniqueness', and 'I follow my own rules'. Our findings add to the depth and breadth of knowledge regarding application of neutralization theory in the context of ISS by introducing new techniques of neutralization while highlighting the most significant techniques that require practitioner attention. But more importantly, our findings point to the danger of taking these neutralizations out of context, since without context, it becomes impossible to judge whether the behavior, or the rule, needs correcting.

7. References

[1] K. D. Loch, H. H. Carr, and M. E. Warkentin, "Threats to information systems: Today's reality, yesterday's understanding," *MIS Q.*, vol. 16, no. 2, pp. 173–186, 1992.

[2] M. Warkentin and R. Willison, "Behavioral and policy issues in information systems security: the insider threat," *Eur. J. Inf. Syst.*, vol. 18, no. 2, pp. 101–105, 2009.

[3] M. Siponen and J. Iivari, "Six design theories for IS security policies and guidelines," *J. Assoc. Inf. Syst.*, vol. 7, no. 7, pp. 445–472, 2006.

[4] G. D. Moody, M. T. Siponen, and S. Pahnila, "Toward a unified model of information security policy compliance," *MIS Q.*, vol. 42, no. 1, pp. 285–311, 2018.

[5] S. H. Von Solms, "Information security governance - Compliance management vs operational management," *Comput. Secur.*, vol. 24, no. 6, pp. 443–447, 2005.

[6] G. M. Sykes and D. Matza, "Techniques of neutralization: A theory of delinquency," *Am. Sociol. Rev.*, vol. 22, no. 6, pp. 664–670, 1957.

[7] A. Vance, M. T. Siponen, and D. W. Straub, "Effects of sanctions, moral beliefs, and neutralization on information security policy violations across cultures," *Inf. Manag.*, p. 103212, 2019.

[8] M. Siponen and A. Vance, "Neutralization: New insights into the problem of employee information systems security policy violations," *MIS Q.*, vol. 34, no. 3, pp. 487–502, 2010.

[9] R. Willison, M. Warkentin, and A. C. Johnston, "Examining employee computer abuse intentions: insights from justice, deterrence and neutralization perspectives," *Inf. Syst. J.*, vol. 28, no. 2, pp. 266–293, 2018.

[10] J. D'Arcy and P.-L. Teh, "Predicting employee information security policy compliance on a daily basis: The interplay of security-related stress, emotions, and neutralization," *Inf. Manag.*, vol. 56, no. 7, p. 103151, 2019.

[11] S. Haag, A. Eckhardt, and A. Schwarz, "The acceptance of justifications among shadow IT users and nonusers – an empirical analysis," *Inf. Manag.*, vol. 56, no. 5, pp. 731–741, 2019.

[12] L. Khansa, J. Kuem, M. Siponen, and S. S. Kim, "To cyberloaf or not to cyberloaf: The impact of the announcement of formal organizational controls," *J. Manag. Inf. Syst.*, vol. 34, no. 1, pp. 141–176, 2017.

[13] J. B. Barlow, M. Warkentin, D. Ormond, and A. R. Dennis, "Don't even think about it! The effects of antineutralization, informational, and normative communication on information security compliance," *J. Assoc. Inf. Syst.*, vol. 19, no. 8, pp. 689–715, 2018.

[14] M. Siponen, P. Puhakainen, and A. Vance, "Can individuals' neutralization techniques be overcome? A field experiment on password policy," *Comput. Secur.*, vol. 88, 2020.

[15] S. Maruna and H. Copes, "What have we learned from five decades of neutralization research?," *Crime and Justice*, vol. 32, no. 2005, pp. 221–320, 2005.

[16] J. B. Barlow, M. Warkentin, D. Ormond, and A. R. Dennis, "Don't make excuses! Discouraging neutralization to reduce IT policy violation," *Comput. Secur.*, vol. 39, pp. 145–159, 2013.

[17] R. E. Crossler, A. C. Johnston, P. B. Lowry, Q. Hu, M. Warkentin, and R. Baskerville, "Future directions for behavioral information security research," *Comput. Secur.*, vol. 32, pp. 90–101, 2013.

[18] A. M. Mahmood, M. Siponen, D. Straub, H. R. Rao, and T. S. Raghu, "Moving toward black hat research in information systems security: An editorial introduction to the special issue," *MIS Q.*, vol. 34, no. 3, pp. 431–433, 2010.

[19] H. Klein and M. Myers, "A set of principles for conducting and evaluating interpretive field studies in information systems," *MIS Q.*, vol. 23, no. 1, pp. 67–94, 1999.

[20] G. Walsham, "Doing interpretive research," *Eur. J. Inf. Syst.*, vol. 15, no. 3, pp. 320–330, Jun. 2006.

[21] P. Balozian and D. Leidner, “Review of IS security policy compliance: Toward the building blocks of an IS security theory,” *DB Adv. Inf. Syst.*, vol. 48, no. 3, pp. 11–43, 2017.

[22] D. Matza, *Delinquency and Drift*. New York: Wiley, 1964.

[23] C. B. Klockars, *The professional fence*. NY: Free Press, 1974.

[24] W. W. Minor, “Techniques of neutralization: A reconceptualization and empirical examination,” *J. Res. Crime Delinq.*, vol. 18, no. 2, pp. 295–318, 1981.

[25] S. Henry and R. Eaton, *Degrees of Deviance: Student Accounts of Their Deviant Behavior*. Salem: Sheffield Publishing, 1999.

[26] P. Cromwell and Q. Thurman, “The devil made me do it: Use of neutralizations by shoplifters,” *Deviant Behav.*, vol. 24, no. 6, pp. 535–550, 2003.

[27] J. W. Coleman, *Criminal Elite: Understanding White Collar Crime*. New York: St. Martin’s Press, 1998.

[28] S. J. Harrington, “The effect of codes of ethics and personal denial of responsibility on computer abuse judgments and intentions,” *MIS Q.*, vol. 20, no. 3, pp. 257–278, 1996.

[29] M. Nicho and F. Kamoun, “Multiple case study approach to identify aggravating variables of insider threats in information systems,” *C. Assoc. Inf. Syst.*, vol. 35, no. 18, pp. 333–356, 2014.

[30] V. K. G. Lim, “The IT way of loafing on the job: cyherloafing, neutralizing and organizational justice,” *J. Organ. Behav.*, vol. 23, no. l, pp. 675–694, 2002.

[31] M. Silic, J. B. Barlow, and A. Back, “A new perspective on neutralization and deterrence: Predicting shadow IT usage,” *Inf. Manag.*, vol. 54, no. 8, pp. 1023–1037, 2017.

[32] S. Hinduja, “Neutralization theory and online software piracy: An empirical analysis,” *Ethics Inf. Technol.*, vol. 9, no. 3, pp. 187–204, 2007.

[33] J. R. Ingram and S. Hinduja, “Neutralizing music piracy: An empirical examination,” *Deviant Behav.*, vol. 29, no. 4, pp. 334–366, 2008.

[34] M. Siponen, A. Vance, and R. Willison, “New insights into the problem of software piracy: The effects of neutralization, shame, and moral beliefs,” *Inf. Manag.*, vol. 49, no. 7–8, pp. 334–341, 2012.

[35] S. Bauer, E. W. N. Bernroider, and K. Chudzikowski, “Prevention is better than cure! Designing information security awareness programs to overcome users’ non-compliance with information security policies in banks,” *Comput. Secur.*, vol. 68, pp. 145–159, 2017.

[36] S. Altamimi, T. Storer, and A. Alzahrani, “The role of neutralisation techniques in violating hospitals privacy policies in Saudi Arabia,” *2018 4th Int. Conf. Inf. Manag. ICIM 2018*, pp. 133–140, 2018.

[37] P. L. Teh, P. K. Ahmed, and J. D’Arcy, “What drives information security policy violations among banking employees? Insights from neutralization and social exchange theory,” *J. Glob. Inf. Manag.*, vol. 23, no. 1, pp. 44–64, 2015.

[38] T.-C. Lin, J. S.-C. Hsu, Y.-C. Wang, and S. Wu, “Examining the antecedents of employee unauthorized computer access,” *J. Stat. Manag. Syst.*, vol. 21, no. 3, pp. 493–517, 2018.

[39] L. Cheng, W. Li, Q. Zhai, and R. Smyth, “Understanding personal use of the internet at work: An integrated model of neutralization techniques and general deterrence theory,” *Comput. Human Behav.*, vol. 38, pp. 220–228, 2014.

[40] R. Rajah and V. K. G. Lim, “Cyberloafing , Neutralization , And Organizational Citizenship Behavior,” in *Pacific Asia Conference on Information Systems*, 2011.

[41] S. Bauer and E. Bernroider, “From Information Security Awareness to Reasoned Compliant Action : Analyzing Information Security Policy Compliance in a Large Banking Organization,” *DB Adv. Inf. Syst.*, vol. 48, pp. 44–68, 2017.

[42] S. Kim, K. Yang, and S. Park, “An Integrative Behavioral Model of Information Security Policy Compliance,” *Sci. W. J.*, 2014.

[43] S. Sarker, X. Xiao, and T. Beaulieu, “Qualitative studies in information systems: A critical review and some guiding principles,” *MIS Q.*, vol. 37, no. 4, pp. iii–xviii, 2013.

[44] S. Sarker, X. Xiao, T. Beaulieu, and A. S. Lee, “Learning from first-generation qualitative approaches in the IS discipline: An evolutionary view and some implications for authors and evaluators (PART 1/2),” *J. Assoc. Inf. Syst.*, vol. 19, no. 8, pp. 752–774, 2018.

[45] S. Sarker, X. Xiao, T. Beaulieu, and A. S. Lee, “Learning from first-generation qualitative approaches in the IS discipline: An evolutionary view and some implications for authors and evaluators (PART 2/2),” *J. Assoc. Inf. Syst.*, vol. 19, no. 9, pp. 909–923, 2018.

[46] V. K. G. Lim and T. S. H. Teo, “Prevalence, perceived seriousness, justification and regulation of cyberloafing in Singapore: An exploratory study,” *Inf. Manag.*, vol. 42, no. 8, pp. 1081–1093, Dec. 2005.

[47] K. Njenga and I. Brown, “Conceptualising improvisation in information systems security,” *Eur. J. Inf. Syst.*, vol. 21, no. 6, pp. 592–607, 2012.

[48] R. Piekkari, C. Welch, and E. Paavilainen, “The case study as disciplinary convention: Evidence from international business journals,” *Org. Res. Methods*, vol. 12, no. 3, pp. 567–589, 2009.

[49] M. Keutel, B. Michalik, and J. Richter, “Towards mindful case study research in IS: A critical analysis of the past ten years,” *Eur. J. Inf. Syst.*, vol. 23, no. 3, pp. 256–272, 2014.

[50] N. Siggelkow, “Persuasion with case studies,” *Acad. Manag. J.*, vol. 50, no. 1, pp. 20–24, Feb. 2007.

[51] M. D. Myers and M. Newman, “The qualitative interview in IS research: Examining the craft,” *Inf. Organ.*, vol. 17, no. 1, pp. 2–26, Jan. 2007.

[52] M. Karjalainen, S. Sarker, and M. Siponen, “Toward a theory of information systems security behaviors of organizational employees: A dialectical process perspective,” *Inf. Syst. Res.*, vol. 30, no. 2, pp. 687–704, 2019.

[53] V. Braun and V. Clarke, “Using thematic analysis in psychology,” *Qual. Res. Psychol.*, vol. 3, no. 2, pp. 77–101, 2006.

[54] J. W. Coleman, “Toward an Integrated Theory of White-Collar Crime,” *Am. J. Sociol.*, vol. 93, no. 2, pp. 406–439, 1987.

[55] S. Bauer, E. W. N. Bernroider, and K. Chudzikowski, “Prevention is better than cure! Designing information security awareness programs to overcome users’ non-compliance with information security policies in banks,” *Comput. Secur.*, vol. 68, pp. 145–159, 2017.

[56] B. Von Solms, “Information security - A multidimensional discipline,” *Comput. Secur.*, vol. 20, no. 6, pp. 504–508, 2001.

[57] R. Baskerville and M. Siponen, “An information security meta-policy for emergent organizations,” *Logist. Inf. Manag.*, vol. 15, no. 5/6, pp. 337–346, 2002.

[58] P. Ifinedo, “Information systems security policy compliance: An empirical study of the effects of socialisation, influence, and cognition,” *Inf. Manag.*, vol. 51, no. 1, pp. 69–79, 2014.

[59] M. S. Davis, “Crimes mala in se: An equity-based definition,” *Crim. Justice Policy Rev.*, vol. 17, no. 3, pp. 270–289, 2006.

[60] S. P. Green, “The conceptual utility of malum prohibitum,” *Can. Philos. Rev.*, vol. 55, no. 1, pp. 33–43, 2016.

[61] M. Siponen and T. Klaavuniemi, “Narrowing the Theory’s or Study’s Scope May Increase Practical Relevance,” in *Proceedings of the 52nd Hawaii International Conference on System Sciences*, 2019.

[62] K. C. Demek, R. L. Raschke, D. J. Janvrin, and W. N. Dilla, “Do organizations use a formalized risk management process to address social media risk?,” *Int. J. Account. Inf. Syst.*, vol. 28, no. December 2017, pp. 31–44, 2018.

[63] L. Y. Connolly, M. Lang, J. Gathegi, and D. J. Tygar, “Organisational culture, procedural countermeasures, and employee security behaviour A qualitative study,” *Inf. Comput. Secur.*, vol. 25, no. 2, pp. 118–136, 2017.