Journal of the Association for Information Systems (2021) **22**(3), 797-826
doi: 10.17705/1jais.00680

RESEARCH ARTICLE

ISSN 1536-9323

High-Risk Deviant Decisions: Does Neutralization Still Play a Role?

Bradley S. Trinkle[1], Merrill Warkentin[2], Kalana Malimage[3], Nirmalee Raddatz[4]

[1]Mississippi State University, USA, brad.trinkle@msstate.edu
[2]Mississippi State University, USA, m.warkentin@msstate.edu
[3]Florida Gulf Coast University, USA, kmalimage@fgcu.edu
[4] University of Memphis, USA, nraddatz@memphis.edu

Abstract

Extant research has shown that neutralization processes can enable potential IS security policy violators to justify their behavior and overcome the deterrence effect of sanctions in order to engage in unethical behaviors. However, such sanctions are typically moderate and not career ending. We test the boundary conditions of this theory by evaluating whether neutralization plays a role in overcoming the impact of extreme levels of deterrence. We extend the Siponen and Vance (2010) framework within a professional context that assigns extreme sanctions to violators. Using the scenario-based factorial survey method common in IS security research, we collected data from future auditors who understand these extreme sanctions. We test the reasons that auditors may use to form intentions to falsify information concerning an information security issue with a company's accounting information system, thereby jeopardizing data integrity and security by modifying working papers to hide irregularities and, by doing so, violating their professional standards, which could result in career-ending sanctions. We empirically validated and tested the theoretical model. Our results show that sanctions play an important role in reducing employees' intentions to violate policy but that, even under extreme boundary conditions, employees might seek to rationalize their unethical behavior by denying responsibility for their actions through, for example, arguing that their supervisors pressured them into performing the violations. We also establish that messages heightening the awareness and perceptions of the certainty and severity of organizational punishment are likely to attenuate such deviant behaviors. We discuss the implications of these findings and suggest future avenues for research.

Keywords: Deterrence Theory, Security, Neutralization, Compliance, Ethics, Theory Contextualization, Boundary Conditions

Fred Niederman was the accepting senior editor. This research article was submitted on June 30, 2017 and underwent three revisions.

1 Introduction

The literature on violations of organizational information security policy has evaluated violations that may invoke a managerial sanction (punishment), which is presented as having a deterrent effect. However, this rich body of literature has evaluated situations in which the punishment was measured and not extreme. We seek to extend and amplify the findings of Siponen and Vance (2010) by testing the application of their theory regarding the impacts of neutralization and deterrence on employee intentions to violate policies under broader boundary conditions. In accordance with Whetten's (1989) suggestion that theory is strengthened when conditions that may restrict the breadth of current theoretical understanding are better understood, we use the context of violations

of auditor rules to explore whether the findings regarding the deterrent effect of sanctions also apply when the sanction threat is an extreme, potentially career-ending punishment.

The former Wall Street darling Enron Corporation offers a prime example of auditor rule violations; in this case, the audit firm and the client organization colluded to commit financial fraud. Established in 1985, Enron was once a corporate giant in the energy and gas industry and one of the largest companies in the United States. With its demise in December 2001, Enron's auditor, Arthur Andersen & Company, was subjected to considerable scrutiny for validating Enron's fraudulent books (Abelson & Glater, 2002). As a result, considerable debate regarding auditor independence has emerged in the accounting and auditing literature (Bazerman et al., 2002).

Prior to the enactment of the Sarbanes-Oxley (SOX) Act of 2002, auditors relied far more on consulting revenue generated from clients than revenue generated from audits themselves. In the case of Arthur Andersen, more than half of the $52 million in fees received from Enron was attributable to consulting services rather than regular audit fees (Abelson & Glater 2002), suggesting that an auditor might be tempted to simply ignore fraudulent bookkeeping found with a major client. Indeed, as Abelson and Glater (2002, p. 1) point out: "There's no way that you could have a client which is that huge and important to you and not be tempted to turn your head away from problems."

While the current post-SOX regulations prohibit auditors from providing consulting services to their clients, auditors remain motivated to maintain the good graces of their clients because their clients have the power to fire them at any time during an audit. Although ignoring a client's fraudulent bookkeeping activities and returning favorable results can subject an auditor to severe penalties, auditors might be conflicted as to whether they should offer clients favorable results in order to retain the clients. Thus, even under the threat of severe sanctions, auditors might seek to rationalize the practice of overlooking certain irregularities or financial misstatements discovered during an audit.

In the present study, we extend and amplify the findings of Siponen and Vance (2010) by testing the application of their theory elucidating the impacts of neutralization and deterrence on employee intentions to violate policies under broader boundary conditions. Siponen and Vance offer an explanation for how employees rationalize their failure to comply with information systems security policies, a major concern for information technology security managers. They propose a theoretical model, based on criminology's deterrence theory, that highlights the role of "techniques of neutralization" used by potential violators to overcome the impact of organizational sanctions. Such techniques "provide a temporary release from their conventional restraints, including formal and informal sanctions" (Akers & Sellers 2004, p. 488), thereby neutralizing feelings of guilt or shame by enabling potential offenders to justify or rationalize their actions. Matza (1964) calls this temporary release "drift"—"an episodic relief from moral restraint" (Maruna & Copes 2005, p. 231). Siponen and Vance's empirical findings show that various techniques of neutralization are directly associated with employee intentions to violate IS security policy; they work in tandem with the direct impacts of both formal and informal sanctions identified in other research.

Subsequently, D'Arcy and Herath (2011) have called for more work on deterrence and suggest taking a cue from criminologists and refining deterrence theory by testing "the conditions under which the threat of sanctions is likely to influence behavior" (p. 655) using various situational variables. Willison and Warkentin (2013) also call for more research to understand the roles of neutralization and deterrence in the information security context. They suggest that researchers should study neutralization in relation to specific forms of computer abuse and their influence on the effectiveness of deterrence, especially at the margins of our current understanding of this phenomenon. Barlow et al. (2013) call for more research into the role of neutralization by "extreme policy breakers" whose decision factors may fall outside the "normal" range. Accordingly, we ask: *Do employees who face extreme sanctions yet still violate security policies also use techniques of neutralization to justify their decisions?*

Johns (2006) and other scholars have recently called for greater scrutiny of theorization and theory contextualization in an effort to improve the sophistication, value, and applicability of our theoretical lenses. Salovaara and Merikivi (2015) suggest that reexamining published studies to verify or extend their findings offers the opportunity to increase the knowledge of the *boundary conditions* of existing theories and strengthen the research community by accelerating the exchange of interaction between researchers. Whetten (1989) describes boundary conditions as functions that "place limitations on the propositions generated from a theoretical model. These temporal and contextual factors set the boundaries of generalizability, and as such constitute the range of the theory" (p. 492). Boundary conditions should be tested to ensure that theories apply to broader contexts. In several key articles in the *Journal of the Association for Information Systems*, leading IS scholars have urged us to pursue this process: Weber (2012) states that theories must circumscribe the boundary or domain of a theory, i.e, "the phenomena it is intended

to cover." (p. 6). Citing Gray and Cooper (2010, p. 627), Weber adds that "some scholars argue that a field's understanding of the boundary conditions associated with its theories is a good proxy for the quality of its theories and the state of the field more generally (Weber, 2012, p. 6). Indeed, Kohli and Grover (2008, p. 1) maintain that "it is important to set the boundary conditions" for IS research domains. Furthermore, Grover (2012) reports that IS research must "develop clear boundary conditions" (p. 262) and suggests that researchers should "enforce definitional boundary conditions" in their work (p. 266). Seddon and Scheepers (2012, 2015) reiterate these research guidelines and argue that extant works should be tested for the refinement of boundary conditions. Whetten et al. (2009) explicate how theory contextualization, or the extent to which a theory explicitly accounts for relevant contextual conditions, enables scholars to provide a theoretical contribution. We test the boundary conditions for the theoretical lenses of neutralization theory and deterrence theory in the context of auditor rule violations in which potential violators clearly understand the extreme magnitude of the sanction associated with the ethical violation: suspension or loss of their license to practice.

Although previous InfoSec studies focusing on information security policy violations have not directly discussed whether policy violations are ethical or not, they imply that policy violations are unethical through the use of scenario-based methods. Siponen and Vance (2010) justify the use of scenario-based methodology because it "offer[s] an indirect way of measuring intention to commit unethical behavior," and it "can incorporate situational details thought to be important in decisions to behave unethically" (pg. 492). Siponen and Vance also identify issues related to policy violations, such as software piracy and computer abuse, as unethical. D'Arcy et al. (2009) do not discuss ethics specifically but identify security policy violation behaviors such as personal use of company email as "unethical and/or inappropriate" (p. 82).

Most of the recent InfoSec studies that have tested deterrence (D'Arcy & Hovav, 2007; Herath & Rao, 2009; Higgins et al., 2005; Kankanhalli et al., 2003; Li et al., 2010; Pahnila et al., 2007; Siponen et al., 2007; Zhang et al., 2009) focus on policy violations rather than on the ethics of acts of security policy noncompliance. D'Arcy and Herath (2011) discuss "moral beliefs," which refer to the "extent to which one perceives an illicit act to be morally offensive" (p. 646), instead of a complete ethical system. This seems appropriate, given that determining what is ethical or not can be based on a subjective individual judgment. Relevant to this paper, auditors hold special responsibility, and they are bound by a code of professional conduct that is enforced by the AICPA's Professional Ethics Executive Committee (PEEC). Furthermore, Siponen and Vance (2010) tested a binary (comply or not comply) decision at relatively low levels of perceived cost and benefit to the potential policy violator. The rationalization allowed regular workers to engage in minor violations when the payoff was not particularly great.

For "run-of-the-mill" common behaviors, the extant literature has done a tremendous job of researching deterrence related to IS behaviors in terms of policy violations. Certainly, the threat of prison sentences may also be a potent deterrent of violation intentions. However, in the context of auditors conducting an IS audit, committing fraudulent acts that may result in losing their CPA license and subsequently their ability to practice their chosen profession is not a run-of-the-mill behavior with a run-of-the-mill punishment. Thus, the experimentally manipulated scenario presented in our research design places the participants in a situation that enables testing of the boundary conditions of the relevant theories and thereby contributes to the extant literature. We test boundary conditions by testing the efficacy of the extant theory under extreme levels of perceived formal organizational sanctions. Therefore, we selected a sample comprised of individuals who understand that, if they are caught, the sanction for engaging in the violation of professional certification standards described would likely result in the termination of their careers.

We seek to extend and strengthen the applicability of the Siponen and Vance (2010) framework, as it applies to policy violation behaviors and test the boundary conditions of extant applications of this theory. Specifically, we seek to contribute to the debate on the role of neutralization as an influence on the security decisions of employees by testing why auditors form the intention to (1) violate their professional standards (which could result in career-ending sanctions), (2) violate policy by altering strategic data by modifying working papers to hide irregularities and (3) thereby jeopardize the integrity and security of strategic corporate information.

1.1 Internal Data Integrity Threats

Firms must maintain the security of their systems by protecting data against external and internal threats to data integrity, but internal threats to data integrity represent the greatest challenge. Unethical auditing behavior represents a significant and pernicious internal attack on data integrity. Auditors are stewards and curators of strategic information and hold a special responsibility in this context. The goal of managing information security is to ensure the confidentiality, integrity, and availability—traditionally called the CIA triad—of valuable information assets that may be strategic, protected, sensitive, or proprietary (Anderson, 2003; Parker, 1998). Corporate fraud, including

unethical auditing behavior, creates significant costs for businesses, and incidents have been increasing. (For a thorough explanation of the corporate fraud violation environment, please see Appendix A.)

We draw on neutralization theory and deterrence theory, which are prominent in the criminology literature, to focus on identifying the antecedents of auditors' behavioral intentions to violate policy by altering evidence regarding an information security issue involving the accounting information system. Specifically, we contextualize the contributions of Siponen and Vance (2010) in our research and test the boundary conditions of their theory. The remainder of this paper is structured as follows. First, we summarize the extant literature on internal control deficiencies, fraud, and auditor standards. Next, we identify relevant gaps in the literature and develop a theoretical model based on well-established prominent theories in criminology regarding deviant behavior. We then discuss the research method and results of the hypothesis testing. Finally, we conclude the paper by discussing our findings, their implications on theory and practice, and future research directions.

2 Research Motivation and Theoretical Background

Insider information is a strategic resource that must be protected (Renaud et al., 2019). Extensive evidence indicates that insider threats, including information alteration and theft, represent a significant organizational problem that is difficult to address (Barlow et al., 2018; Ho & Warkentin, 2017; Kaspersky, 2015; Kim et al., 2019; Ormond et al., 2019; PricewaterhouseCoopers 2014; Willison et al., 2018). Though any insider is capable of nonmalicious deviant behavior (Guo et al., 2011), the greatest damage generally results when a critical member of an organization behaves against the interests of that organization in an illegal and/or unethical manner (Warkentin & Willison 2009). The term "insider" refers to employees, contractors, or other stakeholders who have (1) legitimate access to the facilities and information systems of the organization, and (2) intimate knowledge of internal organizational processes that may allow them to exploit weaknesses (Willison & Warkentin 2013). Additionally, certain privileged insiders have greater access to strategic information and greater knowledge of key business processes (Sharma & Warkentin, 2019), which may exhibit flaws in the organizational process control for protecting information assets (Butler, 2012). Because trusted insiders can potentially expose the organization to a great deal of potential harm, they pose a significant threat.

Management is responsible for designing and implementing internal controls capable of reducing or eliminating the threats posed by insiders. Internal controls are defined as "a process—effected by those charged with governance, management, and other personnel—designed to provide reasonable assurance about the achievement of the entity's objectives with regard to the reliability of financial reporting, effectiveness and efficiency of operations, and compliance with applicable laws and regulations" (AICPA 2009, p. 1843). According to the AICPA SAS No. 115, a deficiency exists when the design or operation of a control does not allow management or employees to prevent, or detect and correct misstatements or fraud on a timely basis while performing their assigned functions. Deficiencies can be deemed material weaknesses or significant deficiencies and auditors should evaluate the severity of each deficiency identified during an audit.

Audit firms are engaged to perform information systems audits, which are intended "to review and evaluate internal controls that protect the system." (Romney & Steinbart 2015, p. 315) If any significant deficiencies or material weaknesses related to internal controls in the information system are identified, the auditor is required to communicate that in writing to management and to those charged with governance as part of the audit. If the deficiencies are not significant deficiencies or material weaknesses and the auditor decides to properly communicate this information to management, this communication must be documented (AICPA 2009). Intentionally failing to report significant deficiencies or material weakness in the internal controls of the information system by modifying audit working papers and thus producing an inaccurate audit report is fraud and can make the organization vulnerable to the threats to the information system that remain uncontrolled. The Office of the Inspector General of Idaho has shown that the following weaknesses are considered high impact and may lead to increased vulnerabilities in organizational information systems: inadequacies in the logical access security controls, physical access controls, network security, and security control policies and procedures (Salmon, 2014).

Employees who violate policies by failing to comply with established information reporting standards may be motivated by various root causes. Greed, revenge, or managerial pressures may motivate noncompliance. Employees may engage in noncompliant policy workarounds motivated by positive goals or may lack a clear understanding of policies and standards. Auditing standards represent an exception to "understandable" violations that may sometimes be excused because the violation of the auditing standards described here is always an ethical breach that can result in career-ending (maximum) sanctions. (For an in-depth assessment of the motivation and consequences of security policy violation behavior, see

Willison and Warkentin, 2013.) The extended security action cycle (Willison & Warkentin, 2013) suggests that employees may progress from the motivation stage to the formation of behavioral intentions to commit computer abuse (deviance behavior and unethical act) in a cognitive process explained by various theories—in our case, deterrence theory and neutralization theory.

Neutralization theory and deterrence theory form the foundation of this investigation and inform our theoretical model, which is shown in Figure 1. The model shows how auditor behavioral intentions to violate policy by altering evidence concerning an information security issue with the accounting information system are directly influenced by neutralization, perceived sanctions, and the degree of violation. Neutralization theory suggests that individuals apply techniques of neutralization to justify unethical behavior. Deterrence theory suggests that, in the presence of negative sanctions or punishments, individuals are less likely to commit deviant behavior or violate policy. We argue that the degree of violation, i.e., whether the individual removes or modifies the deficiencies in working papers, influences behavioral intentions to violate policy.

2.1 Theory of Neutralization

Sykes and Matza (1957) originally proposed that criminal offenders often use justifications in rationalizing their deviant behavior, thereby enabling them to violate social norms without being deterred by feelings of guilt or shame. This process is basically a mechanism whereby the potential offender neutralizes behavioral norms, making them inoperative, and frees him- or herself to engage in deviant behavior without feeling that it is actually wrong (Rogers & Buffalo, 1974). Sykes and Matza (1957) proposed five techniques of neutralization that enable offenders to engage in deviant acts or behaviors that violate social norms: (1) denial of the victim, (2) condemnation of the condemners, (3) appeal to higher loyalties, (4) denial of responsibility, and (5) denial of injury. Additional techniques of neutralization were later presented by other scholars, such as the metaphor of the ledger (Klockars, 1976), defense of necessity (Minor, 1981), and denial of the necessity of the law (Coleman, 1985). For a thorough discussion of neutralization theory in the context of information systems security, see Willison and Warkentin (2013).

Social norms are presumed to be the grammar of social interactions, which acts as a set of rules and guidelines to determine what is acceptable and what is not in a society (Bicchieri, 2005). When an individual disrupts these social norms by engaging in deviant behavior, neutralization techniques will provide the individual with the freedom to momentarily suspend the obligation to uphold social norms. However, this rationalization does not necessarily entail a rejection of the commonly accepted social norms but rather an acceptance of the norms and a subsequent justification of them in order to engage in the deviant behavior (Eliason & Dodder 1999). In the current study, the social norms of ethical behavior in the auditing profession (e.g., exercising due care, following company policies, adhering to applicable rules and regulations, etc.) are set forth in codes of conduct in accounting firms, state accounting boards, the American Institute of Certified Public Accountants, and other governing bodies of the accounting profession.

Techniques of neutralization have proven to be a powerful lens for understanding individual intentions to violate societal norms or organizationally sanctioned actions in many contexts. Eliason and Dodder (1999) investigated the techniques of neutralization used by deer poachers to justify their hunting activities. Although neutralization techniques, in general, were found to have a significant impact on the justification of these activities, denial of responsibility, the metaphor of the ledger, the defense of necessity, and the condemnation of the condemners were found to be the most common justifications used by the deer poachers. Additionally, Brennan (1974) studied the techniques of neutralization used by individuals who receive abortions, and Priest and McGrath (1970) investigated how the techniques of neutralization are used by young adult marijuana smokers. Brennan (1974) found that individuals use some techniques of neutralization, such as denial of responsibility, condemnation of the condemners, and appeals to higher loyalties to rationalize getting an abortion and to prevent associated guilt, anxiety, or depression. Alvarez (1997) also applied techniques of neutralization to explain why individuals cooperated with group acts of genocide.

Dunford and Kunz (1973) used some of the techniques of neutralization as a lens to explain the reduction of dissonance within a religious community. Empirical tests of neutralization theory as an antecedent of actual criminal behavior have yielded mixed results because the theory is often understood as a means to determine the etiology of the mental state of criminal defendants (Maruna & Copes 2005), which presumably led them to commit crimes. According to Maruna and Copes, (2005), neutralization theory and the rationalization techniques used by offenders should be viewed as contributing to the persistence or cessation of a crime rather than as a theory of criminal etiology because offenders cannot neutralize their actions prior to committing crimes. As stated by Sykes and Matza (1957), "it is by learning these techniques that the juvenile becomes delinquent" (p. 667).

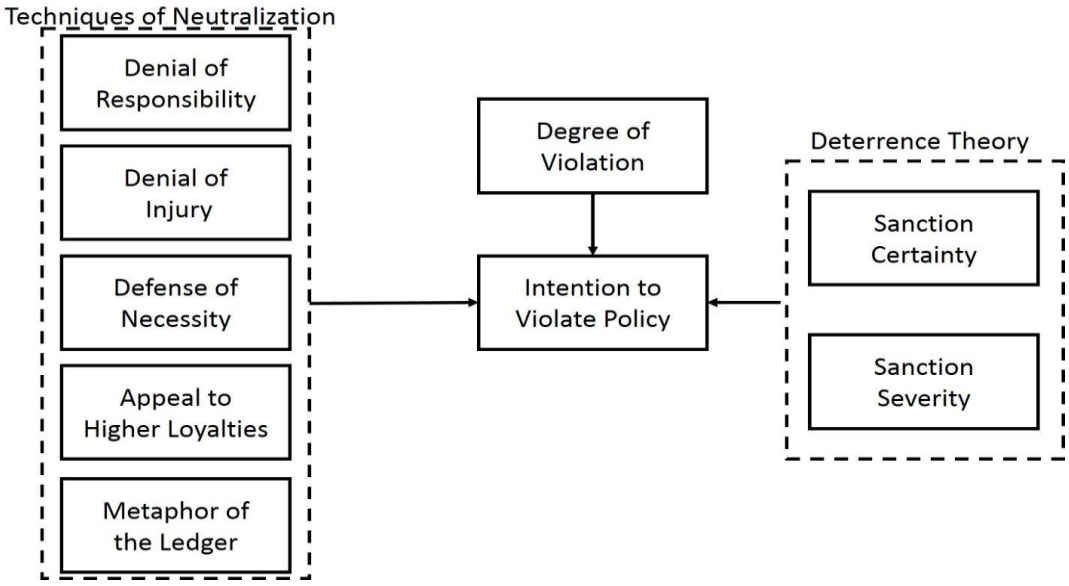

Figure 1. Conceptual Model

But in a recent review of the theory, Copes and Deitzer (2015) conclude that, when applied to various specific acts of deviance, the theory is widely accepted as a result of empirical validation as either a direct antecedent of social deviance (norm violation) or as a positive moderator of other impacts on deviance (Hinduja, 2007; Smallridge & Roberts, 2013). Recent advancements have demonstrated the efficacy of this theory in understanding how neutralization use by offenders is differentiated by situational factors (Copes & Deitzer, 2015), which is our goal. The breadth of empirical support for the role of these methods of justifying rule-breaking behaviors establishes this as a solid foundation for the context of our focal phenomenon. Accordingly, Willison and Warkentin (2013) call for further applications of this theoretical tool as a means of investigating organizational security policy violation intentions.

Siponen and Vance (2010) empirically evaluated how employees justify their computer security policy violation behavior by utilizing six neutralization techniques: defense of necessity, appeal to higher loyalties, condemn the condemners, metaphor of the ledger, denial of injury, and denial of responsibility, along with the formal and informal sanctions. Their results reveal that techniques of neutralization exert a significant impact on an employee's intention to violate organizational security policies. Barlow et al. (2013) also show that employees suppress their ethical instincts to comply with information security policies by cognitively applying these techniques of neutralization. (Willison & Warkentin, 2013) also found that neutralization plays a role in overcoming guilt and shame, thus enabling individuals to form intentions to violate information system security policy, a type of workplace deviance. Barlow et al. (2018) investigated whether various types of organizational communication could dissuade employees from using neutralization techniques to justify their deviant policy violations. Their results indicate that security communications and training centered on neutralization techniques are effective methods that organizations can use to minimize employee policy violations. Finally, Willison et al. (2018) tested both deterrence and neutralization as modifiers of the relationship between perceptions of organizational injustice and the intention to commit computer abuse. The study results indicate that neutralization through the denial of the victim and the metaphor of the ledger positively moderate the relationship between perceptions of procedural, organizational injustice and the intention to commit computer abuse.

Because each neutralization technique is unique, previous research projects have carefully and logically assessed each technique within the context of the focal phenomenon of violation and violators. This is typically accomplished by empirically testing the relevant techniques to determine whether each technique may individually prove to be a source of variance in the intention to commit deviant behavior. Because our focal phenomenon was the working professional who contemplates committing an egregious career-ending violation, we selected a specific situation in which employees are faced with extreme sanctions for violations. Subsequently, we carefully read the literature on audit fraud and consulted with both auditors and educators to assess the possible role of each neutralization technique within the auditor fraud context to select the most likely ones for further investigation. Collectively, the sources indicated that the following five neutralization

techniques fit the context of our study: denial of responsibility, denial of injury, appeal to higher loyalties (Sykes & Matza 1957), defense of necessity (Minor 1981), and metaphor of the ledger (Klockars 1976). Potential uses of each neutralization technique proposed by the auditors and/or educators are included in the development of the first five hypotheses. The following section introduces these neutralization techniques as theoretical foundations of our research hypotheses.

2.1.1 Denial of Responsibility

When using denial of responsibility, individuals justify their actions by stating that they were a victim of the occurrence and therefore lack responsibility for their actions. Moreover, individuals justify their actions by simply stating that it was not their fault and they were forced into the situation (Sykes & Matza, 1957). An auditor, for example, may reason that since a supervisor told him or her to perform a particular action (e.g., reporting a number of billable hours that differ from those hours actually worked on a particular job), the supervisor is responsible for the action, thus absolving the auditor of the responsibility. In the context of IS security, Siponen and Vance (2010) found that denial of responsibility has a significant positive influence on an employee's intention to violate company security policies. Furthermore, Harrington (1996) found that denial of responsibility has a significant impact on information system employees' computer abuse intentions and judgments. Therefore, based on these considerations, we hypothesize:

H1: Auditors using denial of responsibility are more likely to form behavioral intentions to violate policy.

2.1.2 Denial of Injury

When using denial of injury, the individual justifies actions by reasoning that the actions did not cause any real harm or damage and the victim can afford any harm done (Sykes & Matza 1957). For example, a shoplifter in a large retailer may rationalize an action because the retailer can handle the loss. A nurse may violate a hospital's privacy policy by reading a celebrity's medical chart, but if it is motivated only by curiosity and no data are distributed (no breach), then no tangible harm is experienced and the nurse may neutralize the policy violation in this manner. An auditor may rationalize reporting fewer billable hours than actually worked because the client's bill will be lower and the auditing firm will likely retain the client's services in the future because of the auditor's perceived efficiency. Similarly, computer criminals may justify their actions by claiming that they are just hacking hardware and are not causing any harm to individuals, or workers may feel that they can skip security procedures if they feel that the steps are unnecessary. In the context of IS security, Siponen and Vance (2010) have found denial of injury to have a significant impact on employee intentions to violate information security policies. Therefore, based on these considerations, we hypothesize:

H2: Auditors using denial of injury are more likely to form behavioral intentions to violate policy.

2.1.3 Defense of Necessity

When using defense of necessity, the offender justifies that rule-breaking is necessary and that there is no reason to feel guilty about the action (Minor, 1981). Starving individuals steal food to survive. The healthcare literature often cites examples of how medical caregivers employ various workarounds in order to provide timely and effective patient care, even if these workarounds violate security policies. Koppel et al., (2012) offer the example of a nurse charged with matching the barcode on the patient's wrist (which calls for a 10m dose) with the barcode on medications dispensed by the hospital pharmacy (which filled the prescription with two separate 5mg doses). The barcodes do not match, generating an error code requiring a time-consuming report. However, to provide the dose and move on to the next patient, the nurse proceeds to violate a security procedure in the interest of time. Puhakainen (2006) reports that employees claim they must ignore policies to meet deadlines. For example, an employee may argue that it is necessary to share a password with a coworker in certain circumstances in order to perform job duties. Barlow et al. (2018) give the example of an employee who gets an urgent call from a coworker facing a deadline who needs information saved on the hard drive of an office computer with no remote access; thus, the caller shares the password needed to access the information for the report. An auditor may rationalize that reporting a lower number of billable hours than actually worked because is necessary to ensure that the audit team stays on budget. In the context of IS security, Siponen and Vance (2010) found that the defense of necessity positively correlates with the intention to violate company security policies. Therefore, based on these considerations, we hypothesize:

H3: Auditors using the defense of necessity are more likely to form behavioral intentions to violate policy.

2.1.4 Appeal to Higher Loyalties

When using the technique of appeal to higher loyalties, the violator justifies the offense by advocating that it is for the greater good of society (Sykes & Matza 1957). More specifically, an individual might sacrifice the demands or the social norms of the larger society in favor of a smaller social group, such as a gang, family, or a circle of friends. For example, individuals might

argue that it is necessary to steal money in order to feed one's family. LaBeff et al. (1990) investigated how students who cheat have used neutralization techniques to suppress the guilt. Their results suggest that students appeal to higher loyalties by simply stating that helping friends matters more than not cheating. Auditors might rationalize reporting a lower number of billable hours than actually worked in order to help their supervisors manage efficient teams. In the IS security context, Siponen and Vance (2010) found that the appeal to higher loyalties has a significant influence on an employee's intention to violate the company security policy. Therefore, based on these considerations, we hypothesize:

H4: Auditors using the appeal to higher loyalties are more likely to form behavioral intentions to violate policy.

2.1.5 Metaphor of the Ledger

This particular neutralization technique works by balancing certain good acts with bad acts. Klockars (1976) suggests that when individuals believe they have performed enough good deeds to compensate for one or two bad deeds, they may engage in deviant behaviors without guilt. In such situations, individuals might focus on the criminal act itself as compensation for good deeds previously performed (Piquero et al., 2005). Willison et al. (2018) discuss an employee who felt he had been such a model employee for so long that it would be alright to violate the computer security policy (stealing his boss's password to see everyone's raises) just one time. An auditor may rationalize reporting a lower number of billable hours than actually worked since the extra work performed resulted in the discovery of an error that, when corrected, resulted in the financial statements being reported in accordance with generally accepted accounting principles. In the context of IS security, Siponen and Vance (2010) found that the metaphor of the ledger has a significant positive effect on employees' intentions to violate company security policies. Another study conducted by Hollinger (1991) examined the effect of the metaphor of the ledger along with three other neutralization techniques in production deviance and workplace theft. Their results revealed a positive correlation between the metaphor of the ledger and production deviance. Therefore, based on these considerations, we hypothesize:

H5: Auditors using the metaphor of the ledger are more likely to form behavioral intentions to violate policy.

2.2 Deterrence Theory

Deterrence theory suggests that employees rationally violate policies if the perceived benefits outweigh the risks. This cognitive appraisal process results in reduced motivation to engage in rule-breaking behavior if individuals believe that the risk of getting caught is high (certainty of sanctions), that severe penalties will be applied if they are caught (severity of sanctions), and/or that punishment will be swift (celerity of sanctions). In the deterrence literature, studies utilizing sanction celerity have produced inconclusive results (Nagin & Pogarsky, 2001); further, they have found sanction certainty to be more effective in deterring deviant behavior than sanction severity or sanction celerity (Pogarsky, 2002). Nagin and Pogarsky (2001) further establish this notion by indicating that the theory "does not concern a 'connection' between behavior and consequences, but rather whether potential consequences already recognized by the decision-maker seem sufficiently 'costly' to deter behavior" (p. 867). Echoing this, Raddatz et al. (2020) found that sanction severity and sanction certainty have the strongest influence on computer usage policy compliance intentions, whereas the authors did not find that sanction celerity had any influence. Similarly, Nagin and Pogarsky (2001) found that sanction celerity did not have an impact on deterring drunk driving.

This referent theory has been widely applied in information security research, especially in terms of the roles of perceived sanction severity and certainty (D'Arcy & Herath, 2011). Straub and Nance (1990) suggest that the detection and punishment of violators can minimize computer abuse. Similarly, Straub (1990) found that the use of information security deterrents results in a decreased incidence of computer abuse. Straub and Welke (1998) implemented an action research study in which they highlight the importance of communicating the certainty and severity of sanctions as a part of insider education and training programs in order to minimize security violations. Kankanhalli et al. (2003) investigated the use of sanctions to enhance information security and found that deterrents lead to the improved effectiveness of information security.

Straub et al. (1993) further applied deterrence theory in a field experiment and concluded that communicating sanctions to employees can reduce the likelihood of insider information security violations. Harrington (1996) found that codes of ethics, a type of formal sanction applied to the organization generically, do not affect insiders' judgments or intentions to commit computer abuse. However, generic codes of ethics were found to affect insiders that ranked high in the denial of responsibility, which is a form of rationalization. Similarly, IS-specific codes of ethics did not affect judgment or intentions, except in the case of computer sabotage, which is a severe type of computer abuse. Thus, the effects of codes of ethics were found to be "sporadic and weak" (Harrington, 1996, p. 273). D'Arcy et al. (2009) found that IS security policies, awareness programs, and

computer monitoring influence the perceived severity of formal sanctions, which leads to the reduced intention to misuse IS. In their study, the certainty of formal sanctions did not have any effect on intentions to misuse IS. However, Siponen et al. (2007) applied both formal and informal sanctions to explain insiders' compliance with information security policy and found that both forms of sanctions predict insiders' compliance with IS security policies. D'Arcy and Devaraj (2012) later found that both forms of sanctions have direct and indirect influence on the intentions to misuse technology. Thus, although the results of previous studies are mixed and opinions are diverse regarding the definitive role of sanctions on information security compliance intentions and behaviors (D'Arcy & Herath, 2011), the overall research stream supports the adaptation of deterrence theory from criminology to the information systems context.

Several information security researchers have used deterrence theory to predict deviant and conforming user behavior in the IS security context (D'Arcy & Herath, 2011; D'Arcy & Hovav, 2007; D'Arcy et al., 2009; Peace et al., 2003; Siponen & Vance, 2010). However, the relationships between the correlations of sanction severity and certainty toward behavioral intentions are not consistent among the studies. For example, Peace et al. (2003) found sanction certainty and severity to have a significant impact on the individual's attitude toward software piracy, whereas D'Arcy et al. (2009) found that sanction severity has a significant impact on reducing IS misuse intentions but sanction certainty's impact is insignificant.

Furthermore, Herath and Rao (2009) used protection motivation theory and deterrence theory to investigate employee security policy compliance and found the certainty of detection has a positive impact, whereas the severity of penalty has a negative impact on security policy compliance intentions. Because of the inconsistent nature of the findings based on deterrence theory and the lack of studies conducted in information security research on auditor standards violations, we used two major components of deterrence theory in our research to test the antecedents of unethical auditor behavior resulting in policy violations: *sanction severity* and *sanction certainty*. Based on these research findings on the application of deterrence theory, we hypothesize:

H6: When faced with high sanction severity, auditors are less likely to form behavioral intentions to violate policy.

H7: When faced with high sanction certainty, auditors are less likely to form behavioral intentions to violate policy.

2.3 Degree of Violation

If an external auditor finds that significant weaknesses exist in internal controls during the course of fieldwork, the auditor is required to include those weaknesses in the working papers. However, an audit supervisor may ask the auditor to remove the deficiencies from the working papers or minimize the references to the control deficiencies for various reasons. First and foremost, under the current external audit recruitment system, the client organization has the full authority to hire and fire the auditors that they recruit to audit their financial statements. Under this commonly accepted method, it has become a well-known practice for organizations to fire external auditing firms that deliver unfavorable audits. Thus, auditors are highly motivated to remain in the client's good graces by delivering favorable results. Second, an external auditor's future career may depend on the potential success with a current client organization, which further increases the motivation to provide favorable audit results (Bazerman et al. 2002). However, to the extent that more extreme sanctions are more commonly present for violations of auditing standards, auditors might be torn between violating auditor standards to some degree in order to deliver favorable results to their clients and avoid potential punishment.

For the context of this study, we investigate what an auditor conducting fieldwork would do if a supervisor asked the auditor to make modifications to the internal control deficiencies reported in the working papers. An auditor likely perceives different degrees of violation intensity, based on whether the auditor is asked to remove deficiencies or merely minimize them, which likely influences the auditor's intention to violate policy. Thus, when faced with the decision to modify internal control deficiencies reported in working papers, an auditor may weigh the costs and benefits of such a violation. Because of the severe sanctions associated with an auditor's failure to comply with the Generally Accepted Auditing Standards along with the internal pressure to retain clients through rendering favorable audit results, an auditor may resort to performing the lesser violation. Hence, when faced with more serious violations that could result in career-ending consequences, auditors may be less likely to form the behavioral intentions to violate policy. Therefore, we hypothesize:

H8: When faced with a high degree of violation intensity, auditors are less likely to form behavioral intentions to violate policy.

2.4 The Techniques of Neutralization and Deterrence Effects

While deterrence through sanctions is effective in mitigating or eliminating deviant behavior, techniques of neutralization allow offenders to minimize feelings

of guilt or shame by rationalizing their actions. In the context of information security research, scholars have utilized deterrence theory as a means to explain an individual's intention to violate information security-related policies. However, even in the presence of severe sanctions, individuals may engage in deviant behavior, such as violating organizational policies. The theory of neutralization from the field of criminology presents "techniques of neutralization" used by potential violators to overcome the impact of organizational sanctions proposed by deterrence theory. Extant literature in the field of information security has explored the impact of deterrence and neutralization through investigating the intention to violate IS security policy (Barlow et al., 2013; Siponen & Vance, 2010), intention to use shadow IT (Silic et al., 2017), and employee computer abuse (Willison et al., 2018).

Siponen and Vance (2010) explored the impact of deterrence in the specific form of formal and informal sanctions along with six neutralization techniques (defense of necessity, appeal to higher loyalties, condemnation of the condemners, metaphor of the ledger, denial of injury, and denial of responsibility) and their impact on intention to violate IS security policy. Their results indicate that both formal and informal sanctions have an insignificant influence in the presence of neutralization. These findings can be attributed to the fact that, when the severity of punishment for policy violations is not severe enough to deter employees, employees may easily rationalize their guilt, shame, and all other components of sanctions through neutralization techniques.

In a similar vein, Willison et al. (2018) explored the impact of distributive and procedural justice on computer abuse and the effect of formal sanctions, as well as techniques of neutralization and their moderating effects on the relationship between organizational justice and intentions to abuse computers. Their findings indicate that procedural justice influences abuse intentions and that sanction certainty and techniques of neutralization moderate this influence. Thus, it can be inferred that the influence of sanctions and neutralization may be context-dependent, whereas the successful implementation of sanctions is highly dependent on factors such as the organization's ability to enforce punishments with certainty, employees' awareness of such punishments, and the seriousness of the violation under consideration.

In the context of our study, given that auditors belong to a special category of employees who are required to abide by various rules and regulations such as the Generally Accepted Auditing Standards, the Statements on Auditing Standards, and the AICPA Code of Professional Conduct, the same organizational interventions (e.g., sanctions) and the same neutralization techniques may or may not be similarly effective. Furthermore, because of the more extreme sanctions faced by auditors, they may or may not rationalize their actions through the use of neutralization techniques. Therefore, this study seeks to contribute to the existing information security literature by testing the impact of sanctions and neutralization.

3 Method

Insiders who abuse their information access privileges must be identified, but the research instruments for adequate insider threat research data collection and measurement are unfortunately limited and largely ineffective (Crossler et al., 2013; Warkentin, Straub et al., 2012). This lack of effective mechanisms and data for studying the insider threat phenomenon undermines the ability to defend organizational assets against internal perpetrators. For our study, we used a widely used scientific technique known as the scenario-based factorial survey method, which has been employed by criminologists (Jasso, 2006; Taylor, 2006) and information security researchers (Barlow et al., 2013; Barlow et al., 2018; Johnston et al., 2016; Trinkle et al., 2014; Vance et al., 2013; Vance et al., 2015; Willison et al., 2018), to collect data for our investigation. Scenario-based methods are a common means of assessing behaviors that are antisocial and/or ethical/unethical in nature (Siponen & Vance, 2010) because of their ability to elicit forthright responses from study participants who might otherwise feel vulnerable to potential retribution for honestly disclosing their actions. By asking respondents to read a scenario and imagine themselves in the context of the scenario's character, the researcher can establish a reliable and valid measure for behavioral intention as it relates to the various factors found in the scenario, even though the behavior may be socially undesirable.

Factorial survey instruments are scenario-based instruments that randomly provide participants with multiple versions of a realistic scenario that randomly varies the situational information (the tested factors) with the remainder of the scenario being fixed (Taylor, 2006), thus yielding a crossed experimental design (Jasso & Rossi 1977). This technique provides a realistically complex instrument (Lyons, 2008), with approximately orthogonal factors (Lyons, 2008; Rossi & Anderson, 1982), and the details distributed across participants (Trinkle et al., 2014; Warkentin, McBride et al., 2012). This technique combines a variety of aspects used in field surveys with the control and orthogonality offered by experimental design (Jasso, 2006; Rossi & Anderson, 1982). Furthermore, by inviting our participants to put themselves in the role of the scenario character, the factorial survey method enables the collection of norm-violating intentions with little influence of social desirability bias. For our

factorial survey study, participants received three randomly selected unique variations (scenarios) of a vignette that we developed, in which the degree of violation, technique of neutralization, and level of deterrence were manipulated. According to Willison et al (2012, p. 277): "Because of the recommended practice among factorial survey experiments of removing unrealistic, contextually invalid, or logically impossible scenarios from the full population of scenario versions (Jasso 2006), the chance of multicollinearity among predictor variables (dimensions) in a model does not remain zero, but in all likelihood does remain quite small." The development of the instrument, the participant pool, and the independent and dependent variables are discussed in the remainder of this section.

We provided our respondents with a written description of a realistic situation (vignette) in which various factors were manipulated and the scenario character was told to violate policy, which could lead to extreme sanctions, including losing professional certification, thereby ending one's career. Respondents may hesitate to report true intentions in traditional surveys despite the assurance of anonymity. However, when respondents answer from the perspective of a scenario character, the widely adopted research presumption is that social desirability bias (or acquiescence bias) is minimized and respondents are more likely to provide honest answers regarding the vignette. O'Fallon and Butterfield (2005) report that out of 174 ethical decision-making articles in business journals, 55% of these journals employed scenario methods of data collection. As the scenario method has been used to study issues such as information security policy violations (Barlow et al., 2013; Barlow et al., 2018; D'Arcy et al., 2009; Siponen & Vance, 2010), privacy concerns (Malhotra et al., 2004), and media choices (Straub & Karahanna, 1998), we used the scenario method because it is an appropriate way to collect information relating to personal and ethical issues such as those studied in this research.

3.1 Participants

We collected data from an original sample of 121 graduate and undergraduate (senior-level) accounting students at a large university in the southeast United States. Each participant received three randomly selected unique scenarios, yielding 363 possible complete responses.[1] Of the 363 possible cases, 59 were removed from the data set because of incomplete survey responses or failing a manipulation check (from participants who may have skimmed through the instrument), yielding 304 valid response cases from 104 participants. Of the cases that were removed, 45 were incomplete and 14 failed the manipulation check.[2]

We specifically chose accounting students as an appropriate sampling frame for this project for several reasons. Information system auditing is an activity that crosses functional boundaries between IS and auditing. Although the security issues of the accounting information systems in a company are a concern for both IT and accounting, and although both information systems auditors and (internal and external) financial auditors are involved in the audit process, only external auditors are mandated to audit the information system and report on any weaknesses (such as security issues) during the *financial statement audit*. IS students do not typically learn about financial statement audit working papers nor do they learn that modifying them could be a high-sanction violation that could end their career. However, all accounting students in our subject pool absolutely understood that this was an extreme sanction situation. Accounting students are taught in auditing courses (which all participants had previously taken) that altering working papers to remove or minimize significant or material weaknesses discovered during an audit may be considered fraud (significant weaknesses) or an act that discredits the profession (immaterial weaknesses) and may result in the revocation of their license as a certified public accountant by their state board of accountancy. In other words, any scenario we developed that was appropriate for IS students would not have contained this critical element of our investigation—i.e., merely being fired from a job is not as severe as losing one's professional license. Our focal research phenomenon required the perspective of a certified public accountant, as they face extreme sanctions for violations of ethical standards, which is a primary research question of this project.

[1] Random assignment of the scenarios was used to control for any order-effects bias. We use mixed-model analysis to develop the models to test our hypotheses, as mixed-model analysis addresses the lack of independence associated with the use of multiple measures from the same participant (Vance et al., 2013).

[2] The manipulation check, as shown in Appendix C, asked the participants to identify if the supervisor in the scenario told "Joe" (the character they are playing) to remove or modify the references to the control deficiencies regarding the Triple Point AIS package from the working papers. All of the participants in the experiment had at least one auditing course(s)in which learned the significance of the working papers and the possible consequences of altering the working papers. Therefore, they would understand the meaningful differences between removing and minimizing information from the working papers and that altering the working papers may be considered as an act discreditable to the profession, which may lead to a state board of accountancy revoking their CPA license.

The original participant pool consisted of 122 students, of which one declined to participate, resulting in a 99.2% response rate. Each of these students had previously passed multiple courses that included discussion about ethics and in which they were taught that violations like the one described in our scenario could result in them losing their professional certification.

Evidence supports sampling from student populations, in general (Compeau et al., 2012; Gordon et al., 1986). More specifically, prior research has used students in accounting and financial fraud settings and has found them to be acceptable subjects (Betz et al., 1989; Stanga & Turpen, 1991). Frequently, entry-level auditors perform tests of accounting information system controls; therefore, the use of students as a sampling frame is appropriate, as the experimental scenario is in an information systems audit setting.

Graduate students comprised 21.2% (22) of the participants, and 78.8% (82) were undergraduate students. Approximately 32% percent (33) of the participants in the study had internships. Men made up 51% (53) of the participants, and 49% (51) of the participants were women. The majority of the participants were in the age groups of 18-21 (50) and 22-29 (49). The results from testing for differences in responses across the two age groups did not indicate a significant difference in means of the dependent variable (t = 0.995, p-value = 0.32). Therefore, age was not included in the model.

3.2 Expert Review Panel and Pre-Test

Content validity for the scenario, its various manipulations, and the behavioral intent scale was verified via an exhaustive literature review and an expert review panel consisting of subject matter experts and experts in survey instrument design. An expert panel of three experienced accounting researchers examined the experimental material prior to pre-testing. The panel attested to the readability, understandability, and realism of the instrument. We incorporated several of their suggestions into the instrument prior to pre-testing.

To further validate our instrument, a sample of 24 graduate accounting students who had held internships participated in a formal pre-test of the instrument, including the various scenario versions. These participants judged the instrument to be readable, understandable, and realistic with respect to the tasks of an entry-level auditor.

3.3 Instrument

To thoroughly examine the focal phenomenon, we developed an online instrument on www.qualtrics.com to investigate the factors influencing an auditor's behavioral intention to violate policy. The experiment used a factorial survey method design (Rossi & Nock, 1982) with three manipulated factors. The manipulated factors included the degree of violation, techniques of neutralization used, and level of deterrence.

The scenario used in the present study is a modified version of the "Alice and the ABC Company" case, originally developed by Thorne (2000, p. 157). The original version of the case has been successfully used in Ge and Thomas (2008), Earley and Kelly (2004), and Thorne et al. (2003). We modified the case to conform to the style of the factorial survey method and our research questions. Appendix B contains the entire instrument, with a scenario shell, the factors and their manipulations, the dependent variables, and demographic questions. We also present a sample scenario version in Appendix C.

3.4 Variables

3.4.1 Independent Variables

The degree of violation is a bivariate manipulation that asked participants to (1) remove all of the references to control deficiencies regarding the accounting information system from the report, or to (2) minimize the references to control deficiencies regarding the accounting information system from the report.

We manipulated the use of the techniques of neutralization in six ways: (1) no technique of neutralization used. Or, a statement relating to (2) denial of responsibility, (3) denial of injury, (4) defense of necessity, (5) appeal to higher loyalties, or (6) metaphor of the ledger. Table 1 presents each independent variable. The option of no technique of neutralization was given to provide a control group. This variable was omitted from the analysis in order to provide coefficients, z-statistics, and p-values for the variables relating to the tested hypotheses.

The level of deterrence is a four-way manipulation with all possible pairs of the following options: sanction certainty (likelihood of being caught) was either minimal or severe and sanction severity (level of punishment) was either minimal or severe.

3.4.2 Dependent Variable

The dependent variable in the current research is the likelihood that the participants would behave unethically by altering their working papers to minimize or reduce references to an information system control weakness. The participants provided responses to two questions regarding the likelihood of violating the Generally Accepted Auditing Standards: (1) the likelihood that they would modify the working papers (DV1), and (2) the likelihood that another auditor in the same situation would modify the working papers (DV2).

Table 1. Independent Variables

Variable	Retained in the model*	Hypothesis (expected sign)	Manipulation
Techniques of Neutralization			
Denial of responsibility	Yes	H1 (+)	Believes that since his supervisor told him to modify the report, he has no control over the decision
Denial of injury	Yes	H2 (+)	Believes that no one would be harmed by modifying the report
Defense of necessity	Yes	H3 (+)	Believes that if he does not modify the report, his firm will lose [client name] as a client
Appeal to higher loyalties	Yes	H4 (+)	Believes that modifying the report would not be as bad as modifying the financial statement numbers
Metaphor of the ledger	Yes	H5 (+)	Believes that all her past reports were appropriate, so it would be OK to modify the report just this one time
(No technique of neutralization)	No		This item would not have been in the scenario.
Deterrence theory			
Low sanction certainty, low sanction severity	No		Believes that her chances of being caught are low, but if caught, the punishment would be minimal
Low sanction certainty, high sanction severity	Yes	H6 (-)	Believes that her chances of being caught are low, but if caught, the punishment would be severe
High sanction certainty, low sanction severity	Yes	H7 (-)	Believes that her chances of being caught are high, and if caught, the punishment would be minimal
High sanction certainty, high sanction severity	Yes	H6 & H7 (-)	Believes that her chances of being caught are high, and if caught, the punishment would be severe
Degree of violation			
Degree of violation: high	Yes	H8 (-)	Remove all of the references to control deficiencies regarding the [software co. name] AIS package from the report
Degree of violation: low	No		Minimize the references to control deficiencies regarding the [software co. name] AIS package from the report

Note: * One of the underlying assumptions of mixed-model analysis requires that none of the independent variables in the model be linear combinations of other independent variables in the model. Therefore, in order to test our hypotheses and the underlying theories using mixed-model analysis, we retained all of the variables where a technique of neutralization was present, sanction certainty and/or sanction severity were high, and where the degree of violation was high.

Fully anchored 5-point Likert-type scales, which ranged from 1 = *definitely would not modify the working papers* to 5 = *definitely would modify the working papers*, were used to capture participants' responses. The responses to the two likelihood questions were averaged to yield the dependent variable (DVAVE). This two-item technique reduces the social desirability response bias associated with asking only for the likelihood that the participant would personally modify the working papers (Chung & Monroe 2003; Cuixia, 2003; Robinson, 2012; Trinkle et al. 2014).

3.4.3 Control Variables and Other Manipulations

We controlled for possible differences within the sample through several control variables. As previously discussed, the sample contained both graduate and undergraduate students. Though Stanga and Turpen (1991) and Betz et al. (1989) both used graduate and undergraduate students as samples, neither study presented any results indicating a difference between undergraduate and graduate students in terms of moral decision-making. However, we would expect that graduate students would have a better understanding of the ethical expectations of the accounting profession because they would have likely taken more courses with audit and ethics components, leading to the expectation that as they progress through their education, they would be less likely to behave unethically. Therefore, we controlled for graduate and undergraduate status with a dummy variable. We expect the same to be the case with those students who have participated in an internship, as they would have likely gained firsthand experience of auditors navigating ethical decisions. Thus, we also controlled for completion of an internship with a dummy variable.

Prior research is mixed on the differences between how men and women respond to decisions of moral judgment. Betz et al. (1989) and Stanga and Turpen

(1991) find that men and women respond differently. However, Rest (1986) found no difference across genders. The lack of consensus in the extant research led to the inclusion of gender as a control variable in the current study.

To control for possible biased reactions to nontested items in the scenario, we manipulated several other factors. We randomly manipulated the gender of the main character, the client's name, the software company's name, and the firm's name. An expert panel of behavioral researchers examined the list of client, company, and firm names and found them to be free of possible regional biases and frivolity.[3]

4 Results

We conducted a mixed-model analysis to generate results for the hypothesis testing. The mixed-model technique was used because of the associated lack of independence (Vance et al. 2013) of the participants considering multiple scenarios; mixed-modeling adjusts for the correlation associated with repeated measures. The mixed command in Stata 14 was used to generate the linear mixed-model results. Further, we conducted a relative-weight analysis (Johnson, 2000). Relative-weight analysis determines the proportionate contribution that each variable contributes to the model R^2 by considering both the direct effect of each variable and its joint effect with other variables in the model (Johnson, 2000). Table 2 presents the descriptive statistics for the dependent variables. The Cronbach's alpha (Cronbach, 1951) of 0.885 supports the reliability of the scale of the dependent variable. Table 3 presents the correlation matrix for the variables. All correlations are less than 0.70, thus multicollinearity is not an issue. We expected that the degree of violation variable (RM1) would have been better correlated to the deterrence theory variables (DT2, DT3, and DT4), as one would expect that, as the severity of the violation increases, the severity of the penalty would also increase. The correlations in the current study may be an indication that the participants viewed both violations as equally severe since both are considered fraud, and auditors are taught that fraud is unethical and may result in severe punishment.

We used the Shapiro-Francia test to test the normality of the continuous dependent variables. The tests showed that DV1 (z = 4.03, p-value<0.01) was not normally distributed, while DV2 (z = 0.84, p-value = 0.2) and DVAVE (z = 1.11, p-value = 0.13) were normally distributed. Therefore, DVAVE meets the normality assumption of mixed-model analysis for continuous variables and was used in an unaltered state in the model testing. The remaining variables are binary and not subject to the normality assumption.

Further analysis of the responses to DV1 and DV2 yielded interesting findings regarding a possible social desirability bias. The results of a Pearson chi-square test (chi-square = 97.56, p-value < 0.01) and the two-sample Wilcoxon rank-sum test (z = 12.76, p-value < 0.01) indicate that social desirability bias is likely to exist, as the median value for DV1 is significantly lower than the median value of DV2. Non-parametric tests were used because DV1 was not being normally distributed.

Furthermore, 76.6% (233/304) of the observations contained responses to DV1 that were lower than the matched responses for DV2. This finding indicates that social desirability bias may have been involved in the participants' responses to the likelihood that they would modify the working papers (DV1). Of the 24.4% (71/304) of the observations that did not indicate a possible social desirability bias, 58 (19.1% of 304) provided identical responses for both DV1 and DV2, while 13 (4.3% of 304) provided responses indicating that the responding participant was more likely to modify the working papers than another auditor in the same situation.

4.1 Hypothesis Testing

To evaluate the results of the data collection, we first evaluated each hypothesis individually. Subsequently, we performed a relative-weight analysis to determine which factors contribute the most to the R^2 value.

4.1.1 Individual Items

H1-H5 concern the effectiveness of techniques of neutralization on influencing an auditor's behavioral intention to violate policy. H6 and H7 address the effects of deterrence theory. H8 concerns the degree of violation. Table 4 presents the results of the mixed-model analysis for the significance of the individual hypotheses. The results suggest that the neutralization technique denial of responsibility (TN1) (z = 2.13, p-value < 0.05) significantly contributes to the likelihood that the participants would form the intention to behave unethically. Thus, H1 is supported. The remaining neutralization techniques, denial injury (H2), defense of necessity (H3), appeal to higher loyalties (H4), and metaphor of the ledger (H5), do not significantly contribute to the participants' likelihood of forming intentions to behave unethically.[4] Thus, the results do not support these hypotheses.

[3] The client, company, and firm names were randomly selected from the following list: Crossroads, Inc., Newline Company, Everlast Industries, Paxton, Inc., True Blue Corporation, 4th Street Company, Sunset Industries, Century Corporation, Triple Point Enterprises, Dynamic Corporation, Agile Industries, Creative Corp., Parker Enterprises, Freeland Enterprises, Aspire Enterprises, and Peak Industries.

[4] One-tailed p-values are used for hypothesis testing.

Table 2. Descreptive Statistics

Panel A: Participant-specific statistics		
Variable	**Frequency**	**Percentage**
Age group		
18-21	50	48.1%
22-29	49	47.1%
30-39	2	1.9%
40-49	2	1.9%
50-59	1	1.0%
Gender		
Male	53	51.0%
Female	51	49.0%
Student classification		
Graduate student	22	21.2%
Undergraduate student	82	78.8%
Internship		
Yes	33	31.7%
No	71	68.3%
N= 104		

Panel B: Dependent variable				
Variable	**Mean**	**Standard deviation**	**Minimum**	**Maximum**
DV1	2.07	1.157	1	5
DV2	3.42	1.123	1	5
DVAVE	2.75	0.098	1	5

Note: N = 304. DV1 = The likelihood that the participant would behave unethically in the given situation,.
DV2 = The likelihood that others in the given situation would behave unethically. DVAVE = Average of the likelihood that the participant and others in the same situation would behave unethically.

Table 3. Correlation Matrix

	DVAVG	**TN1**	**TN2**	**TN3**		**TN4**	**TN5**	**DT2**	**DT3**	**DT4**	**RM1**	**Gender**	**Internship**	**Grad**
DVAVG	1													
TN1	0.112*	1												
TN2	-0.064	-0.179**	1											
TN3	0.102	-0.162**	-0.187***	1										
TN4	-0.045	-0.188***	-0.216***	-0.195***		1								
TN5	0.036	-0.173**	-0.199***	-0.180**		-0.208***	1							
DT2	-0.043	0.039	0.129*	-0.201***		0.006	-0.109	1						
DT3	-0.018	-0.208***	0.142**	0.033		0.244***	-0.231***	-0.285***	1					
DT4	-0.257**	-0.061	0.035	0.167**		-0.145**	0.092	-0.302***	-0.293***	1				
RM1	0.048	0.016	0.117*	0.102		-0.377***	0.181**	0.028	-0.013	-0.072	1			
Gender	-0.033	0.021	0.026	-0.158**		0.025	-0.107	0.076	0.053	-0.119*	-0.018	1		
Internship	0.088	0.045	-0.005	0.045		-0.009	0.033	-0.060	-0.097	0.092	-0.091	-0.333***	1	
Grad	-0.057	0.036	-0.017	-0.003		0.050	-0.092	-0.006	0.065	0.059	-0.039	-0.132*	0.303***	1

Note: N = 304, * Significant at the 0.05 level ** Significant at the 0.01 level *** Significant at the 0.001 level
TN1 = Denial of Responsibility, TN2 = Denial of injury, TN3 = Defense of necessity, TN4 = Appeal to higher loyalties
TN5 = Metaphor of the ledger, DT2 = Sanction certainty is low and sanction severity is high, DT3 = Sanction certainty is high and sanction severity is low,
DT4 = Sanction certainty is high and sanction severity is high,
RM1 = Degree of Violation where 1 = remove all of the references and 0 = minimized all references
Grad = Dummy variable where 1 = graduate student and 0 = undergraduate student, Gender = Dummy variable where 1 = male and 0 = female
Internship = Dummy variable where 1 = participated in an internship and 0 = did not participate in an internship

Table 4. Mixed Model Analysis Results for the Individual Impact of Magnitude of Alteration, Techniques of Neutralization, and Deterrence Theory on an Auditor's Behavioral Intention to Violate Policy

	Predicted Sign	Beta	Z
(Constant)	n/a	3.13	16.79**
TN1	+	0.36	2.13*
TN2	+	0.02	0.18
TN3	+	0.22	1.42
TN4	+	0.16	1.17
TN5	+	0.01	0.06
DT2	-	-0.54	-4.13**
DT3	-	-0.41	-3.44**
DT4	-	-1.06	-9.16**
RM1	-	-0.14	-1.33
Grad	-	-0.10	-0.50
Gender	n/a	-0.07	-0.42
Internship	-	0.20	1.09

Note: N=304, R2 = 0.16, * Significant at the 0.05 level, ** Significant at the 0.001 level
TN1 = Denial of responsibility, TN2 = Denial of injury
TN3 = Defense of necessity, TN4 = Appeal to higher loyalties,TN5 = Metaphor of the ledger,
DT2 = Sanction certainty is low and sanction severity is high,DT3 = Sanction certainty is high and sanction severity is low,
DT4 = Sanction certainty is high and sanction severity is high
RM1 = Degree of violation where 1 = remove all of the references and 0 = minimized all references
Grad = Dummy variable where 1 = graduate student and 0 = undergraduate student, Gender = Dummy variable where 1 = male and 0 = female
Internship = Dummy variable where 1 = participated in an internship, and 0 = did not participate in an internship

Table 5. Relative Weight Analysis

	Raw Relative Weights	Relative Weights as a Percentage of R^2
TN1	0.013	8.3%
TN2	0.001	0.5%
TN3	0.017	11.3%
TN4	0.001	0.8%
TN5	0.003	2.3%
DT2	0.010	6.5%
DT3	0.006	4.0%
DT4	0.085	56.6%
RM1	0.001	0.6%
Grad	0.004	2.5%
Gender	0.001	0.6%
Internship	0.009	5.9%

Note: R2 = 0.15, TN1 = Denial of Responsibility, TN2 = Denial of Injury, TN3 = Defense of Necessity, TN4 = Appeal to a Higher Loyalties
TN5 = Metaphor of the ledger, DT2 = Sanction certainty is low and sanction severity is high
DT3 = Sanction certainty is high and sanction severity is low, DT4 = Sanction certainty is high and sanction severity is high
RM1 = Degree of violation where 1 = remove all of the references and 0 = minimized all references
Grad = Dummy variable where 1 = graduate student and 0 = undergraduate student, Gender = Dummy variable where 1 = male and 0 = female
Internship = Dummy variable where 1 = participated in an internship and 0 = did not participate in an internship

H6 and H7 address the impact of perceived potential certainty and severity of the sanctions in terms of auditors' behavioral intention to violate policy, and the results support both hypotheses. The results suggest that high severity of sanctions combined with low certainty of sanctions significantly contributes to the reduction of the participants' likelihood of forming intentions to behave unethically (H6) (z = -4.13, p < 0.001), as do high certainty of sanctions combined with low severity of sanctions (H7) (z = -3.44, p-value < 0.001), making it less likely that the participants would behave unethically. High certainty of sanctions accompanied with high severity of sanctions yielded results that provide further support for H6 and H7, since the results for this combination (H7) (z = -9.16, p-value < 0.001) have a significant negative relation with the participants' likelihood of forming intentions to behave unethically. Increasing the degree of violation from minimizing references concerning the system control weaknesses to removing references concerning the control weakness from the working papers did not significantly contribute to the participants' likelihood of forming intentions to behave unethically (z = -0.14, p-value = 0.08). Thus, H8 is not supported.

While the R^2 value in this study is relatively low (R^2 = 0.15), we believe that the results of this study are informative. As discussed by (Hair Jr. et al. 2016), R^2 values are dependent on the model complexity and the research discipline; they do not necessarily indicate whether a regression model provides an adequate data fit. Essentially, R^2 values tend to be significantly lower for studies that comprise an inherently greater amount of unexplainable variation (e.g., studies attempting to explain human behavior) in comparison to studies predicting physical processes. Thus, the low R^2 can be attributed to the specific nature of our dependent variable (i.e., auditors' intentions to falsify information), which essentially consists of a significant amount of unexplainable variation beyond what is explained by the neutralization and deterrence theories.

The results do not indicate significance for any of the control variables (university status, gender, or participation in an internship). This is interesting because we expected that the increased exposure to classroom discussions about the importance of ethics in the accounting profession, along with witnessing professionals ethically practicing accounting during an internship, might significantly reduce the participants' likelihood of forming intentions to behave unethically.

4.1.2 Relative Weight Analysis

The results of the relative weight analysis (Johnson, 2000) contained in Table 5 indicate that the presence of both high certainty and high severity of sanctions (DT4) explain 56.6% of the variance in the participants' likelihood of forming intentions to behave unethically. The remainder of the deterrence theory variables, DT2 and DT3, explain 6.5% and 4.0% of the remaining variance, respectively. The most important techniques of neutralization, as explained by their percentage of explained variance, are defense of necessity (11.3%) and denial of responsibility (8.3%).

Interestingly, two of the techniques of neutralization (TN1 and TN3) reversed positions from the mixed-model results. This is not unusual, as a variable may not be a significant contributor in a mixed-model or regression analysis because it is related to another variable in the model.

However, in relative weight analysis, this variable may have a large relative weight because the predictable variance is distributed across all related variables. The opposite may be true for a significant predictor in a mixed-model or regression analysis in that its unique variance may generate significant results but it may have a small relative weight.

The results of the relative-weight analysis add further support to the tested hypotheses, indicating that if the participants' believe that they are not responsible for their unethical behavior (H1) and/or that behaving unethically is necessary (H3), they are more likely to consider behaving unethically. However, in keeping with deterrence theory, if the punishment (severity) for behaving unethically is high (H6) and/or the likelihood of getting caught (certainty) is high (H7), the participants are less likely to form intentions to behave unethically.

4.1.3 Sensitivity Analysis

Because of the differences in DV1 and DV2, we performed sensitivity analysis by testing the hypotheses on models developed with the individual items in the DVAVE construct used as the dependent variables. Because DV1 was not being normally distributed, we used the log of DV1. The results of the two models are very similar to the primary results of DVAVE, which are presented in the previous section. For the separate models with logDV1 and DV2 as the dependent variables, the significance of the coefficients of all of the dependent variables are identical to the DVAVE results, except that TN1 is no longer significant. However, TN1 approaches significance in the DV2 model. The change in the significance for TN1 illustrates the effect of social desirability in the results for the logDV1 model and necessitates the need to average DV1 and DV2. Appendix D presents the results of the mixed model analysis for the sensitivity analysis.

5 Discussion

Because auditors behaving unethically is a high-impact threat to the security and integrity of corporate information, its causes and drivers require careful empirical analysis. When auditors choose to modify the working papers to avoid reporting irregularities in the information system uncovered during an audit, it is important to recognize the factors that may contribute positively or negatively to such behavior. The results of our work contribute to the practical understanding of this important phenomenon and provide a research foundation for further investigation.

5.1 Summary of Results

Our findings show that the technique of denial of responsibility influences auditors' behavioral intentions to violate policy (H1 is supported), but the use of other techniques is not supported by our experimental results (denial injury: H2, defense of necessity: H3, appeal to higher loyalties: H4, and metaphor of the ledger: H5). Further, we established that perceptions of sanction certainty (H6) and severity (H7) have a negative influence on the formation of the behavioral intention to violate policy, thereby establishing the role of punishment as a powerful deterrent to unethical behavior resulting in policy violation by auditors. Finally, the degree of violation, whether it was a serious blatant violation or a relatively less deviant one, was not found to matter in the context

of our study (H8 is not supported). Overall, we can conclude that auditors may justify their unethical behavior but the expectation of severe and certain punishment can ameliorate this intent.

5.2 Contribution to Research and Theory

Our research empirically tested the role of justification by auditors, which enables them to rationalize unethical behavior, coupled with the impact of sanctions on intentions to violate policy. Our results highlight the important role that persuasive communications can play in influencing auditors to avoid behaviors that they know are in clear violation of their professional standards of conduct, and which are subject to significant professional sanctions. The fact that such behaviors continue to be a problem means that we must test all causes, and our findings offer a tangible contribution to the literature examining this phenomenon. We further validate the role of sanction severity and sanction certainty, established in the extant literature, within the focal phenomenon of this study. We investigated the influence of sanctions and neutralizations in extreme boundary conditions and found that even in these cases, deterrence theory is robust and plays a significant role in deterring behavioral intentions to violate norms and standards. Nevertheless, some techniques of neutralization continue to have a significant effect on behavioral intentions to violate a policy.

A conceptual explanation for the combined influence of sanctions and neutralization techniques is that, even in the presence of extreme punishments, employees may ignore sanctions if they feel they can avoid detection or if the expected punishment is not severe (even if caught). These assumptions can be viewed as a means by which employees neutralize their actions even in the presence of sanctions. Thus, through the techniques of neutralization, employees may eliminate guilty feelings or self-blame (Sykes & Matza 1957) and may thus defuse the effect of sanctions by rationalizing their actions (Siponen & Vance, 2010).

Sanction severity and certainty could be context-dependent; some organizations may immediately fire employees for policy violations whereas others may not. Additionally, for sanctions to be effective, they must be perceived as fair and appropriate by employees, which further prevents employee backlash or other unintended consequences. Thus, it may be presumed that while severe sanctions imposed with certainty are necessary to minimize policy violations, employees may still invoke neutralization techniques to rationalize their actions in situations where they intend to violate organizational policies. These findings provide evidence to support the need to test behavioral theory beyond existing boundary conditions to determine whether the initial findings are robust. Overall, our work empirically establishes the finding that cognitive mediating processes can lead auditors to either violate policy or reject the temptation to do so.

5.3 Contribution to Practice

Our findings reveal implications for practice, especially regarding the role of organizational levers of influence, including sanctions and other persuasive communications intended to suppress the influence of rationalization and enhance the motivation to comply with standards and policies. With respect to the significant influence of sanctions on an employee's intention to violate company policy, it can be inferred that sanctions mainly serve as a deterrent for employees who intend to violate these policies. Additionally, organizations can implement sanctions as a means of establishing a legal foundation that allows the organization to undertake well-defined punishments for employees who are caught violating organizational policies. Furthermore, perceptions of sanction severity and certainty rely on an employee's *awareness* of the existence of these sanctions. Though not tested in this study, we believe that organizations can increase employee awareness through interventions such as security education, training, and awareness programs (SETA). The effectiveness of such programs is mainly dependent on the organization's ability to take clearly defined actions against employees who violate the policies. Thus, sanctions may be only useful to the extent that the organization is willing to impose them effectively—otherwise, sanctions might be counterproductive.

In the context of our study, the implications suggest that employers should be clear and unambiguous about the organizational punishment that will be directed toward auditors who violate their professional standards and violate policy, even if employees may be tempted to rationalize or justify their deviant behavior. However, because we establish that auditors may cognitively rationalize their unethical behaviors, we expose the need to address a specific human decision process that is subject to external influences. Regardless of which neutralization technique (or techniques) facilitates specific policy violations, it is imperative that organizations proactively endeavor to thwart the likelihood of employees seeking to justify their actions.

To the extent that more extreme sanctions are more typical in auditor rule violation settings, the content presented to auditors in colleges and universities, in continuing education classes, and in various publications should explicitly articulate the message that rationalization should be avoided and that sanctions that are tough and certain. Such measures should be effective in reducing the incidence of unethical auditor behavior. Nonspecific messages will likely have less effect than explicit messages in the

training materials. Results reported in Johnston et al., 2018 establish the increased effectiveness of such messages when their rhetoric is designed to match the audience and context. Further, ongoing reminders (e.g. psychological "nudges") to staff auditors will result in greater compliance with professional standards of conduct.

Generalizing to other contexts beyond auditors, it is interesting to consider the role and effectiveness of comparable career-ending sanctions. Employees caught embezzling funds by hacking into their employers' servers have not uniformly faced extreme sanctions; in some cases, these employees were hired as consultants to identify security vulnerabilities. In the modern era, norm-violating behaviors in the workplace, especially in the entertainment media, have ended the careers of several very prominent broadcasters, journalists, actors, sports stars, and movie executives. It remains to be seen whether sanctions will deter future potential violators. Within the criminal justice system, there continues to be debate on the role of extreme sanctions, such as the death penalty or imprisonment for life without the possibility of parole. Our findings suggest that, even in the context of extreme sanctions, individuals will justify their deviant behavior and engage in extremely egregious behaviors.

5.4 Research Limitations and Future Research

We adopted numerous measures to ensure the validity of our experimental design, measures, and analysis, but we identified certain research limitations. Our sampling frame consisted of undergraduate and graduate accounting students as proxies for auditors. Accounting students may or may not be as sensitive to deterrence tactics as other subjects but they did provide a reasonable proxy for an important sector of powerful actors who are authorized and capable of corrupting data integrity in a significant way. Though we did not use practicing auditors in our sample, our theories can be tested using our reasonable surrogates, as these high-sanction situations would be recognized by all auditors, whether entry level or more experienced. It is possible that more experienced auditors would evaluate the scenarios differently and it is possible that real opportunities to behave unethically would be met with different outcomes than reported in response to our hypothetical scenarios. We recognize that, even with full recognition of extreme sanctions, students were evaluating a hypothetical situation that may have reduced salience when contrasted with a practicing auditor with a mortgage and hungry children at home. Related to this limitation is the clustering of our respondents' ages. Although age was not identified as a behavioral determinant, it is possible that older auditors might respond differently when exposed to similar messages on the job.

A limitation of the factorial survey method is the chance that the study participants may have already been involved in similar experiences and may feel compelled to adopt neutralization techniques to preserve their self-image rather than justify the actions of the scenario characters (Siponen & Vance, 2010). However, this is unlikely given our sampling pool. Also, there is no known empirical control for this potential confound when using self-reporting. Siponen and Vance (2010) suggest that the expected number of previous computer abuse violators was likely insufficient to skew the results of their study and we suggest that the same expectation is reasonable for ours.

Further, we did not test for the impacts of measures to increase the perceived accountability of our subjects (the degree to which they felt they were held accountable for their actions), which has been shown to exert an influence on violation decisions (Vance et al., 2015). Future research could investigate this factor or could investigate this decision-making process using emerging neurophysiological research techniques (Anderson et al., 2015; Warkentin et al., 2016) designed to generate objective measures of cognitive and affective processes. Future research could also differentiate the specific impacts of various extreme levels of sanction severity, certainty, and celerity.

Another limitation concerns the cross-sectional design of this study. Because the factorial survey design is cross-sectional, it did not allow us to account for the temporal effects of drift—"a temporary period of irresponsibility or an episodic relief from moral constraint" (Maruna & Copes, 2005, p. 231). Drift could influence intentions to commit computer abuse and Maruna and Copes (2005) identify these limitations associated with utilizing the factorial survey design in their study as well. Both limitations could be overcome by employing a longitudinal design, which should be considered in future research.

We tested the impact of five techniques of neutralization: the denial of responsibility, the denial of injury, the defense of necessity, the appeal to higher loyalties, and the metaphor of the ledger in the context of auditor rule violations. Our results indicate that employees utilize two of these rationalization techniques—specifically, the denial of responsibility and the appeal to higher loyalties—in their intentions to violate policy. While we were able to evaluate the specific techniques of neutralization applicable in the context of our study, we did not investigate whether an employee can invoke a single or several neutralization techniques in the context under investigation. Thus, future research should attempt to explore whether

these neutralization techniques are mutually exclusive or whether an individual feels the necessity to rationalize their deviant actions through several neutralization techniques. Furthermore, we tested the five dominant techniques of neutralization, though many others have been identified. Future researchers could explore the impact of other rationalizations that auditors may use to rationalize unethical behavior.

Future research efforts could also explore the use of neutralization techniques ex post, rather than a priori, in terms of how they are used to assuage guilt or remorse felt in response to deviant workplace behavior after the fact. Although Siponen and Vance (2010) and other IS scholars have investigated the role of neutralization as an antecedent to the formation of intention, it certainly could apply to subsequent behavior as well, especially regarding behavioral acts that are spontaneous rather than deliberative. We urge further research into this interesting potential phenomenon.

Sanction certainty is at the heart of much debate in the criminal justice system (e.g., mandatory sentencing guidelines, stiffer fines, etc.) and has also been the focus of much research in information security. Although other elements of deterrence (i.e., severity and celerity) are interesting, we wanted to test the theoretical boundaries of this fundamental core element of deterrence theory, especially in terms of violators rationalizing norm-violating actions. Future research should similarly test the theoretical boundaries of other elements of both deterrence and neutralization.

Cover-up behaviors also represent a future avenue of research that could provide additional insight into the factors that influence auditors' and IS professionals' behavioral intentions to violate policies. Future research could test the findings of our research and other boundary conditions in other domains and environments. For example, physicians and others subject to severe sanctions for policy violations might offer an interesting context. Similarly, all students know that cheating in class may be subject to severe penalties, including expulsion from school. Our target behavior may represent an anomalous or unique violation scenario, so relaxing the boundary conditions from extreme sanctions (for ethical breaches of professional auditors) to slightly less severe sanctions (for auditors, physicians, politicians, or other professionals) could help establish the level at which sanction severity is efficacious. The perceived sanction severity boundary should be tested in multiple domains to strengthen our findings.

6 Conclusion

We contextualized and explored the boundary conditions of the techniques of neutralization and deterrence theory by applying the theoretical lenses of the theories' determinants in a professional context with severe deterrence levels. To achieve this objective, we used a scenario-based experiment to understand key determinants of the formation of auditors' behavioral intentions to violate policy by modifying working papers to hide irregularities, thereby jeopardizing the integrity and security of the accounting information system. Our results indicate that auditors may justify their unethical behavior by denying responsibility for their personal actions, perhaps by believing that they had no choice. We did not find sufficient evidence to suggest that these behaviors systematically influence the dependent variables, and we can presume that most auditors act in accordance with professional standards in every circumstance. Also, we demonstrated that perceived severity of punishment and the certainty of receiving punishment are significant deterrents to auditors in this context. Although further research into this phenomenon is needed, we contribute to the understanding of this phenomenon by showing that auditors can and will violate policy if they can justify their actions and if the punishment is not strong or certain, leading to practical implications for the profession. We also suggest that our results validate the earlier contribution of Siponen and Vance (2010) and Willison, et al. (2018) regarding the role of neutralization in enabling norm-violating behavior in the context of information security standards. Our findings also offer insights into the roles that deterrence and neutralization processes play in IS-related workplace deviant behavior in general by more closely scrutinizing the applicable range of key boundary conditions—i.e., the actual severity of formal sanctions. Our work adds to the extant literature on deterrence theory and the techniques of neutralization, which collectively provide foundational support for factors leading to employees' behavioral intentions to violate organizational policies.

References

Abelson, R. & Glater, J. D. (2002). Enron's collapse: The auditors: Who's keeping the accountants accountable. https://www.nytimes.com/2002/01/15/business/enron-s-collapse-the-auditors-who-s-keeping-the-accountants-accountable.html

ACFE. (2012). *Report to the nations on occupational fraud and abuse*. https://www.acfe.com/uploadedFiles/ACFE_Website/Content/rttn/2012-report-to-nations.pdf

AICPA (2009). Communicating internal control related matters identified in an audit https://www.aicpa.org/Research/Standards/AuditAttest/DownloadableDocuments/AU-C-00265.pdf

Akers, R. L. & Sellers, C. S. (2004). *Criminological theories: Introduction, evaluation, and application* (4th ed.). Roxbury Press.

Alvarez, A. (1997). Adjusting to genocide: The techniques of neutralization and the Holocaust. *Social Science History*, *21*(2), 139-178.

Anderson, B. B., Vance, A., Kirwan, B., Jenkins, J., & Eargle, D. (2015). Using fMRI to explain the effect of dual-task interference on security behavior. *Proceedings of the Gemunden Retreat on NeuroIS*.

Anderson, J. M. (2003). Why we need a new definition of information security. *Computers & Security*, *22*(4), 308-313.

Barlow, J. B., Warkentin, M., Ormond, D., & Dennis, A. R. (2013). Don't make excuses!: Discouraging neutralization to reduce IT policy violation. *Computers & Security*, *39*(Part B), 145-159.

Barlow, J. B., Warkentin, M., Ormond, D., & Dennis, A. R. (2018). Don't even think about it! The effects of anti-neutralization, informational, and normative communication on information security compliance. *Journal of the Association for Information Systems*, *19*(8), 689-715.

Barrack, J. A. (2005). Auditor Responsibility Under the federal securities laws: A note from the Worldcom securities litigation. *American Journal of Trial Advocacy*, *29*(1), 1-18.

Bazerman, M. H., Loewenstein, G., & Moore, D. A. (2002). Why good accountants do bad audits. *Harvard Business Review*, *80*(11), 96-103.

Betz, M., O'Connell, L., & Shepard, J. M. (1989). Gender differences in proclivity for unethical behavior. *Journal of Business Ethics*, *8*(5), 321-324.

Bicchieri, C. (2005). *The grammar of society: The nature and dynamics of social norms*. Cambridge University Press.

Brennan, W. C. (1974). Abortion and the techniques of neutralization. *Journal of Health and Social Behavior*, *15*(4), 358-365.

Butler, J. M. (2012). Privileged password sharing: "Root" of all evil. *SANS Analyst Program*. https://www.sans.org/reading-room/whitepapers/analyst/privileged-password-sharing-root-evil-35195

Chung, J. & Monroe, G. S. (2003). Exploring Social desirability bias. *Journal of Business Ethics*, *44*(4), 291-302.

Coleman, J. W. (1985). *The criminal elite: The sociology of white collar crime*. Worth Publishers.

Compeau, D., Marcolin, B., Kelley, H., & Higgins, C. (2012). Generalizability of information systems research using student subjects: A reflection on our practices and recommendations for future research. *Information Systems Research*, *23*(4), 1093-1109.

Congress. (2002). *Sarbanes-Oxley Act of 2002*. US Government Printing Office.

Copes, H. & Deitzer, J. R. (2015). Neutralization theory, In W. G. Jennings, *The Encyclopedia of Crime and Punishment*. Wiley.

COSO (1994). *Internal control: Integrated framework*. Jersey City, NJ: Committee of Sponsoring Organizations of the Treadway Commission.

Cronbach, L. J. (1951). Coefficient alpha and the internal structure of tests. *Psychometrika*, *16*(3), 297-334.

Crossler, R. E., Johnston, A. C., Lowry, P. B., Hu, Q., Warkentin, M., & Baskerville, R. (2013). Future directions for behavioral information security research. *Computers & Security*, 32(1), 90-101.

Cuixia, L., Jian, X., & Zhongfang, Y. (2003). A compromise between self-enhancement and honesty: Chinese self-evaluations on social desirability scales. *Psychological Reports*, *92*(1), 291-298.

D'Arcy, J. & Devaraj, S. (2012). Employee Misuse of Information Technology Resources: Testing a Contemporary Deterrence Model. *Decision Sciences*, *43*(6), 1091-1124.

D'Arcy, J. & Herath, T. (2011). A review and analysis of deterrence theory in the IS security literature: Making sense of the disparate findings. *European Journal of Information Systems*, 20(6), 643-658.

D'Arcy, J. & Hovav, A. (2007). Deterring internal information systems misuse. *Communications of the ACM, 50*(10), 113-117.

D'Arcy, J., Hovav, A., & Galletta, D. (2009). User awareness of security countermeasures and its impact on information systems misuse: A deterrence approach. *Information Systems Research*, 20(1), 79-98.

Dunford, F. W. & Kunz, P. R. (1973). The neutralization of religious dissonance. *Review of Religious Research, 15*(1), 2-9.

Earley, C. E. & Kelly, P. T. (2004). A note on ethics educational interventions in an undergraduate auditing course: Is there an "Enron effect"? *Issues in Accounting Education, 19*(1), 53-71.

Eliason, S. L. & Dodder, R. A. (1999). Techniques of neutralization used by deer poachers in the Western United States: A research note. *Deviant Behavior, 20*(3), 233-252.

Ge, L. & Thomas, S. (2008). A cross-cultural comparison of the deliberative reasoning of Canadian and Chinese accounting students. *Journal of Business Ethics, 82*(1), 189-211.

Goode, S. & Lacey, D. (2011). Detecting complex account fraud in the enterprise: The role of technical and non-technical controls. *Decision Support Systems, 50*(4), 702-714.

Gordon, M. E., Slade, L. A., & Schmitt, N. (1986). The "Science of the Sophomore" revisited: From conjecture to empiricism. *Academy of Management Review, 11*(1), 191-207.

Gray, P. H. & Cooper, W. H. (2010). Pursuing failure. *Organizational Research Methods, 13*(4), 620-643.

Grover, V. (2012). The information systems field: Making a case for maturity and contribution. *Journal of the Association for Information Systems, 13*(4), 254-272.

Guo, K. H., Yuan, Y., Archer, N. P., & Connelly, C. E. (2011). Understanding nonmalicious security violations in the workplace: A composite behavior model. *Journal of Management Information Systems, 28*(2), 203-236.

Hair Jr, J. F., Hult, G. T. M., Ringle, C., & Sarstedt, M. (2016). *A primer on partial least squares structural equation modeling (PLS-SEM)*. SAGE.

Harrington, S. J. (1996). The Effect of codes of ethics and personal denial of responsibility on computer abuse judgments and intentions. *MIS Quarterly, 20*(3), 257-278.

Herath, T. & Rao, H. (2009). Protection motivation and deterrence: A framework for security policy compliance in organisations. *European Journal of Information Systems, 18*(2), 106-125.

Higgins, G. E., Wilson, A. L., & Fell, B. D. (2005). An application of deterrence theory to software piracy. *Journal of Criminal Justice and Popular Culture, 12*(3), 166-184.

Hinduja, S. (2007). Neutralization theory and online software piracy: An empirical analysis. *Ethics and Information Technology, 9*, 187-204.

Ho, S. M. & Warkentin, M. (2017). Leader's dilemma game: An experimental design for cyber insider threat research. *Information Systems Frontiers, 19*(2), 377-396.

Hollinger, R. C. (1991). Neutralizing in the workplace: An empirical analysis of property theft and production deviance. *Deviant Behavior, 12*(2), 169-202.

Huang, S.-M., Yen, D. C., Yang, L.-W., & Hua, J.-S. (2008). An investigation of Zipf's Law for fraud detection. *Decision Support Systems, 46*(1), 70-83.

Humpherys, S. L., Moffitt, K. C., Burns, M. B., Burgoon, J. K., & Felix, W. F. (2011). Identification of fraudulent financial statements using linguistic credibility analysis. *Decision Support Systems, 50*(3), 585-594.

Jasso, G. (2006). Factorial survey methods for studying beliefs and judgments. *Sociological Methods & Research, 34*(3), 334-423.

Jasso, G. & Rossi, P. H. (1977). Distributive justice and earned income. *American Sociological Review, 42*, 639-651.

Johns, G. (2006). The essential impact of context on organizational behavior. *Academy of Management Review, 31*(2), 386-408.

Johnson, J. W. (2000). A heuristic method for estimating the relative weight of predictor variables in multiple regression. *Multivariate Behavioral Research, 35*(1), 1-19.

Johnston, A. C., Warkentin, M., Dennis, A. R., & Siponen, M. (2018). Speak their language: Designing effective messages to improve employees' information security decision making. *Decision Sciences, 50*(2), 245-284.

Johnston, A. C., Warkentin, M., McBride, M., & Carter, L. (2016). Dispositional and situational

factors: Influences on information security policy violations. *European Journal of Information Systems, 25*(3), 231-251.

Kankanhalli, A., Teo, H.-H., Tan, B. C. Y., & Wei, K.-K. (2003). An integrative study of information systems security effectiveness. *International Journal of Information Management, 23*(2), 139-154.

Kaspersky. (2015). *The threat within: 3 out of 4 companies affected by internal information security incidents*, http://usa.kaspersky.com/about-us/press-center/press-releases/2015/threat-within-3-out-4-companiesaffected-internal-information-s

Kim, H. L., Hovav, A., & Han, J. (2019). Protecting intellectual property from insider threats. *Journal of Intellectual Capital, 21*(2), 181-202.

Klockars, C. B. (1976). *The Professional Fence*. Free Press.

Kohli, R. & Grover, V. (2008). Business value of IT: An essay on expanding research directions to keep up with the times. *Journal of the Association for Information Systems, 9*(1), 24-39.

Koppel, R., Davidson, S. M., Wears, R. L., & Sinsky, C. A. (2012). Health care information technology to the rescue. In R. Koppel & S. Gordon (Eds.), *First, do less harm: Confronting the inconvenient problems of patient safety* (pp. 62-89). Cornell University Press.

KPMG. (2011). *Who is the typical fraudster*. https://www.kpmg.com/CEE/en/IssuesAndInsights/ArticlesPublications/Documents/who-is-the-typical-fraudster.pdf

LaBeff, E. E., Clark, R. E., Haines, V. J., & Diekhoff, G. M. (1990). Situational ethics and college cheating. *Sociological Inquiry, 60*(2), 190-198.

Li, H., Zhang, J., & Sarathy, R. (2010). Understanding compliance with internet use policy from the perspective of rational choice theory. *Decision Support Systems, 48*(4), 635-645.

Lyons, C. J. (2008). Individual perceptions and the social construction of hate crimes: A factorial survey. *Social Science Journal, 45*(1), 107-131.

Malhotra, N. K., Kim, S. S., & Agarwal, J. (2004). Internet users' information privacy concerns (IUIPC): The construct, the scale, and a causal model. *Information Systems Research, 15*(4), 336-355.

Maruna, S. & Copes, H. (2005). What have we learned from five decades of neutralization research? *Crime and Justice, 32*, 221-320.

Matza, D. (1964). *Delinquency and drift: From the research program of the center for the study of law and society*. Transaction Publishers.

Minor, W. (1981). Techniques of neutralization: A reconceptualization and empirical examination. *Journal of Research in Crime & Delinquency, 18*(2), 295-318.

Nagin, D. S. & Pogarsky, G. (2001). Integrating celerity, impulsivity, and extralegal sanction threats into a model of general deterrence: Theory and evidence. *Criminology, 39*(4), 865-892.

Ngai, E. W. T., Hu, Y., Wong, Y. H., Chen, Y., & Sun, X. (2011). The application of data mining techniques in financial fraud detection: A classification framework and an academic review of literature. *Decision Support Systems, 50*(3), 559-569.

O'Fallon, M. J. & Butterfield, K. D. (2005). A review of the empirical ethical decision-making literature: 1996-2003. *Journal of Business Ethics, 59*(4), 375-413.

Ormond, D., Warkentin, M., & Crossler, R. E. (2019). Integrating cognition with an affective lens to better understand information security policy compliance. *Journal of the Association for Information Systems, 20*(12), 1794-1843.

Pahnila, S., Siponen, M., & Mahmood, A. (2007). *Employees' behavior towards IS security policy compliance.* Paper presented at the 40th Annual Hawaii International Conference on System Sciences.

Parker, D. B. (1998). *Fighting computer crime: A new framework for protecting information*. Wiley.

Peace, A. G., Galletta, D. F., & Thong, J. Y. L. (2003). Software piracy in the workplace: A model and empirical test. *Journal of Management Information Systems, 20*(1), 153-177.

Piquero, N. L., Tibbetts, S. G., & Blankenship, M. B. (2005). Examining the role of differential association and techniques of neutralization in explaining corporate crime. *Deviant Behavior, 26*(2), 159-188.

Pogarsky, G. (2002). Identifying "deterrable" offenders: Implications for research on deterrence. *Justice Quarterly, 19*(3), 431-452.

PricewaterhouseCoopers. (2014). *Managing cyber risks in an interconnected world: Key findings from The Global State of Information Security® Survey 2015*. https://www.pwc.com/gx/en/consulting-services/information-security-survey/assets/the-global-state-of-information-security-survey-2015.pdf, 1-42.

Priest, T. B. & McGrath, J. H. (1970). Techniques of neutralization: Young adult marijuana smokers. *Criminology, 8*(2), 185-194.

Protiviti. (2012). *2012 Sarbanes-Oxley Compliance Survey*. https://www.protiviti.com/sites/default/files/united_states/insights/2012-sox-compliance-survey-protiviti.pdf.

Puhakainen, P. (2006). *A design theory for information security awareness* (Unpublished dissertation), University of Oulu, Oulu, Finland.

Raddatz, N. I., Marett, K., & Trinkle, B. S. (2020). The impact of awareness of being monitored on computer usage policy compliance: An agency view. *Journal of Information Systems, 34*(1), 135-149.

Renaud, K., Von Solms, B., & Von Solms, R. (2019). How does intellectual capital align with cyber security? *Journal of Intellectual Capital, 20*(5), 621-641.

Rest, J. R. (1986). *Moral development: advances in research and theory*. Praeger.

Robinson, S., Robertson, J., & Curtis, M. (2012). The effects of contextual and wrongdoing attributes on organizational employees' whistleblowing intentions following fraud. *Journal of Business Ethics, 106*(2), 213-227.

Rogers, J. W. & Buffalo, M. D. (1974). Neutralization techniques: Toward a simplified measurement scale. *Pacific Sociological Review, 17*(3), 313-331.

Romney, M. B. & Steinbart, P. J. (2015). *Accounting information systems* (13th ed.). Pearson Education, Inc.

Rossi, P. H. & Anderson, A. B. (1982). The factorial approach: An introduction. In P. H. Rossi & S. L. Nock (Eds.), *Measuring social judgments: The factorial survey approach*. SAGE.

Rossi, P. H. & Nock, S. L. (1982). *Measuring social judgments: The factorial survey approach*. SAGE.

Salmon, T. M. (2014). Weaknesses in Idaho's information system general controls over its Medicaid claims processing system increase vulnerabilities. *HHS Office of Inspector General*. https://oig.hhs.gov/oas/reports/region9/ 91203009.asp

Salovaara, A. & Merikivi, J. (May 27-29, 2015, 2015). IS research progress would benefit from increased falsification of existing theories. *Proceedings of the European Conference on Information Systems.*

SEC. (2007). Sarbanes-Oxley Section 404: A guide for small business (1-4). https://www.sec.gov/info/smallbus/404guide.pdf

Seddon, P. B. & Scheepers, R. (2012). Towards the improved treatment of generalization of knowledge claims in IS research: Drawing general conclusions from samples. *European Journal of Information Systems, 21*(1), 6-21.

Seddon, P. B. & Scheepers, R. (2015). Generalization in IS research: Critique of the conflicting positions of Lee & Baskerville and Tsang & Williams. *Journal of Information Technology, 30*(1), 30-43.

Sharma, S., & Warkentin, M. (2019), Do I really belong? Impact of employment status on information security policy compliance. *Computers & Security, 87*, 1-12.

Silic, M., Barlow, J. B., & Back, A. (2017). A new perspective on neutralization and deterrence: Predicting shadow IT usage. *Information & Management, 54*(8), 1023-1037.

Siponen, M., Pahnila, S., & Mahmood, A. (2007). Employees' adherence to information security policies: an empirical study, In H. Venter, M. Eloff, L. Labuschagne, J. Eloff, & R. von Solms (Eds.), *New approaches for security, privacy and trust in complex environments* (pp. 133-144). Springer.

Siponen, M. & Vance, A. O. (2010). Neutralization: New Insights into the problem of employee systems security policy violations. *MIS Quarterly, 34*(3), 487-502.

Smallridge, J. L. & Roberts, J. R. (2013). Crime Specific neutralizations: An empirical examination of four types of digital piracy. *International Journal of Cyber Criminology, 7*(2), 125-140.

Stanga, K. G. & Turpen, R. A. (1991). Ethical judgments on selected accounting issues: an empirical study. *Journal of Business Ethics, 10*(10), 739-747.

Straub, D. & Karahanna, E. (1998). Knowledge worker communications and recipient availability: Toward a task closure explanation of media choice. *Organization Science, 9*(2), 160-175.

Straub, D. W. (1990). Effective IS security: An empirical study. *Information Systems Research, 1*(3), 255-276.

Straub, D. W., Carlson, P. J., & Jones, E. H. (1993). Deterring cheating by student programmers: A field experiment in computer security. *Journal of Management Systems, 5*(1), 33-48.

Straub, D. W. & Nance, W. D. (1990). Discovering and disciplining computer abuse in organizations: A field study. *MIS Quarterly, 14*(1), 45-60.

Straub, D. W. & Welke, R. J. (1998). Coping with systems risk: Security planning models for management decision making. *MIS Quarterly, 22*(4), 441-469.

Sutton, S. G. (2006). Enterprise systems and the re-shaping of accounting systems: A call for research. *International Journal of Accounting Information Systems, 7*(1), 1-6.

Sykes, G. M. & Matza, D. (1957). Techniques of neutralization: A theory of delinquency. *American Sociological Review, 22*(6), 664-670.

Taylor, B. J. (2006). Factorial surveys: Using vignettes to study professional judgement. *British Journal of Social Work, 36*(7), 1187-1207.

Thorne, L. (2000). The development of two measures to assess accountants' prescriptive and deliberative moral reasoning. *Behavioral Research in Accounting, 12*, 139-169.

Thorne, L., Massey, D. W., & Magnan, M. (2003). Institutional context and auditors' moral reasoning: A Canada-U.S. comparison. *Journal of Business Ethics, 43*(4), 305-321.

Trinkle, B. S., Crossler, R. E., & Warkentin, M. (2014). I'm game, are you? Reducing real-world security threats by managing employee activity in online social networks. *Journal of Information Systems, 28*(2), 307-327.

Vance, A., Lowry, P. B., & Eggett, D. (2013). Using accountability to reduce access policy violations in information systems. *Journal of Management Information Systems, 29*(4), 263-289.

Vance, A., Lowry, P. B., & Eggett, D. L. (2015). A new approach to the problem of access policy violations: Increasing perceptions of accountability through the user interface. *MIS Quarterly, 39*(2), 345-366.

Warkentin, M., McBride, M., Carter, L., & Johnston, A. (2012). The role of individual characteristics on insider abuse intentions. Proceedings of the Americas Conference on Information Systems.

Warkentin, M., Straub, D., & Malimage, K. (2012). Featured talk: Measuring secure behavior: A research commentary. *Proceedings of the Annual Symposium of Information Assurance & Secure Knowledge Management*.

Warkentin, M., Walden, E. A., Johnston, A. C., & Straub Jr., D. W. (2016). Neural correlates of protection motivation for secure IT behaviors: An fMRI exploration. *Journal of the Association for Information Systems, 17*(3), 194-215.

Warkentin, M. & Willison, R. (2009). Behavioral and policy issues in information systems security: The insider threat. *European Journal of Information Systems, 18*(2), 101105.

Weber, R. (2012). Evaluating and developing theories in the information systems discipline. *Journal of the Association for Information Systems, 13*(1), 2-30.

Whetten, D. A. (1989). What constitutes a theoretical contribution? *Academy of Management Review, 14*(4), 490-495.

Whetten, D. A., Felin, T., & King, B. G. (2009). The practice of theory borrowing in organizational studies: Current issues and future directions. *Journal of Management, 35*(3), 537-563.

Willison, R. & Warkentin, M. (2013). Beyond deterrence: An expanded view of employee computer abuse. *MIS Quarterly, 37*(1), 1-20.

Willison, R., Warkentin, M., & Johnston, A. C. (2018). Examining employee computer abuse intentions: Insights from justice, deterrence, and neutralization perspectives. *Information Systems Journal, 28*(2), 266-293.

Zhang, L., Smith, W. W., & McDowell, W. C. (2009). Examining digital piracy: Self-control, punishment, and self-efficacy. *Information Resources Management Journal, 22*(1), 24-44.

Appendix A: The Auditor Fraud Problem

Corporate fraud, including unethical auditing behavior, poses a significant cost to business, and incidents have been increasing. The average cost of these fraudulent acts has been reported to be $1.2 million (KPMG 2011), whereas the estimated total annual costs are in the billions of dollars (ACFE 2012; Humpherys et al., 2011). The American Institute of Certified Public Accountants (AICPA) has also set standards or Generally Accepted Accounting Principles (GAAP) for the preparation, presentation, and reporting of financial statements. Auditors who verify that these financial statements are in accordance with the GAAP are mandated by the AICPA to follow the Generally Accepted Auditing Standards (GAAS). The AICPA also understands the importance of mitigating unethical auditor behavior by issuing a lengthy ethical policy, which all CPAs sign and which is extensively discussed in all accounting education programs. This should effectively neutralize the effect of the techniques of neutralizations adopted by auditors who violate policy (Maruna & Copes 2005,).

Following several major corporate and accounting scandals—such as Enron, WorldCom, and Tyco International—the Sarbanes-Oxley Act (SOX) (Congress 2002) was enacted, setting strict guidelines for auditors in terms of reviewing financial information accuracy and internal controls. The importance of internal controls and their impact on financial statements are highlighted by SOX, Section 404, which requires that a corporation's management and the external auditors report on the adequacy of the company's internal controls on financial reporting (SEC, 2007): "Internal controls promote efficiency, reduce risk of asset loss, and help ensure the reliability of financial statements and compliance with laws and regulations" (COSO, 1994, p. 3).

Since SOX was enacted, the internal controls of corporations have improved significantly (Protiviti, 2012), although concerns remain regarding the adequacy of the improvements. Internal controls, when properly implemented, should reduce the likelihood that employees commit fraudulent activities that go unnoticed. However, according to the 2012 Report to the Nations on Occupational Fraud and Abuse (ACFE 2012), only 1.1% of occupational fraud was detected through IT controls and only 3.3% was detected by external auditors. Interestingly, tips or whistleblowers were responsible for the detection of 43.3% of occupational fraud incidents in 2012 (ACFE 2012). Recent research also suggests that 74% of fraudsters committed their fraudulent acts through the exploitation of weak internal controls (KPMG 2011). These findings indicate that the IT controls and external auditors have generally failed to detect potential red flags that may indicate fraudulent activities. This also suggests that external auditors have not sufficiently reviewed the efficiency of the IT controls or have overlooked potential IT control deficiencies for various reasons instead of bringing it to the attention of the management in writing.

Auditors must make decisions at the nexus of the internal and external environment; they work for an auditing firm (with its own unique profile of influences on auditors' decisions), but they also make decisions that directly affect the firms they audit. At the heart of the influences over their decisions is the immediate workplace, however, including explicit or implicit pressures by their managers. There is a plethora of research related to occupational fraud and on how to detect these cases of fraud at an early stage (Goode & Lacey 2011; Huang et al., 2008; Humpherys et al., 2011; Ngai et al., 2011). External auditors have come under scrutiny since the Enron scandal and regulations such as SOX have set strict guidelines for them to follow. Though it is important to identify why employees commit fraudulent acts in their organizations, it is also important to identify why auditors commit unethical acts. In fact, it is of paramount importance to address this critical threat to the validity of corporate financial information, given the unique role that auditors play. In one of the most publicized accounting scandals in history, WorldCom executives were found to have used fraudulent accounting practices between 1999 and 2002 to alter strategic information for the purpose of disguising its mounting losses. Arthur Andersen LLP was the firm's auditing firm. During the ensuing trial, it was discovered that a key working paper was substantially altered to hide Andersen's knowledge that WorldCom had improperly capitalized expenses as early as 1999 (Barrack, 2005). The reasons that led one of the Big Five auditing companies to modify working papers to hide irregularities remain unclear. Similar incidents in which intentional noncompliance of auditing standards and other fraudulent acts committed by auditors have come into light in the last few years and are likely to materialize in the coming years as well. The causes prevail as a critical research question; indeed Sutton (2006) and others have called for more practical research into this phenomenon. However, empirical research investigating the antecedents that lead auditors to commit fraudulent acts does not exist.

Appendix B: Sample Instrument

Instrument shell: In addition to varying the orthogonal representation of each research construct, we also varied other terms to reduce various forms of potential bias. All such items that vary are enclosed in brackets. The underlined items are the factors for the factorial survey method (orthogonally distinct) and are underlined for emphasis to help participants identify the item statements that vary from scenario version to scenario version.

[Auditor Name] and the [Client Name]

[Auditor Name] is a senior auditor and a CPA for a national CPA firm that provides audit, tax, and consulting services for multiple clients. [Auditor Name] is the auditor in charge of the fieldwork on the [Client Name] audit. ([Client Name] is a publicly traded longstanding client of the firm and receives both audit and tax services). Another longstanding publicly-traded client is [Software Company Long Name], which has developed a software package called the [Software Company Name Short Name] Accounting Information System (AIS) which is licensed to the general public as well as some of the firm's clients, including [Client Name]. The [Software Company Name Short Name] AIS is a popular system and [Client Name] recently issued a press release that they were adopting this system. During the course of this audit assignment, [Auditor Name] is asked to evaluate the information systems general controls of the accounting information system which happens to be the [Software Company Name Short Name] AIS.

After testing the controls for the inventory impairment computer application, [Auditor Name] uncovers an information technology weakness in the [Software Company Name Short Name] AIS system which may introduce IT security vulnerabilities. [Auditor Name] believes that these security-oriented control deficiencies are significant and therefore, material. After reviewing the working papers for the information technology general controls portion of the audit, [Auditor Name]'s supervisor told him to [Degree of Violation Statement]. [Auditor Name] [Technique of Neutralization Statement]. [Auditor Name] [Deterrence Theory Statement].

Table B1. Factors and their Respective Items (Variables)

Factor	Manipulation
Techniques of neutralization	
Denial of responsibility	Believes that since his supervisor told him to modify the report, he has no control over the decision
Denial of injury	Believes that no one would be harmed by modifying the report
Defense of necessity	Believes that if she does not modify the report, his firm will lose [client name] as a client
Appeal to higher loyalties	Believes that modifying the report would not be as bad as modifying the financial statement numbers
Metaphor of the ledger	Believes that all her past reports were appropriate, so it would be OK to modify the report just this one time
(No technique of neutralization)	This item would not have been in the scenario.
Deterrence theory	
Low sanction certainty, with low sanction severity	Believes that his chances of being caught are low, but if caught, the punishment would be minimal
Low sanction certainty, with high sanction severity	Believes that her chances of being caught are low, but if caught, the punishment would be severe
High sanction certainty, with low sanction severity	Believes that his chances of being caught are high, and if caught, the punishment would be minimal
High sanction certainty, with high sanction severity	Believes that her chances of being caught are high, and if caught, the punishment would be severe
Degree of violation	
Degree of violation: high	Remove all of the references to control deficiencies regarding the [software co. Name] AIS package from the report
Degree of violation: low	Minimize the references to control deficiencies regarding the [software co. Name] AIS package from the report

Appendix C: Sample Instrument

Varied items randomly populated (conditions for this sample instrument = technique of neutralization: defense of necessity; deterrence level: high sanction certainty, with high sanction severity; degree of violation: high):

Joe and Creative Corp

Joe is a senior auditor and a CPA for a national CPA firm that provides audit, tax, and consulting services for multiple clients. Joe is the auditor in charge of the fieldwork on the Creative Corp audit. (Creative Corp is a publicly traded longstanding client of the firm and receives both audit and tax services). Another longstanding publicly traded client is Triple Point Enterprises, which has developed a software package called the Triple Point Accounting Information System (AIS) which is licensed to the general public as well as some of the firm's clients, including Creative Corp. The Triple Point AIS is a popular system and Creative Corp recently issued a press release that they were adopting this system. During this audit assignment, Joe is asked to evaluate the information systems general controls of the accounting information system which happens to be the Triple Point AIS.

After testing the controls for the inventory impairment computer application, Joe uncovers an information technology weakness in the Triple Point AIS system which may introduce IT security vulnerabilities. Joe believes that these security-oriented control deficiencies are significant and therefore, material. After reviewing the working papers for the information technology general controls portion of the audit, Joe's supervisor told him to remove all of the references to control deficiencies regarding the Triple Point AIS package from the working papers. Joe believes that if he does not modify the report, his firm will lose Triple Point Enterprises as their client. Joe believes that his chances of being caught are high, and if caught, the punishment would be severe.

It is stated in the scenario that Joe is told by his supervisor to:

_____ remove all of the references to control deficiencies regarding the Triple Point AIS package from the working papers

_____ minimize the references to control deficiencies regarding the Triple Point AIS package from the working papers.

If you were Joe, what is the likelihood that you might follow the supervisor's instructions and modify the working papers?

Unlikely to modify the working papers		Unsure		Likely to modify the working papers
1	**2**	**3**	**4**	**5**

What is the likelihood that other auditors in Joe's situation might follow the supervisor's instructions and modify the working papers?

Unlikely to modify the working papers		Unsure		Likely to modify the working papers
1	**2**	**3**	**4**	**5**

Please tell us a little about yourself. Remember that you are completely anonymous.

Your Gender:

Male Female

Your Age:

18-21 22-29 30-39 40-49 50-59 60+

Did you have an internship? Yes No

*** Please note that the student's university status as a graduate or undergraduate student was not queried in the instrument. We obtained this information by directing the participants to separate instruments for graduate students and undergraduate students.

Appendix D: Sensitivity Analysis of the Individual Items Composing the Dependent Variable

Table D1. Panel A: USING logDV1: Mixed Model Analysis Results for the Individual Impact of Magnitude of Alteration, Techniques of Neutralization, and Deterrence Theory on an Auditor's Behavioral Intention to Violate Policy

	Predicted sign	Beta	Z
(Constant)	n/a	0.81	8.13*
TN1	+	0.10	1.06
TN2	+	-0.05	-0.71
TN3	+	0.03	0.42
TN4	+	0.05	0.64
TN5	+	-0.06	-0.86
DT2	-	-0.23	-3.43*
DT3	-	-0.22	-3.20*
DT4	-	-0.49	-7.72*
RM1	-	-0.10	-1.83
Grad	-	-0.03	-0.28
Gender	n/a	0.02	0.18
Internship	-	0.06	0.59

Note:
N = 304, R^2 = 0.16, *Significant at the 0.001 level
TN1 = Denial of responsibility, TN2 = Denial of injury, TN3 = Defense of necessity, TN4 = Appeal to higher loyalties,
TN5 = Metaphor of the ledger
DT2 = Sanction certainty is low and sanction severity is high, DT3 = Sanction certainty is high and sanction severity is low
DT4 = Sanction certainty is high and sanction severity is high,
RM1 = Degree of Violation where 1 = remove all of the references and 0 = minimized all references
Grad = Dummy variable where 1 = graduate student and 0 = undergraduate student, Gender = Dummy variable where 1 = male and 0 = female
Internship = Dummy variable where 1 = participated in an internship and 0 = did not participate in an internship

Table D2. Panel B: USING DV2: Mixed Model Analysis Results for the Individual Impact of Magnitude of Alteration, Techniques of Neutralization, and Deterrence Theory on an Auditor's Behavioral Intention to Violate policy

	Predicted sign	Beta	Z
(Constant)	n/a	3.83	19.31**
TN1	+	0.33	1.84
TN2	+	0.02	0.14
TN3	+	0.21	1.30
TN4	+	0.14	1.02
TN5	+	0.03	0.22
DT2	-	-0.58	-3.79**
DT3	-	-0.40	-3.11*
DT4	-	-1.11	-7.93**
RM1	-	-0.07	-0.56
Grad	-	-0.11	-0.52
Gender	n/a	-0.19	-1.06
Internship	-	0.26	1.34

Note:N = 304, R^2 = 0.16, * Significant at the 0.01 level ** Significant at the 0.001 level
TN1 = Denial of responsibility, TN2 = Denial of injury, TN3 = Defense of necessity, TN4 = Appeal to higher loyalties
TN5 = Metaphor of the ledger
DT2 = Sanction certainty is low and sanction severity is high, DT3 = Sanction certainty is high and sanction severity is low
DT4 = Sanction certainty is high and sanction severity is high,
RM1 = Degree of Violation where 1 = remove all of the references and 0 = minimized all references
Grad = Dummy variable where 1 = graduate student and 0 = undergraduate student, Gender = Dummy variable where 1 = male and 0 = female
Internship = Dummy variable where 1 = participated in an internship and 0 = did not participate in an internship

About the Authors

Bradley S. Trinkle is the H. Devon Graham Professor in Accounting in the Richard C. Adkerson School of Accountancy at Mississippi State University. His research primarily focuses on information security and the impact of financial disclosures via social media on nonprofessional investors. Brad's research has appeared in the *Journal of Information Systems*, *International Journal of Accounting Information Systems*, and others. He is an associate editor for the *Journal of Intellectual Capital* and a member of the advisory/review board for the *Journal of Information Systems.*

Merrill Warkentin is a William L. Giles Distinguished Professor at Mississippi State University, where he serves as the James J. Rouse Endowed Professor of Information Systems. He was named an ACM Distinguished Scientist in 2018. His research, primarily on the organizational, contextual, and dispositional influences on individual behaviors in the contexts of information security, privacy, and social media has appeared in *MIS Quarterly*, *Journal of MIS*, *Journal of the Association for Information Systems*, *European Journal of Information Systems*, *Information Systems Journal*, *Information & Management*, *Decision Sciences*, and others. Dr. Warkentin is the author or editor of seven books and has co-authored over 100 peer-reviewed journal articles. He is the editor-in-chief of the *Journal of Intellectual Capital* and serves or has served in editorial roles for *MIS Quarterly*, *Information Systems Research*, *Journal of the Association for Information Systems*, *Decision Sciences*, *European Journal of Information Systems*, *Information & Management*, and other journals. He has held officer and other leadership positions at the AIS, DSI, IFIP, and ACM. His work has been funded by NSF, NATO, NSA, DoD, Homeland Security, IBM, and others.

Kalana Malimage is an assistant professor of accounting at Florida Gulf Coast University. His research interests include information security and privacy, accounting information systems, fraud examination, forensic accounting, and auditing. His prior research has appeared in *Journal of Information Systems* and *Journal of Forensic and Investigation Accounting*.

Nirmalee Raddatz is an assistant professor of accounting at the University of Memphis. She holds a PhD in management information systems and a master's in taxation from Mississippi State University. Her primary research interests include behavioral research in accounting and information systems that mainly focuses on fintech, cybersecurity, blockchain technology, and artificial intelligence. Her work has appeared in *Journal of Information Systems* and *Journal of Information Systems Security.*