Communications of the Association for Information Systems

Volume 55 Paper 1

7-27-2024

Explanations of Insider Deviant Behavior in Information Security: A Systematic Literature Review

Emmanuel Anti
University of Vaasa

Tero Vartiainen
University of Vaasa

Recommended Citation
Anti, E., & Vartiainen, T. (2024). Explanations of Insider Deviant Behavior in Information Security: A Systematic Literature Review. Communications of the Association for Information Systems, 55, 1-36. https://doi.org/10.17705/1CAIS.05501

Explanations of Insider Deviant Behavior in Information Security: A Systematic Literature Review

Cover Page Footnote

This manuscript underwent peer review. It was received 01/24/2024 and was with the authors for five months for two revisions. Stephen McCarthy served as Associate Editor.

Communications of the Association for Information Systems

Research Article DOI: 10.17705/1CAIS.05501 ISSN: 1529-3181

Explanations of Insider Deviant Behavior in Information Security: A Systematic Literature Review

Emmanuel Anti
School of Technology and Innovations
University of Vaasa
0009-0007-3802-4875

Tero Vartiainen
School of Technology and Innovations
University of Vaasa
0000-0003-3843-8561

Abstract:

Insider deviant behavior (IDB) in information security (IS) poses significant threats to public and private organizations. To enhance our understanding of IDB, we conducted a systematic review of existing literature, analyzing theories from the fields of criminology (e.g., Deterrence Theory), sociology (e.g., Social Control Theory), and psychology (e.g., Neutralization Techniques) utilized in IS research on IDB. We identified 46 theories from these disciplines, which we categorized into four main groups: psychological and behavioral, organizational, sociocultural, and decision-making. Additionally, we classified their constructs into eight key factors. Further, ten IDBs frequently studied in IS were identified. Our analysis identified relationships among these theories emphasizing shared concepts that improve our comprehension of IDB. These relationships and their implications for theory and practice are discussed offering insights into the multifaceted nature of insider deviance and the diverse theoretical lenses through which they can be examined. This review not only consolidates existing knowledge but also lays the groundwork for future research in effectively addressing insider deviant behavior.

Keywords: Insider Deviant Behavior, Systematic Literature Review, Information Security, Theories.

This manuscript underwent peer review. It was received 01/24/2024 and was with the authors for five months for two revisions. Stephen McCarthy served as Associate Editor.

1 Introduction

Insider threats are a complex and ongoing concern for public and private sector organizations. Insider threats immensely affect organizations, regardless of whether their acts are intentional or negligent (Jones & Colwill, 2008). While the risks posed by insider threats are widely recognized in business and academia, insider threat strategies are becoming more sophisticated due to the complex nature of human behavior and the motivations behind their attacks on organizational defenses. Cybersecurity Insiders (2023) estimates that 74% of organizations acknowledge being vulnerable to insider threats, an 8% increase since 2022. Furthermore, 74% of organizations reported an increase in insider attacks, up from 68% in 2021. Insider attacks cause critical data loss, brand damage, financial losses, and organizational operational disruptions. With such significant implications for organizations, external threats dominate attack headlines, while incidents involving insiders are frequently underreported. There is a solid case to be made that focusing on insider threats may divert attention away from external threats, which are common and equally damaging; however, organizations must recognize that both insider and external threats are significant security concerns and must be addressed effectively.

Insiders are trusted individuals within an organization who have the authority to violate one or more security policy rules and thus pose a severe threat to information security due to their intimate knowledge of an organization's internal operations, processes, data, systems, or other resources (Green, 2014; Steele & Wargo, 2007). According to IBM Security and the Ponemon Institute (2023), the average data breach cost reached an all-time high of USD 4.45 million in 2023, representing a 2.3% increase over the 2022 cost of USD 4.35 million. The report further indicates that identifying and resolving breaches initiated by malicious insiders took about ten months (308 days). The time it took to identify and resolve incidents involving insiders, as reported by IBM Security and the Ponemon Institute (2023), demonstrates how organizations struggle to deal with insider threats, which supports Steele and Wargo's (2007) assertion that unlike the external threat actor, the employee or insider is challenging to identify, monitor, and protect against.

Robinson and Bennett (1995) define workplace deviance as any deliberate act that contravenes essential organizational norms and threatens the welfare of an organization, its members, or both. Insider actions in information and cybersecurity like Computer abuse (Harrington, 1996; Straub & Nance, 1990), IS Misuse (D'Arcy et al., 2009; Hovav & D'Arcy, 2012), Intention to Violate ISSP (Siponen & Vance, 2010; Vance & Siponen, 2012) to name a few, are considered insider deviant behaviors (IDBs) that violate norms and negatively impact the welfare of an organization and its members. Understanding insider motivations that trigger such behaviors is critical in dealing with insider threats, according to (Hunker & Probst, 2011)because it allows organizations to identify potential risk factors and indicators of malicious intent. Performance issues, discontent, contempt for authority, disengagement, and anger management can all impact such intentions. Furthermore, Hunker and Probst (2011) emphasize the importance of understanding that not all insider threats are malicious or intentional, as some insiders may cause harm inadvertently due to a lack of knowledge, carelessness, or manipulation by external threats. For example, an employee may leave their computer unattended while signed in, unintentionally download malware, or be duped into disclosing sensitive information using social engineering techniques such as phishing.

To better understand IDBs' motivations and intentions, information and cybersecurity researchers have adapted theories from criminology, for example, Deterrence Theory (Beccaria, 1963; Gibbs, 1968), from sociology for example Social Control Theory (Agnew, 1991), and psychology, for example, Neutralization Techniques (Gresham & David, 1957). The use of these theories in information and cybersecurity research reflects the need to understand IDB from various points of view due to this phenomenon's complex and multifaceted nature. These theories are grounded in empirical research which serves as a foundation for formulating hypotheses, conducting research, and deriving practical implications to address insider threats. The landscape of information security is constantly evolving and the adaptability of these theories allows researchers to address novel challenges. The ability to adapt is crucial for effectively addressing the ever-changing strategies used by insiders within an organization.

Though technical solutions can detect suspicious activity or unauthorized access they may not account for the human component. Technological solutions cannot determine whether an insider is behaving intentionally or unintentionally. People can exploit weaknesses, circumvent security safeguards, or abuse legitimate access for nefarious purposes. Therefore, adapting theories from other disciplines may help explain how situations influence human decisions, beliefs, and attitudes and test how various incentives affect people's motivation and behavior in information and cybersecurity contexts. Several psychological,

sociological, and criminological theories have been applied to study IDBs, including theories of deterrence, rational choice, motivational, strain, and situational theories. These theories focus on factors contributing to insider behaviors, such as observation and modeling, personality traits, personal gain, revenge, boredom, strain, and situational and environmental factors. Though all these theories explain why insiders behave in deviant ways, the theories used may reveal some factors unique to individuals, organizations, or both that cause deviant behaviors and provide different explanations.

In this study, we aim to advance the study of IDB by identifying the various theories used in IS research on IDB, analyzing their constructs, finding out what explanation they give for IDB, and identifying knowledge gaps and future research. This study will conduct a literature review on the theories used in behavioral research in information and cybersecurity that have been adapted from psychology, sociology, and criminology and will contribute to a better understanding of how these theories explain the motivations and intentions that encourage IDB in the information and cybersecurity spheres. As a result, we proposed the following research question:

RQ: How do psychological, sociological, and criminological theories explain insider deviant behavior in information security?

This study is organized as follows: Section 2 provides background information on insider deviant behaviors (IDBs). Section 3 describes the methodology for conducting the literature review, Section 4 presents the findings, Section 5 describes the synthesis, and Sections 6 and 7 present the discussions and conclusion.

2 Literature on Insiders and Deviant Behaviors

2.1 Who is an Insider

Insiders are defined by Brackney and Anderson (2004) as anyone who has access to, privilege over, or knowledge of information systems and services. Bishop and Gates (2008) expand the definition of an insider in terms of two abilities: breaking security policies through allowed access and violating access control policies through illegal access. The definitions above indicate how insiders can use their privileged access to intentionally or unintentionally cause harm to an organization and its assets.

The insider is a member of an organization with legitimate authorization and can harm an organization's information systems' confidentiality, integrity, and availability through intentional or unintentional acts (Warkentin & Willison, 2009). Insiders are critical to every organization because they are trusted to use their access privileges appropriately by ensuring that organization information is not disclosed and that they follow the rules and policies that have been established within the organization. According to Crossler et al. (2013) and Warkentin and Willison (2009), insider actions that pose direct or indirect threats to organizational digital assets can be divided into two categories: those that are intentional, such as sabotage, stealing, and industrial or political espionage, and unintentional, such as selecting a simple password, visiting non-work related websites using corporate computers, and inadvertently posting confidential data onto unsecured networks.

2.2 Deviant Behavior

Humphrey and Palmer (2013) define deviant behavior as "behavior that does not conform to norms and rules" (2013, p. 3). According to Robinson and Bennett (1995), employee deviance involves deliberate actions that violate important organizational norms and jeopardize the organization's security or safety. Theft, fraud, lying, vandalism, unauthorized leaks, and aggressive behavior are examples of such deviance. The definitions of deviant behavior by (Humphrey & Palmer, 2013; Robinson & Bennett, 1995) consider only the physical action and exclude the cognitive aspect. For example, expressing one's thoughts requires both physical and cognitive actions. Individuals who express religious, political, or scientific beliefs that do not conform to social norms may be considered deviants. We argue in this study that deviant behavior is a combination of voluntary cognitive and physical actions because the decision to act deviantly begins with an individual thinking about, planning, and carrying out the intended act. Therefore, we define deviant behavior as *a voluntary physical or mental process contravening a social group or organization's norms, policies, or rules with negative or positive consequences.* For example, when an individual uses technical means to disrupt or compromise an organization's business operations, they go through a mental and physical process of analyzing the organizational system, identifying the weaknesses, planning the attack, carrying it out, and finding justification or rationalizations for their actions. Physical processes include installing malicious software, theft of hardware, and unauthorized copying of sensitive data. Individuals may

act for financial gains or revenge as positive outcomes based on self-interest, utilitarian, or ethical reasons. For organizations, insider deviance can lead to positive outcomes, such as knowing the vulnerabilities in their security systems and policies and finding mitigation strategies. The example emphasizes that deviant behavior, whether intentional or unintentional, includes both physical and cognitive actions and that the act can have both negative and positive consequences for the actor or the organization. Insiders within an organization are often considered trusted individuals due to their legitimate access to facilities and information, as well as their knowledge of the organization and the location of valuable assets (Colwill, 2009) and their actions can have either positive or negative consequences on an organization. In our study, IDB in information and cybersecurity refers to *"trusted individuals within an organization who intentionally or unintentionally violate norms, policies, or rules through cognitive and physical processes to achieve outcomes, whether negative or positive, for themselves or the organization."*

3 Systematic Literature Review

Watson and Webster (2020) emphasize the significance of literature reviews in academic research by stating that reviewing prior, relevant literature is essential to any academic project. Further, an effective review establishes a solid foundation for advancing knowledge by facilitating theory development, closing research gaps, and uncovering research gaps. Schryen (2015) adds that a literature review critically assesses and summarizes the existing body of knowledge in a given field and serves as a foundation for identifying weaknesses and poorly understood phenomena in the existing literature, enabling problematization of assumptions and theoretical claims in the existing body of knowledge, and helps scholars avoid 'reinventing the wheel' and allows for the conduct of gradual research by building on what other researchers have done. Watson and Webster (2020) also contend that the literature review serves as the foundation for research in the Information Systems (IS) field and that review articles are critical to advancing IS as a field of study. We followed the Preferred Reporting Items for Systematic Reviews and Meta-Analysis (PRISMA) guidelines to answer our research question (Page et al., 2021). Following the PRISMA guidelines, we identified relevant articles, selected articles based on eligibility criteria (screening), extracted the data from the selected articles, and synthesized the data.

3.1 Identification of Articles

We developed inclusion and exclusion criteria to identify papers relevant to our studies. The criteria we devised include papers written in English, peer-reviewed papers, completed research papers, papers emphasizing information security, papers that applied criminological, sociological, and psychological theories from 1990 to 2023, papers that analyzed employee or IDB, and empirical papers. We excluded short papers, commentaries, opinion pieces, papers that focused on technical aspects of insider threats, and papers that focused on external threats in information and cybersecurity.

We selected papers published in high-level IS journals and conferences. We selected journals from the Basket of 8 that AIS senior scholars highly recommend. European Journal of Information Systems (EJIS), Information Systems Journal (ISJ), Information Systems Research (ISR), Journal of Association of Information Systems (JAIS), Management Information Systems Quarterly (MISQ), and Journal of Management Information Systems (JMIS) were among the journals searched. We also looked for papers in journals such as Elsevier and Emerald. We then looked at papers from IS conference proceedings like ECIS, ICIS, HICSS, AMCIS, and other databases with studies relevant to our research. While the IS journals and conferences provided valuable insights, we recognized the need for a comprehensive approach. We then extended our search to broader databases, including Scopus and Web of Science as they cover a wide range of disciplines, ensuring that we capture relevant studies beyond the scope of specialized journals

Additionally, Google Scholar was used to ensure no relevant papers were missed during our initial search in specialized databases and to cross-validate the results obtained from the examined databases. The search string we devised for finding relevant papers included the following keywords:

("Insider" OR "Employee") AND ("IS Misuse" OR "Intention to violate ISSP" OR "IS non-compliance" OR "Computer Abuse")

In our search strategy, we used both "IS" and "Information Security" to ensure a comprehensive literature review. This approach allowed us to capture a wide range of studies examining insider deviant behavior from both system and security perspectives. We further incorporated 'cybersecurity' into our search criteria, but most literature focused on technical and external threats, while theoretical papers mainly addressed

general management decisions rather than insider or employee perspectives. To maintain specificity, we opted to focus on information security.

3.2 Selection of Articles

We selected and screened 448 articles in total. First, we began by scanning the abstracts and titles of the articles. We checked to see if our inclusion criteria, such as topic, language, and year, were met. For example, we perused whether the title or abstract contained keywords like insider or employee, information security, or theory. Many of the studies did not meet our criteria. We also discovered studies that included our keywords, such as insider threat, insider security, or employees but were focused on technical solutions for insider threats.

Second, we reviewed the articles by reading the full text and determining their eligibility. We then removed duplicates and excluded some papers because they were conceptual rather than empirical. The abstract screening did not indicate they were conceptual, and it took a full paper reading to establish it. We eventually included 86 articles in our analysis based on our eligibility criteria. These articles were selected because they were relevant to our research. Our selection process is presented in Figure 1.

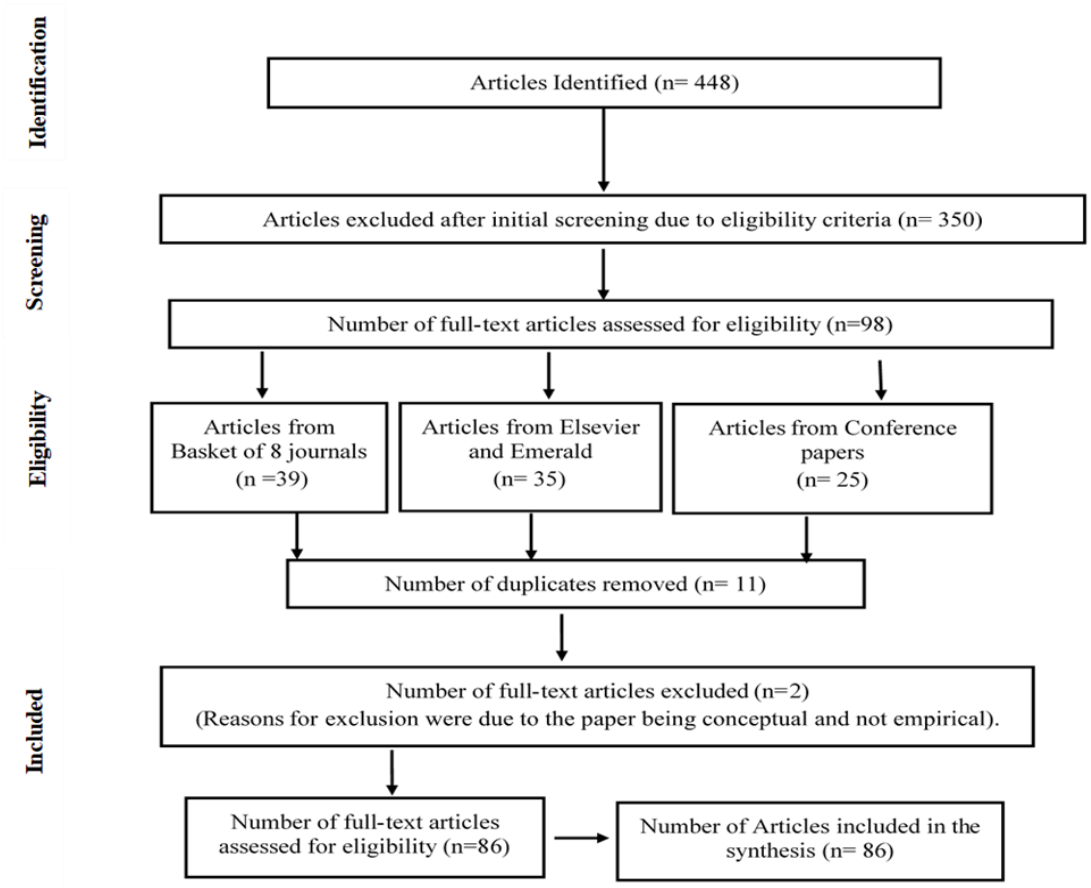

Figure 1. Prisma Flowchart Diagram

4 Data Extraction

We devised a data extraction form using an inductive approach to collect attributes from each article, collate, and summarize the relevant answers to our research question. We extracted attributes such as author(s), title, journal/conference, year of publication, theories, keywords, research method, variables studied, research aim(s), research question(s), and summary of findings. The attributes collected are presented in Table 1.

Table 1. Data Attributes Collected

Attributes	Description of Attribute
Author(s)	The name(s) of the persons who authored the article(s)
Title	The title of the study
Journal/Conference	The name of the publication venue
Year of Publication	The year the article was published.
Theories	The theories applied in the study
Keywords	Given the keywords of the study
Research method	Methods applied in the study
Variables studied	The phenomenon being measured or studied.
Research aim(s)	The goal or idea of the study
Research question(s)	The questions that were answered in the study
Summary of findings	The results from the study

Both authors analyzed and coded the articles to ensure that the process was rigorous and that divergent opinions were addressed and agreed upon. Our discussions took place in a hybrid format (in-person meetings and online via Teams or Zoom). We focused on identifying theories and their components and discussing how they have been applied in IS to study IDB to ensure they adequately address our research question.

5 Data Synthesis

We compiled the theories and their constructs and compared them to IS studies to see how they explain IDB in information security. The theories identified were classified into four categories. Further, the constructs of the theories were also classified into eight categories that explain the motivations and intentions behind IDB in information security settings. Finally, the findings were synthesized.

5.1 Findings

We identified 46 theories adapted from sociology, criminology, and psychology in our SLR that have been applied to study IDB in information security. We then classified these theories into four categories: psychological and behavioral, organizational, sociocultural, and decision-making. The constructs of the theories were also classified into eight factors: psychological factors, organizational factors, situational and environmental factors, sociocultural factors, coping and emotional factors, information processing and technology factors, ethical and value-based factors, and socioeconomic factors. Table 2 shows the classifications of the theories.

Table 2. Classification of the Theories

Psychological and Behavioral	Organizational	Sociocultural	Decision-Making
Fear Appeal (Rogers, 1975; Rogers & Deckner, 1975) **Rational Choice Theory** (Hogarth & Reder, 1987) **Fraud Triangle Theory** (Albrecht et al., 1984, 2008) **Routine Activity Theory** (Cohen & Felson, 1979) **Situational Action Theory (SAT)** (Wikström, 2014; Wikström et al., 2017) **Expectancy Theory** (Vroom, 2005) **Social Cognitive Theory** (Bandura, 1988) **Protection Motivation Theory** (Rogers, 1983; Rogers & Prentice-Dunn, 1997) **Deterrence Theory** (Beccaria, 1963; Gibbs, 1968) **Theory of Reasoned Action** (Fishbein, 1979) **Theory of Cognitive Moral Development** (Kohlberg, 1963, 1971) **Theory of Motivational Types of Values** (Schwartz, 1992) **Neutralization Theory** (Gresham & David, 1957; Sykes & Matza, 2017) **Reactance Theory** (Brehm & Brehm, 2013) **Social Information Processing Theory (SIPT)** (Salancik & Pfeffer, 1978) **Dispositional and Situational Factors** (Digman, 1997)	**High-Performance Work Systems (HPWS) Theory** (Boxall & Macky, 2009) **Theory of Structural Empowerment** (R. Kanter, 1993; R. M. Kanter, 1977, 2008) **Opportunity Structure for Crime Model** (Dijk, 1994) **Fairness Theory (FT)** (Folger & Cropanzano, 2001) **Transactional Model of Stress and Coping** (Lazarus & Folkman, 1984) **Theory of Planned Behavior** (Ajzen, 1991) **Organizational Justice Theory** (Greenberg, 1987) **Boundary Management Theory** (Ashforth et al., 2000) **Framework of Emotions** (Beaudry & Pinsonneault, 2010) **Self-Determination Theory (SDT)** (Ryan & Deci, 2000) **Agency Theory** (Milgram, 1963, 1974) (Boal & Cummings, 1981) **Organizational Citizenship Behavior** (D. Katz, 1964; Organ, 1988, 2014) **Organizational control theory (OCT)-** (Eisenhardt, 1985; Ouchi, 1979)	**Hofstede's Cultural Dimensions** (Hofstede, 1984; Hofstede & McCrae, 2004) **Social Control Theory** (Agnew, 1991; Hirschi, 1969, 2017) **Social Action Theory (SAT)** (Weber, 1978, 1991) **Value-Based Compliance (VBC)** (Karlsson & Hedström, 2019) **Activity Theory (AT)** (Kuutti, 1996) **Justice Theory** (Rawls, 1971)	**Technology Acceptance Model (TAM)** (Davis, 1989; Davis et al., 1989) **Goal Framing Theory** (Lindenberg & Steg, 2007) **General Strain Theory** (Agnew, 1992) **Coping Theory** (Lazarus & Folkman, 1984) **Affective Events Theory (AET)** (Weiss & Cropanzano, 1996) **Prospect Theory** (Kahneman, 1979; Kahneman & Tversky, 2013) **Theory of Accountability** (Tetlock, 1983) **Moral Disengagement Theory** (Bandura, 1999) **Appraisal Theory** (Dewe, 1991; Lazarus, 1991; Scherer et al., 2001) **Cognitive Evaluation Theory (CET)** (Boal & Cummings, 1981) **Self-Efficacy Theory** (Bandura, 1977; Bandura & Wessels, 1994)

Further, the IS-studied deviant behaviors we found are as follows: computer abuse, computer fraud, IS security compliance and non-compliance, IS misuse, IS security policy violations (malicious and non-malicious), shadow IT, unauthorized disclosure, computer crime, IS security abuse, and access policy violations. Table 3 presents the deviant behaviors identified.

Table 3. Insider Deviant Behaviors in IS Studies

Deviant Behaviors	Definitions
Computer Abuse	Computer abuse refers to the unauthorized, deliberate, and internally identifiable misuse of assets within an organization's information system, including hardware, programs, data, and services (Straub & Nance, 1990).
Computer Fraud	Computer fraud involves unauthorized access to computers, manipulation of systems, data alteration, unauthorized resource use, and financial fraud, causing loss and harm to others (Griffith, 1990; Romney, 1995).
IS security compliance and non-compliance	Non-compliance is the refusal or failure to adhere to an organization's information security policies and procedures, while compliance is the strict adherence to the rules and guidelines for protecting its information assets (Safa et al., 2016; M. Siponen et al., 2010).
IS misuse	IS misuse is individuals' intentional use of information systems resources, posing a significant threat to organizations. This can range from unethical actions like personal email use to illegal ones like unauthorized access to confidential information (D'Arcy et al., 2009 D'Arcy & Hovav, 2007).
IS security policy violations (malicious and non-malicious)	Information System (IS) security policy violations involve breaches of established protocols by employees or users, posing significant risks to data security and operational integrity (Vance & Siponen, 2012).
Shadow IT	Shadow IT refers to systems, processes, and organizational units developed autonomously by business departments without official IT support, including social media communication, self-built applications, hardware procurement, and IT-support structures (Rentrop & Zimmermann, 2012).
Unauthorized disclosure	Unauthorized disclosures, or leaks, occur when individuals with insider access or employment release information through unofficial channels (A. M. Katz, 1976).
Computer crime	Computer crime involves illegal activities involving computer or network-connected devices, including virus creation, theft, unauthorized access, and financial fraud (Richardson, 2008).
IS security abuse	Security abuse is the intentional misuse or exploitation of a system's features or vulnerabilities by malicious actors, often involving violating security policies or exploiting system vulnerabilities (Hope et al., 2004; Srivratanakul et al., 2004).
Access policy violations	Access policy violations involve unintentional or deliberate violations of organizational rules and regulations to protect information resources, involving individuals consciously going against the organization's stated norms (Vance et al., 2013).

Though the identified forms of IDBs share common characteristics, there are some noticeable differences from the definitions regarding specific behaviors, motivations, and consequences.

5.2 Specific Behaviors

Behavior refers to an individual, group, or organism's observable actions, reactions, or conduct in response to stimuli or situations. It can be conscious or unconscious, voluntary or involuntary, and is influenced by genetics, cultural background, attitudes, emotions, and personal values (J. W. Kanter et al., 2010). Information security behaviors involve individuals adopting practices to protect information systems from unauthorized access, use, disclosure, disruption, modification, or destruction, including software adoption, policy compliance, strong passwords, software updates, and phishing prevention (Shropshire et al., 2015). Information security behaviors can be conscious, unconscious, voluntary, or involuntary, influenced by knowledge, attitudes, and personality traits, leading to deliberate or automated actions (McCormac et al., 2017). Table 4 describes the specific behaviors associated with the IDB identified.

Table 4. Difference in Specific Behaviors IDB studies

Insider Deviant Behaviors	Specific Behaviors
Computer abuse and Computer Fraud	Unauthorized actions involving computer systems and financial fraud
Non-compliance and IS security policy violations	Refusal or failure to adhere to information security policies
IS misuse	Unethical and illegal use of information system resources
Shadow IT	The development of unapproved IT systems and processes by business departments
Unauthorized disclosures	Insider leaks of information
Computer crime	A wide range of illegal activities related to computers or network-connected devices
Security abuse	The intentional misuse of system features or vulnerabilities
Access policy violations	Violations of organizational rules and regulations to protect information resources.

5.3 Motivations

Eccles and Wigfield (2002) define motivation as a multifaceted process involving biological, emotional, social, and cognitive factors influencing an individual's involvement and perseverance in achieving goals. Biological aspects involve physiological and neurochemical foundations (Simpson & Balsam, 2016), while emotions shape the attractiveness and value of pursuing goals (Reeve, 2018). The social environment creates expectations, norms, and influences, while cognitive processes determine goal perception, evaluation, and pursuit (Eccles & Wigfield, 2020). Concerning IDB, Burns et al. (2023) explain that motivations can be instrumental and expressive. Instrumental motives aim to achieve another objective, like financial benefits, while expressive motives express individual emotions or values. For example, a socially supportive environment boosts self-efficacy (cognitive) and increases motivation and positive emotions, while challenging tasks activate reward systems and encourage goal-oriented behaviors. Table 5 describes the motivations behind these IDBs.

Table 5. Differences in Motivations in IDB studies

Insider Deviant Behaviors	Motivations
Computer abuse and IS misuse	It may be motivated out of personal gain, carelessness, or ignorance.
Computer fraud	Motivated by financial gain and involves fraudulent activities
Non-compliance	Refusal to adhere to security policies without clear motivations.
Shadow IT	A desire for autonomy and the perceived need for customized solutions.
Unauthorized disclosures	Various motivations, including Moral and ideological beliefs. For example, whistleblowing or personal gain.
Computer crime	A broad range of motivations. For example, from financial gain or hacktivism
Security abuse	malicious and aims to exploit vulnerabilities or violate security policies.
Access policy violations	Deliberate violations or unintentional errors.

5.4 Consequences

Consequences refer to the results or outcomes of a particular action or decision. These can be positive or negative, intended or unintended, and affect various aspects such as individuals, groups, or systems (Fish, 1985). Positive information security behaviors improve an organization's security posture, reduce incidents, and foster a security-conscious culture, while negative behaviors increase vulnerability to breaches causing financial losses and reputation damage (McCormac et al., 2017). IDB consequences, therefore, involve understanding the multi-dimensional nature of outcomes, which impact various organizational levels and ecosystems and can vary in predictability and complexity. Table 6 describes the consequences of the identified IDBs.

Table 6 Differences in Consequences in IDB Studies

Insider Deviant Behaviors	Consequences
Computer abuse and IS misuse	Resource misuse or operational disruptions
Computer fraud	Financial harm and fraud
Non-compliance	Policy breaches and security risks.
Shadow IT	Challenges in IT governance and a lack of oversight
Unauthorized disclosures	Damage to an organization's reputation.
Computer crime	Data breaches and financial losses.
Security abuse	Harm to system integrity and data security.
Access policy violations	Jeopardize data security and operational integrity.

Our study analyzed theories applied in IS to study IDB (IDB) in information security, and we identified eight factors, namely psychological factors, organizational factors, situational and environmental factors, sociocultural factors, coping and emotional factors, information processing and technology factors, ethical and value-based factors, and socioeconomic factors.

6 Synthesizing the Factors

6.1 Psychological Factors

IDB in information security is heavily influenced by psychological factors, which are the mental and emotional conditions that influence individuals' behavior and decision-making (Schmideberg, 1946; Schoenherr & Thomson, 2020). Individual motivations, attitudes, and moral ideologies influence the decision to engage in IDB (Schoenherr & Thomson, 2020). Rationalization helps justify actions, while attitudes toward the organization, policies, and security measures influence decision-making (Velazquez, 2020). Further, Moody et al. (2018) explain that psychological factors significantly influence insider deviant behaviors due to perceived control imbalance. Individuals engage in deviance when they perceive a discrepancy between their own control and others' control, which increases when situational cues highlight this imbalance, leading to higher deviant behavior (Moody et al., 2018). Psychological factors can impact whether insiders comply or do not comply with organizational policies, such as information security policies. The psychological factors derived from the theories are described in Table 7.

Table 7. Psychological Factors

Factors	Explanations of Insider deviant behavior	References
Motivations and Intentions	Motivations and intentions are intrinsic, originating from internal sources. Common motivations include financial gain, vengeance, personal dissatisfaction, ideological beliefs, or recognition. Intention involves deliberate choice and strategic planning, influenced by opportunity, perceived risk, and potential rewards.	(Willison & Lowry, 2018; Luo et al., 2020)
Rationalization	Individuals rationalize bad behavior by diminishing it, leading to strategies to mitigate its negative effects on self-worth. Insider deviants commit security violations by reconciling actions with self-image, shifting blame, downplaying harm, denying responsibility, and claiming higher causes.	(Barlow et al., 2013, 2018; H. Chen et al., 2019; Siponen & Vance, 2010)
Moral Beliefs/Ideology	Moral beliefs dictate actions' rightness, while ideology prioritizes practical measures like political or cultural opinions. Moral beliefs can influence ethical decision-making, aligning or diverging from established principles. Political, social, and economic ideologies can also influence insider deviant behavior, such as whistleblower ideologies encouraging disclosure or financial incentives justifying deviance.	(Bansal et al., 2016; D'arcy & Herath, 2011; Luo et al., 2020; Baskerville et al., 2014; Myyry et al., 2009)

Self-Control	Information security is influenced by self-control, which resists immediate gratification. Criminal acts are committed by individuals who perceive unlawful activities as a means to achieve their objectives. Individuals with low self-control are likelier to engage in malicious behaviors, while those with high self-control are less likely to engage in deviant activities.	(D'arcy & Herath, 2011; Luo et al., 2020; Li et al., 2021; Baskerville et al., 2014)
Expectancy/Benefits/Harm (Outcomes)	Individuals make decisions based on perceived gains and losses, considering legal, occupational, reputational, and ethical implications. Insiders assess potential outcomes such as financial prosperity, personal gratification, retribution, or achieving goals, impacting decisions about deviant behavior and leading to cognitive evaluation of costs and benefits.	(Cheng et al., 2013; Li et al., 2021; Siponen et al., 2014)
Self-Efficacy	Self-efficacy refers to an individual's belief in their ability to successfully control actions or events in their lives. It is based on their belief in their cognitive abilities, motivation, and resources. A higher self-efficacy can increase the likelihood of attempting deviant actions, as it influences their behavior and helps them feel confident in their ability to control their lives and events.	(Hooper & Blunt, 2020; Luo et al., 2020; Siponen et al., 2014)
Attitudes (Protective/non-protective),	Attitudes are individuals' perceptions of behavior, influencing actions. There are two types: protective and non-protective. Protective attitudes prioritize ethical behavior and security, while non-protective attitudes lack concern for ethical considerations and can lead to deviant behavior.	(Posey et al., 2015; Ratliff & Hicks, 1998; Shropshire et al., 2015; Siponen et al., 2014; Maasberg et al., 2015)

6.2 Organizational Factors

Organizational factors influence moral behavior, including codes of conduct, rewards, and sanctions, peer and management interactions, ethical training, and organizational culture (Roszkowska & Melé, 2021). Organizational factors like security culture, awareness, and support significantly impact employee compliance with policies and practices thereby affecting their involvement in security practices (Cram et al., 2017). Further Cram et al. (2017) explain that organizational factors significantly influence insider deviant behaviors by shaping the work environment. For example, perceived legitimacy, fairness, and justice of organizational structures affect employees' compliance with rules and regulations. Organizations perceived as legitimate, fair, and just enhance policy compliance and reduce deviant behavior, while monitoring and accountability can enhance security guidelines and mitigate insider deviant activities. Table 8 explains the organizational factors.

Table 8 Organizational Factors

Factors	Explanations of Insider deviant behavior	References
Organizational Culture	Organizational culture influences employee behavior, including values, norms, and expectations. A toxic, unethical culture increases insider threats, while a transparent, accountable, and ethical culture deters insider deviance.	(Box & Pottas, 2014; L. Y. Connolly et al., 2017; Hina et al., 2019; Willison, 2006)
Formal and Informal Controls	Formal controls, such as setting standards and monitoring performance, are crucial in preventing deviant behavior in an organization. Weak controls can create insider threats, while informal controls, like the influence of respected individuals, mitigate these threats.	(D'Arcy et al., 2009; Ifinedo & Idemudia, 2017; Luo et al., 2020; Cheng et al., 2013)
Fairness and Justice	Fairness in reward distribution, decision-making, and treatment significantly influences ethical behavior, with distributive justice promoting equal treatment without bias and interactional justice discouraging deviant behaviors.	(Lowry et al., 2015; Willison, Warkentin, et al., 2018; Alshare et al., 2018; Nehme & George, 2020)
Policies	Clear and consistent enforcement of information security policies and procedures can deter deviant actions, while technology use policies can impact behavior by outlining acceptable usage and potential consequences for violations. A lack of well-defined policies can create opportunities for deviance.	(Willison, Warkentin, et al., 2018; Siponen & Vance, 2010; D'Arcy et al., 2009, 2014; Farshadkhah et al., 2021)

Organizational Citizenship	Organizational citizenship behavior (OCB) is the actions that contribute to an organization's smooth functioning, such as fair treatment and justice, which can foster loyalty and commitment, while negative OCB can lead to deviant behavior.	(Ifinedo, 2015)

6.3 Situational and Environmental Factors

Environmental factors refer to human behavior-influenced aspects of the environment, while situational factors describe circumstances that influence goal prioritization and balance between objectives (Steg et al., 2014). According to Johnston et al. (2016), situational factors in information security are the external influences influencing compliance with policies, including threats, sanctions, social cues, and persuasive communications, while environmental factors in information security are the external context, including industry market conditions and technology service providers, which influence individuals and organizations' security approaches (Gutierrez et al., 2015). According to Moody et al. (2018), situational cues, such as workload pressure or interpersonal conflicts, can also influence the motivation to engage in deviant behaviors by affecting individuals' perceived control or by providing rationalizations for deviance. These factors are crucial in explaining IDB in information security, as they can influence an individual's decisions and actions within and outside an organization. Table 9 explains the situational and environmental factors that influence IDB.

Table 9. Situational and Environmental Factors

Factors	Explanations of Insider deviant behavior	References
Stress Triggers	Internal and external pressures, such as high workloads, deadlines, and hoe and work conflicts, can trigger deviant deadlines, and conflicts can trigger deviant behavior, threatening autonomy. Employee routines and tasks can also encourage exploiting vulnerabilities, with situational factors influencing the cost-benefit analysis.	(Yazdanmehr et al., 2023; Dang, 2014; D'Arcy & Teh, 2019; Maasberg et al., 2015)
Sense of Responsibility	Individuals obey authority when they assume responsibility for their actions, with autonomous states directing actions and taking responsibility and agentic states directing actions and passing responsibility.	(Alshare et al., 2018; Harrington, 1996; Silic et al., 2017; Trinkle et al., 2021; Yazdanmehr & Wang, 2023)
Boundary Management (impact of lifestyle and routine activities)	Boundary management is essential for maintaining work-life balance, preventing insider misconduct, reducing stress, and promoting positive attitudes while overlapping boundaries lead to deviant behavior.	(Willison & Backhouse, 2006; Trieu et al., 2021)
Goal Framing	Organizational goal framing, situational and environmental factors, and social norms significantly influence employee deviance, with positive goals like career advancement reducing it and negative goals increasing it.	(Hedström et al., 2013; Ifinedo, 2022; Kim et al., 2016)

6.4 Sociocultural Factors

Sociocultural factors in information security encompass the collective norms, values, beliefs, and practices within an organization or society that influence individuals' attitudes and behaviors toward information security (Shropshire et al., 2015). These factors include social norms, societal structures, cultural beliefs, and values (Clausen & Huffine, 1975; Shropshire et al., 2015). These elements are integral to understanding how individuals and groups within a society or organization perceive and engage with information security practices. Sociocultural factors shape the collective mindset and behaviors towards security protocols, influencing the effectiveness of information security measures within an organization or society at large (Shropshire et al., 2015). They contribute significantly to understanding information security IDB. The factors are explained in Table 10.

Table 10. Sociocultural Factors

Factors	Explanations of Insider deviant behavior	References
Cultural Differences	Cultural factors like collectivism vs. individualism, uncertainty, gender roles, and short and long-term emphasis can influence attitudes and actions. Comparing deviant behavior across contexts helps understand reasons and triggers, especially when dealing with insider threats.	(Connolly et al., 2017; Al-Mukahal & Alshare, 2015)
Social Bonds and Controls	Societal bonds, cultural and social factors, and group dynamics can prevent social deviance, while pressures, peer support, and social isolation can increase the likelihood of deviant behavior among insiders.	(Yazdanmehr & Wang, 2023; Theoharidou et al., 2005; J. Lee & Lee, 2002; Burns et al., 2023)
Social and Cultural Influences	Social norms within an organization or culture can significantly influence behavior, normalizing deviant actions. Strong peer influence and a culture that tolerates deviant behavior can pressure employees to conform, shaping their perception of right and wrong.	(Lowry et al., 2015; Workman & Gathegi, 2007)

6.5 Coping and Emotional Factors

Coping and emotional factors significantly influence how individuals perceive and respond to information security threats (Liang et al., 2019). Emotion regulation is crucial in understanding individuals' responses to information security threats, while coping mechanisms, such as distancing and self-control, help manage emotional experiences and emotions (Liang et al., 2019). According to Burns et al. (2019), emotions act as an adaptive intermediary between stimuli and behavior, with emotional regulation and coping mechanisms playing a crucial role in insiders responding to security threats and policies. For instance, emotion-focused coping strategies can influence how insiders respond to stressful security policies and either conform to or deviate from expected security practices. These mechanisms are essential for effective threat mitigation, as threats often provoke emotional responses. Table 11 explains the coping and emotional factors.

Table 11. Coping and Emotional Factors

Factors	Explanations of Insider deviant behavior	References
Emotional Regulation	individuals struggling with strong emotions, such as anger or resentment, may resort to deviant behavior. Insiders may use emotion-focused coping strategies to manage the emotional impact of a situation rather than addressing the underlying problem, leading to deviant behavior.	(Baskerville et al., 2014; Yazdanmehr et al., 2023; Trieu et al., 2021)
Coping Efforts	Workplace stress is a complex issue categorized into threats and challenges. If perceived as a threat, individuals may use negative emotions like fear or anger to cope. If a threat is identified, they may resort to deviant actions, with coping strategies ranging from adaptive to maladaptive.	(D'Arcy et al., 2014; Kim et al., 2016; Yazdanmehr et al., 2023)

6.6 Information Processing and Technology Factors

Information processing is a cognitive activity that involves evaluating and understanding information. Individuals with limited experience may require more effortful processing of outcomes or consequences of a behavior, as they may need to evaluate salient traits and attribute strength related to achieving their behavioral goal (Kidwell & Jewell, 2008). Technological factors, on the other hand, refer to the state of technology and its impact on industry operations and activities. They include innovation level, pace of change, digital infrastructure state, technology availability and accessibility, and related laws and regulations (Briz-Ponce et al., 2017). IDB in information security is influenced by information processing and technology factors, which include technical aspects, individual interaction with technology, and organizational information processing within an organization. Table 12 explains these factors.

Table 12. Information Processing and Technology Factors

Factors	Explanations of Insider deviant behavior	References
Access and Privileges	Information security places significant emphasis on the utilization of access controls and privileges. Insiders with privileged access or occupying positions of privilege can exploit their permissions for illicit purposes, such as unauthorized access to data or manipulation of systems.	(Dhillon et al., 2020; Sikolia & Biros, 2016; Vance et al., 2013)
Technology Proficiency	The level of technological proficiency an individual exhibit may influence their tendency to engage in deviant behavior. Individuals with strong technical skills may exhibit greater competence in circumventing security measures or masking their activities, while those with low technical skills may be less interested in circumventing security measures for fear of being caught.	(Box & Pottas, 2014; Lin & Kunnathur, 2013; Vance et al., 2013; Ifinedo, 2015)
Information Flow and Sensitivity	Poorly designed systems and data handling increase unauthorized access and breaches, while sensitive information can attract insiders, leading to mistakes and frustration triggering deviant behavior.	(D'arcy & Herath, 2011) Chu et al., 2015; Sikolia & Biros, 2016; Fan & Zhang, 2011; Maasberg et al., 2015)
Security Awareness	Security training and awareness programs significantly impact an individual's understanding of the consequences of deviant behavior, reducing the likelihood of malicious actions. Lack of awareness about cybersecurity risks and insider threats can lead to unintentional risky behavior, making individuals vulnerable to manipulation.	(Fan & Zhang, 2011) (L. Y. Connolly et al., 2017; D'Arcy et al., 2009; Dhillon et al., 2020; Wall & Buche, 2017; Warkentin et al., 2011; Ifinedo & Idemudia, 2017)
Perceived Detection Risk	Organizations can use behavioral analysis tools to monitor employees' digital behavior, identifying potential insider threats. Inconsistent monitoring can create security gaps, and perceptions of detection can influence deviant behavior. The effectiveness of monitoring and consequences for insider threats can shape this perception.	(Hooper & Blunt, 2020; Fan & Zhang, 2011; Herath & Rao, 2009a;Herath & Rao, 2009b;D'Arcy et al., 2009)

6.7 Ethical and Value-based Factors

According to Tyler et al. (2008), an organization's ethical climate and value-based constructs significantly affect employee deviance. Also, employees judge management's credibility by the extent to which violators are punished, which shows that legitimacy is affected by both value and ethical factors (Tyler et al., 2008). IDB in information security can be viewed through ethical and value-based concepts. Personal values, principles, and a person's sense of right and wrong are the fundamental elements of these concepts, influencing how people behave and make decisions in the workplace (Sadeghi et al., 2023). Furthermore, ethical training has been shown to improve ethical decision-making, highlighting the importance of cultivating ethical awareness and competencies to mitigate insider deviant behavior (Fleischman et al., 2023; Sadeghi et al., 2023). Values alignment between employees and their organization can reduce insider deviant behavior by fostering loyalty, satisfaction, and a sense of belonging, thereby reducing contrary behavior (Fleischman et al., 2023). Table 13 explains the factors.

Table 13. Ethical and Value-based Factors

Factors	Explanations of Insider deviant behavior	References
Ethical Decision Making	Ethical dilemmas in the workplace can lead to difficult choices, influencing behavior or deviance. Strong personal morality serves as a moral compass, reducing the likelihood of actions conflicting with ethical principles.	(Gwebu et al., 2020; Workman & Gathegi, 2007; Bansal et al., 2016; Myyry et al., 2009)

Values Alignment	The alignment of an individual's values with the organization's ethical culture significantly influences their behavior, as the harmony between personal and organizational values leads to increased ethical behavior and reduced deviant actions.	(Gwebu et al., 2020; Wall et al., 2015)
Perceived Ethical Climate	An ethical climate within an organization significantly impacts employee behavior. A climate that promotes honesty and integrity discourages deviant behavior, while a climate that tolerates deviant behavior increases insider threats, thus positively impacting employee conduct.	(Gwebu et al., 2020; Workman & Gathegi, 2007)
Instrumentality and Valence	The perceived consequences of ethical behavior (instrumentality) and the personal importance of ethical values (valence) can influence an individual's decision to act ethically or engage in deviance.	(Burns et al., 2015)
Human Agency	Individuals' capacity to act according to their moral principles and values is crucial. Encouraging employees to exercise their agency to make ethical choices can mitigate deviant behavior.	(Herath & Rao, 2009a)

6.8 Socioeconomic Factors

Socioeconomic factors are the social and economic experiences and realities that influence an individual's or group's behaviors and attitudes. These factors can include income, education, occupation, and other aspects of social class (Adler & Ostrove, 1999). According to Zwilling et al. (2022), socioeconomic factors, such as income, education, and occupation, significantly influence insider deviant behavior in information security. Higher income and occupational status provide better access to cybersecurity training and resources, while education shapes an individual's understanding of information security risks (Zwilling et al., 2022). Socioeconomic class also influences organizational culture and environment, with organizations with a cybersecurity culture having less deviant behavior (Öğütçü et al., 2016). Stress and job security perceptions can also influence insider behavior (Nehme, 2021; Safa et al., 2018). These socioeconomic factors play a significant role in explaining IDB in information security. These external factors are influenced by the broader social and economic context within which individuals and organizations operate. Table 14 highlights these socioeconomic factors.

Table 14. Socioeconomic Factors

Factors	Explanations of Insider deviant behavior	References
Financial Motivation	Economic factors, such as financial difficulties, personal crises, high unemployment, income disparities, and limited job opportunities, often drive insider deviance. High unemployment encourages stability, income disparities create inequality, and limited job opportunities and challenging markets increase risk-taking.	(Baskerville et al., 2014; Willison & Backhouse, 2006)
Criminal Networks (Exposure to offenders)	Individuals with connections to criminal networks in society may be more susceptible to deviant actions, and a black market for stolen data or cybercriminal enterprises that purchase such data can incentivize employees to commit data theft or information security breaches.	(Willison & Backhouse, 2006)
Societal Norms	Broader societal privacy, confidentiality, and data security norms can impact an individual's attitude toward insider deviance. High-value societies may discourage deviant actions, while ethical norms like honesty and integrity can influence moral decisions and perceptions of right and wrong.	(Hooper & Blunt, 2020; Moody et al., 2018; Aurigemma & Mattson, 2017; Cheng et al., 2013; J. Lee & Lee, 2002; Lowry et al., 2015; Rajab & Eydgahi, 2019; Theoharidou et al., 2005; Willison, Lowry, et al., 2018)
Legislation and Regulation	The presence of legal and regulatory frameworks within society can influence individuals' perceptions of the consequences of deviant actions. Stringent laws and penalties can act as deterrents.	(Moody et al., 2018; Arduin & Vieru, 2017)

Social Support	The support or lack of support from one's social networks can influence an individual's decision to engage in deviant actions. Social isolation and lack of emotional support can increase the risk of insider threats.	(Moody et al., 2018; Ifinedo, 2014, 2019)

7 Discussion

This review contributes to the existing literature by identifying and classifying the theories employed in examining IDB within information and cybersecurity. These theories have been categorized into four (4) distinct groups: psychological and behavioral, organizational, sociocultural, and decision-making. Moreover, the constructs derived from the theories were additionally categorized into eight (8) distinct categories: psychological factors, organizational factors, situational and environmental factors, sociocultural factors, coping and emotional factors, information processing and technology factors, ethical and value-based factors, and socioeconomic factors, providing an in-depth explanation of the underlying factors contributing to deviant behavior among insiders within information security contexts. These factors mentioned are posited as meta-level factors that influence insider deviance within the domains of information and cybersecurity. Furthermore, the forms of deviant behaviors that have been extensively researched were identified. While they exhibited specific shared characteristics, there were also discernible variations in specific behaviors, motivations, and consequences.

During the process of gathering articles for this systematic literature review, one study conducted by Moody et al. (2018) emerged. This specific research focused on examining eleven (11) existing theories that are either currently utilized or have the potential to be utilized to explain employees' (non-)compliance and intention towards information security policies. Their study aimed to gain insight into the theoretical and empirical similarities and differences between those theories and models. Additionally, they aimed to determine the extent to which these competing theories and models could be integrated into a unified model that effectively addresses the limitations of the individual component models. In contrast to the study conducted by Moody et al. (2018), our study was more comprehensive and distinct, as we analyzed 46 theories in order to gain a deeper understanding of the explanations they provide for IDB. Further, the study by Moody et al. (2018) does not explicitly research IDB but focuses on a sub-set of behaviors belonging to IDB.

As a contribution to IS literature, our study discovered several relationships among the theories and the elements outlined in the factors, which reveal overlapping constructs and how they contribute to the understanding of IDB. These relationships are discussed below.

7.1 Fear

Fear, a fundamental human emotion, plays a crucial role in how individuals perceive, evaluate, and respond to various situations (Foa & Kozak, 1986). Fear is an emotional response to situational control and uncertainty influencing cognitive and behavioral reactions leading to higher IDB risk perceptions and risk-averse behaviors (Xu et al., 2020). According to Adolphs (2013), fear is an innate emotional response in humans and animals that affects cognitive and behavioral processes like attention, memory, perception, and decision-making. It is deeply ingrained in human nature and can be influenced by psychological states like diminished imagination, impulsive tendencies, excessive self-centeredness, social disapproval, idealized self-interest, and excessive concern for personal appearance. In their study, Moody et al. (2018) emphasized the significance of fear as a determinant in understanding individuals' compliance intentions toward information security policies.

Further, Xu et al. (2020) explain that fear in IS security can lead to insiders valuing IS-related deviant behavior as uncertain and risky, leading to increased legal costs and disapproval. Fear can also influence decision-making, decreasing risky behaviors and promoting protective security behaviors. This can motivate compliance and risk-averse behavior in the workplace, especially regarding organizational security policies. Constructs like self-efficacy (Bandura, 1977; Bandura & Wessels, 1994; Ryan & Deci, 2000{Citation}), reactance (Brehm & Brehm, 2013; Lazarus & Folkman, 1984), and emotions (Beaudry & Pinsonneault, 2010), to mention a few, are evoked through fear, which affects the behavior of individuals.

7.2 Case 1: Snowden's Disclosure of Classified Information

For example, Edward Snowden's 2013 disclosure of classified information from the National Security Agency (NSA) (Greenwald et al., 2013), in our interpretation, could have been motivated by a combination

of complex factors with fear being a significant influence. The types of fear that may have influenced Snowden may have included fear for personal safety, fear of the erosion of democratic freedoms and privacy, and fear of the consequences of inaction.

To elaborate, Snowden, in our interpretation, fearing espionage charges and personal safety (reactance), carefully planned his leak of classified information (self-efficacy). He may have feared an erosion of democratic freedoms and individual privacy (emotions) as he witnessed government surveillance programs overreach without consent. These fears and his belief in the importance of privacy and freedom may have ultimately led him to leak classified documents. Therefore, to reduce IDB risk, organizations should focus on reducing fear among employees by improving situational control, minimizing uncertainty, and adopting motivation-based strategies rather than relying solely on sanction-based methods. Effective communication, job security assurances, supportive human resources practices, and strong connections between security policies and employee values are essential mitigation strategies (Ahmad et al., 2014; Son, 2011)

7.3 Motivation and Values

Motivation and values are crucial in understanding the complex connections between individual principles, motives, and subsequent behaviors (Ajzen, 1991; Albrecht et al., 2008; Fishbein, 1979). Eccles and Wigfield (2002) explain motivation as a complex process that initiates, directs, and sustains goal-oriented behaviors involving biological, emotional, social, and cognitive forces. It is a fundamental determinant of an individual's behavior, encompassing intrinsic and extrinsic influences, whereas values are enduring beliefs about desirable outcomes. Siponen (2000) states that motivation and values significantly influence IDB in information security, with intrinsic motivation influencing engagement and external motivation potentially hindering adherence to security guidelines, while values significantly impact life, team spirit, and organizational atmosphere. A healthy culture and leadership foster intrinsic motivation and security awareness, while misalignment can lead to unethical behavior (Padayachee, 2012). Therefore, motivation and values are integral to understanding the influences of insider behavior in information security (Siponen, 2000). Motivations and values are interconnected, influencing each other in an evolving manner (Eccles & Wigfield, 2002). Motivations can stem from deeply ingrained values or challenge prevailing values due to situational factors. Perceived legitimacy, financial pressures, and value alignments are determinants of employees' behavior, including compliance with information systems security policies (ISSP) (Son, 2011). Individual differences influence subjective interpretation and prioritization of values and motives. Individuals' personal norms and moral beliefs, which are subjective and vary from person to person, can significantly affect their intrinsic motivation to follow or violate organizational rules (Son, 2011). Individual behaviors are external expressions of internal motivations and values (Ajzen, 1991; Albrecht et al., 2008; Fishbein, 1979). Employees who align their values and motivation with their organization's values are more likely to follow its policies and avoid deviant behavior. Conversely, those who do not align with their values may rationalize or engage in deviant actions. The credibility of the organization's policies also influences adherence, as employees are more likely to follow regulations they perceive as fitting, desirable, and fair (Padayachee, 2012; Son, 2011).

7.4 Case 2: AT&T Active Insiders

For example, in the case of AT&T Wireless Active Insiders (Mullen, 2023), several employees became "activated insiders" and took more than a million dollars in bribes from external actors to install malware and hardware. Additionally, some employees illegally disclosed their login credentials to external actors, enabling them to unlawfully unlock and sell the AT&T phones. The external actors successfully infiltrated their systems for five years from 2012 to 2017 (Mullen, 2023). In this case, these insiders' motivation and values played a crucial role in their actions. First, these insiders were motivated by financial gain, leading them to accept bribes for participation, which were not aligned with ethical considerations and loyalty to their employer. The actions of these employees suggest a value system prioritizing personal gain over ethical standards and loyalty. Engaging in criminal activities, such as accepting bribes and installing malware, indicates a willingness to compromise ethical standards for personal benefit. The values driving these actions may also reflect a lack of alignment with the principles of honesty, integrity, and responsibility expected by employers and society. The employees may have rationalized their actions by downplaying ethical implications or arguing that the harm was minimal compared to the benefits they received.

7.5 Coping Mechanisms and Stress Responses

Coping mechanisms and stress responses provide insight into how individuals handle stressors that may lead to deviant behavior (Boal & Cummings, 1981; Lazarus & Folkman, 1984). According to Beaudry and Pinsonneault (2010) and Lazarus and Folkman (1984) regulating intense emotions can be challenging for those dealing with negative emotions. Insiders may resort to deviant behavior using emotion-focused strategies instead of confronting the root cause. Emotions significantly influence employee deviant behavior, particularly in the workplace, where abusive supervision can trigger intense emotional responses like anger, potentially leading to deviant behavior (Nehme & George, 2020). Adaptive coping strategies involve constructive responses, while maladaptive coping strategies involve actions that deviate from societal norms and can lead to a cycle of negative emotions and coping mechanisms (Boal & Cummings, 1981; Lazarus & Folkman, 1984). For example, workplace stress, including long hours, unclear performance expectations, unsafe conditions, and career or job security concerns, can lead to negative emotional responses among employees. These negative emotions can cause individuals to assess their circumstances and perceive their inability to cope effectively, potentially posing a threat and engaging in deviant behaviors. According to Nasaescu et al. (2018), coping mechanisms and stress responses reveal psychological processes influencing deviant behavior, especially in online settings. High emotional arousal promotes information sharing, potentially leading to ICT abuse and societal norm deviance (Nasaescu et al., 2018). Addressing stressors and promoting adaptive coping strategies are crucial for holistic approaches to managing IDS and creating a secure organizational environment.

7.6 Case 3: Former Employee Abusing Administrator Access

A case study of how coping mechanisms and stress responses may lead to insider deviant behavior involves a former employee of a medical device packaging company with administrator access (insider knowledge) to the company's shipping information who created a fake user account to access the company's systems after his termination in March 2020. After receiving his paycheck, he used this account to edit and delete thousands of records, severely impacting the company's shipping process and causing delays in vital PPE equipment during the pandemic (Mullen, 2023; United States Department of Justice, 2020a). The employee's actions, following his termination, can be interpreted as maladaptive coping mechanisms and negative stress responses. The chronology of events leading to his fabricating user accounts to sabotage his previous employer's operations during the pandemic suggests a reaction driven by resentment, revenge, and a lack of constructive coping strategies to deal with job loss and its psychological impacts. The employee's behavior shows he was not able to cope with the stress of job loss in a healthy manner, indicating a high level of distress and a potentially low level of resilience or practical coping skills. This case study emphasizes how organizations should encourage adaptive coping strategies, stress management, and emotional intelligence training for employees to respond to security threats effectively. Offering counseling services and fostering a supportive work environment can help employees address concerns and reduce risks posed by IDBs. Engaging employees in information security initiatives can effectively reduce the risks posed by insiders (Nehme, 2021; Safa et al., 2018).

7.7 Cultural and Societal Dimensions

Crossler et al. (2013) explain that cultural and societal dimensions emphasize the importance of cultural influences on behavior within the organizational context. The existence of cross-cultural differences in IT contexts, such as variations in uncertainty avoidance, collectivism versus individualism, and power distance, substantially influence phenomena such as IDB. These disparities are of utmost importance for ensuring effective communication and collaboration (Crossler et al., 2013). According to Agnew (1991), Bandura (1971, 1986), and Hofstede (1984), cultural and social factors like gender roles, short-term goals, uncertainty, and collectivism significantly influence people's thoughts and behaviors. Understanding these distinctions is crucial when dealing with IDBs. Strong bonds, such as attachment and commitment, significantly impact employees' ethical rule-breaking behavior and their intentions to violate ISSP (Cheng et al., 2013). Group dynamics, peer support, social isolation, and pressures can influence an insider's propensity to engage in deviant behavior (Safa et al., 2016). Positive cultural and organizational attitudes can lower perceived barriers to participation. Societies are classified into high-context and low-context categories based on their communication styles, which are influenced by cultural and social dimensions (Broeder, 2021; Hall, 1976). High-context cultures rely on implicit cues and shared understanding, while low-context cultures are more explicit (Hall, 1976). Miscommunication can lead to IDBs, as employees may misinterpret organizational guidelines. High power distance cultures reduce the likelihood of employees

questioning authority, creating an environment conducive to IDB when directives are issued without critical examination.

Additionally, cultural and societal dimensions significantly influence employee behavior within an organization. Employees' adherence to or deviation from policies is often shaped by their alignment with cultural norms and values, which can affect their perceptions of societal expectations (Bulgurcu et al., 2010). For instance, a culture that values loyalty towards peers may deter reporting suspicious activities and IDBs.

7.8 Case 4: Facebook Security Engineer Misusing Access

An example of how cultural and societal dimensions influence employee behavior is the 2018 case of a Facebook security engineer who was fired for allegedly misusing his access to the company's data to stalk women online (Popken, 2018). The engineer's abusive use of his access privileges to stalk women can be examined by considering cultural and societal factors. However, it is crucial to understand that a complex interaction of personal, societal, and cultural factors shapes individual actions. First, this case shows how gender dynamics and power dynamics are interconnected concepts that can influence behavior, particularly in the context of sexualizing and stalking women (Laffier & Rehman, 2023). Cultural attitudes towards gender and underlying beliefs about entitlement could have influenced the behavior of this engineer. At the same time, power dynamics may have contributed to such actions, which involve individuals feeling empowered to breach norms and ethics due to their status or role within a company or society. Further, the culture of ethics, privacy, and data use at Facebook may have significantly influenced the employee's behavior. Lack of oversight or ethical training may have led to the misuse of access without fear of consequences (Ahmad et al., 2014; Chia et al., 2002). Peer influence and the overall workplace environment might have also influenced such behavior, with a culture of overlooking minor ethical breaches that may have led to more serious violations such as stalking of women online (Hu et al., 2012). While this individual may have acted independently, such actions do not occur in a vacuum. Cultural and societal factors, such as changing norms regarding privacy, technology, gender, and power, can significantly influence IDBs. As such, organizations can reduce risks by addressing cultural norms, fostering a sense of belonging, and utilizing social controls (Hsu et al., 2015). Additionally, addressing cultural diversity is crucial for multicultural environments, improving the effectiveness of information security policies and training programs (Hsu et al., 2015).

7.9 Technological Acceptance

According to Kraemer and Carayon (2007), end users' attitudes towards security significantly impact their interactions with security systems. They may violate security policies if they fail to recognize the importance or find it inconvenient. To achieve optimal technology acceptance, users must perceive the technology as significant and user-friendly. Therefore, technological acceptance is a crucial aspect of the modern information security landscape, as it influences psychological processes that shape behavior. The technology acceptance model (TAM) (Davis, 1989; Davis et al., 1989) proposes that the acceptance of technology is influenced by users' behavioral intention, which is, in turn, determined by their perception of the usefulness of the technology in task performance and their perception of the ease of using it. TAM (Davis, 1989; Davis et al., 1989) posits that the self-efficacy component elicits fear and anxiety in how individuals perceive and evaluate their capacity to adapt to changes. Therefore, perceiving technology as user-friendly may reduce anxiety and resistance, particularly in the context of IDB. As users acquire more knowledge and confidence through direct interaction with a system, they perceive it to be easier to use, thereby reducing computer anxiety (Hackbarth et al., 2003). Systems and tools prioritizing user-friendliness are more likely to be accepted, positively impacting employees' psychological well-being and engagement (Brown, 2002). Trust is crucial in the psychological aspect of technology adoption, as individuals need to trust established systems' reliability and efficacy (Roberts et al., 2021). Acceptance of technology fosters trust, boosts confidence, and reduces deviant behavior. The Social Information Processing Theory (Salancik & Pfeffer, 1978), which examines how individuals form judgments and attitudes within a social context, particularly in an organizational setting, may influence this acceptance. Social cues, like colleague feedback, onlooker effect, and guilt, significantly influence actions and interpretations, thereby contributing to the acceptance of systems and deterring IDBs (Farshadkhah et al., 2021).

7.10 Case 5: Former Cisco Engineer Unauthorized Access

For example, in 2018, a former Cisco engineer intentionally accessed (insider knowledge) Cisco's cloud infrastructure without authorization and caused significant damage. During the unauthorized access, he ran

code from his Google Cloud Project account, deleting 456 virtual machines. This action disrupted nearly 16,000 WebEx teams customer accounts, costing Cisco approximately $1.4 million in employee costs to repair the damage and an additional $1 million in refunds to affected customers (United States Department of Justice, 2020b). The behavior exhibited in this case can be explained in terms of technological acceptance and social information processing, along with the psychological and sociotechnical factors that may have influenced it.

First, the employee's role as an engineer in our interpretation likely contributed to a high level of comfort and familiarity with complex technological systems (significance and user-friendliness). This familiarity may have led to a perception that engaging with these systems, even unauthorized, was within his capabilities. Further, his understanding and acceptance of the technology may have given him a sense of control, influencing his malicious exploitation of the system (Maalem Lahcen et al., 2020). This IDB may have been exacerbated by the online environment, which may have created a sense of anonymity and led to actions that may not be considered in a physical setting. Social cues and norms, especially those dominated by skilled professionals, can influence behavior in these technological environments (Maalem Lahcen et al., 2020). Additionally, this individual understanding of technology and social context may have justified his actions as a skill demonstration or response to grievances. However, the lack of personal connection in cloud infrastructure interaction may have reduced the significance of his actions, thereby underestimating its impact in the real world.

7.11 Moral and Ethical Considerations

Moral and ethical considerations provide a framework for reasoning, rationalization, and ethical principles that guide insider behavior (Warkentin & Willison, 2009). Moral beliefs govern the ethical evaluation of actions, determining their moral validity or invalidity, whereas ideology emphasizes pragmatic considerations such as political or cultural viewpoints. An individual's moral beliefs can impact ethical decision-making, coinciding with or deviating from established ethical principles (Wikström, 2014; Wikström et al., 2017). Moral and ethical considerations significantly influence individuals' decision-making processes, justifications, and adherence to ethical standards (Li et al., 2021). These values are rooted in personal values and beliefs, which form the perception of morality. In IDB, individuals evaluate their actions based on these values, influencing their decision-making processes. Ethical decision-making involves examining the potential impacts of actions on individuals and society using rational or emotional reasoning. Moral reasoning helps individuals evaluate the ethical implications of insider actions, ultimately leading to decisions that align with ethical principles.

7.12 Case 6: Snowden's Disclosure of Classified Information

Again, the case of Edward Snowden suggests a profound interweaving of moral and ethical considerations. Snowden argued that the NSA's mass surveillance programs violated individual privacy rights without public oversight or consent, arguing that this was an unethical infringement of civil liberties (Greenwald et al., 2013). Snowden viewed his actions as a moral stand against this infringement and, therefore, believed that citizens deserved to know the extent of government surveillance to make informed decisions about their privacy and security. As an insider with such knowledge, disclosure of this classified information was compelled by a moral obligation to expose wrongdoing despite personal and legal risks. His actions raised ethical questions about the duty to report unethical practices and the protection needed for those who take such risks; in such a case, ethical dilemmas and decision-making can be used in training to combat IDBs in information security. By incorporating scenarios, role-playing exercises, interactive workshops, feedback, and gamification, organizations can encourage critical thinking regarding ethical decisions and the consequences of their actions and foster a culture of ethical awareness, thereby mitigating insider threats (Gheyas & Abdallah, 2016)

7.13 Practical Measures

According to Puleo (2006), practical measures to mitigate insider deviance involve a combination of strategies focused on human behavior, risk management, and the use of technology. Implementing these measures is essential because they target the underlying causes of insider threats and strive to proactively prevent incidents, rather than merely reacting to them. Further, Puleo (2006) indicates that implementing these measures is crucial because they effectively tackle the complex nature of insider threats, and organizations can greatly mitigate the risk of insider deviance by placing emphasis on early detection

through behavioral observation, integrating human behavior into risk management, and enhancing security practices.

As a contribution to practice, we identified some practical measures organizations can implement to mitigate IDBs. Table 15 highlights these measures.

Table 15. Practical Measures

Measures	Implementation	References
Reducing fear	• Minimization of workplace uncertainty • Adoption of motivation-based strategies • Improving communication • Ensuring job security • Adoption of supportive HR practices	(Ahmad et al., 2014; Son, 2011)
Coping strategies	• Encourage adaptive coping strategies • Encourage Stress management Practices • Emotional intelligence training • Provide counseling services and a supportive work environment • Engage employees in information security initiatives	(Nehme, 2021; Safa et al., 2018)
Organizational culture	• Fostering value and fairness • Establishing a non-punitive system for addressing errors and security incidents • Encouraging employees to report threats without fear of negative consequences	(Ahmad et al., 2014; Chia et al., 2002)
Security Awareness	• Customized security awareness programs considering sociocultural influences and cognitive biases • Encouraging social interactions among employees • Promoting positive role models • Frequent engagement among employees for robust connections, improved oversight, and reduced internal risk	(Hsu et al., 2015; Tsohou et al., 2015)
Ethical Decision Making	• Incorporate scenarios, role-playing exercises, interactive workshops, feedback, and gamification in security training • Encourage critical thinking about ethical decisions during trainings • Foster ethical awareness culture to mitigate insider threats	(Gheyas & Abdallah, 2016)
Trust in technology	• Prioritize transparency, ethics, privacy, and reliability to reduce unethical conduct • Ensuring data management authority and implementing advanced measures like digital biometrics	(Albinson et al., 2019)

Examining these classified theories and factors has brought attention to critical components such as fear, motivation, coping mechanisms, sociocultural influences, acceptance of technology, and moral and ethical considerations that play a role in comprehending IDB. Further, this study has suggested some practical measures that can be implemented to mitigate IDBs.

8 Research Gaps and Recommendations

Our study identified additional areas of research that we recommend for further investigation in the field of IDBs:

The existing theories often assume static conditions, overlooking the constantly evolving nature of real-world environments. The existing literature reveals limitations concerning dynamic theories that consider technological changes, organizational structures, and societal norms. For example, the rapid progress of artificial intelligence (AI), the implementation of hybrid work environments in organizational structures, and the continuous evolution of social and cultural norms necessitate the advancement of dynamic theories that can effectively analyze and explain the impact of these factors on IDBs.

Though the classifications attempted to categorize factors influencing deviant behavior, a unified classification that integrates insights from various theories is lacking. With the exclusion of the research conducted by Moody et al. (2018), which examined a selected number of 11 theories from the overall pool of 46 theories in this study in order to develop an integrated model, there is a notable absence of a comprehensive, unified framework. This absence poses a challenge in gaining an in-depth knowledge of IDB.

Research is needed to understand how moral psychological theories, like moral reasoning, interact with psychological, situational, decision-making, and cultural factors, as there are gaps in understanding how an individual's moral reasoning aligns with other influences on deviant behavior. Moral reasoning is a cognitive process through which individuals evaluate the morality of their actions, but it has yet to be used to study IDB in IS literature.

To further the research on IDB, methodologies and frameworks such as Longitudinal Studies and Agent-Based Modelling (ABM) can effectively address the existing deficiencies in the literature on IDB. Longitudinal Studies conducted over a period of time can document the development of IDB concerning advances in technology, variations in organizational structures, and changes in sociocultural norms. This methodology enables the examination of recurring patterns, emerging behaviors, and causal relationships over a period, offering a valuable understanding of the ever-changing characteristics of IDB. Agent-based modeling (ABM) is a methodology that can simulate complex systems. It enables users to construct complex models by specifying agent behaviors and the environment in which they function (Alonso-Betanzos et al., 2017). Agent-based modeling (ABM) can help understand the complexities of insider decision-making and sociocultural norms in diverse settings. Decision trees can represent agents' decision-making and help understand sustainable behavior dynamics. Through the incorporation of psychological and contextual factors, ABM can provide insights into factors influencing insider deviant behavior and the effectiveness of interventions or policies to reduce such behaviors.

9 Limitations

The systematic literature review conducted in our study proved to be a valuable tool for synthesizing the existing body of knowledge. However, it is essential to acknowledge that certain limitations are associated with our review. The scope of the review was restricted to studies that were published in specific academic journals and conferences, potentially leading to the introduction of publication bias. Furthermore, it is essential to note that the field of information security is characterized by its dynamic nature, which implies that the significance of theories within this field may have evolved and shifted over time. Our systematic review may not have comprehensively covered the latest advancements, emerging theories, or advances in understanding IDB. Additionally, integrating theories from various disciplines, such as criminology, sociology, and psychology, poses challenges in understanding IDB. These challenges arise from differences in terminology, methodologies, and underlying assumptions across these disciplines. Furthermore, our literature review did not include an extensive analysis of demographic factors, the limitations of each theory and the challenges associated with their application in the context of IDB. However, we will address these issues in upcoming research. Lastly, our systematic review was limited to examining and analyzing the existing theories and studies in the academic literature. The review's comprehensiveness may be limited due to theoretical gaps or emerging perspectives that have not been extensively examined.

10 Conclusion

This systematic literature review examined studies on IDB in information security research, focusing on the theories used in criminology, psychology, and sociology. The review identified and categorized four distinct groups of theories and eight categories of derived constructs, providing a comprehensive understanding of factors contributing to IDB in information security contexts. The review also identified ten distinct deviant behaviors, revealing common traits and noticeable behavioral differences, motivations, and consequences. The study comprehensively explains the factors contributing to IDB in information security contexts.

This review emphasized the wide range of theoretical frameworks in explaining the motivations, triggers, and consequences of deviant behavior exhibited by insiders. Various theoretical frameworks and constructs, such as self-efficacy, coping mechanisms, and emotional mechanisms, as well as criminological theories like Fraud Triangle and Deterrence, offer distinct perspectives for analyzing this complicated phenomenon. The presented findings indicate that several variables, such as fear, motivations and values, cultural and

societal dimensions, technology acceptance, coping and emotional mechanisms, and moral and ethical considerations, play a crucial role in understanding how individuals or insiders assess and perceive situational conditions, ultimately influencing their behaviors.

The literature review on insider threats and deviant behaviors highlights the challenges and gaps in the field, including fragmentation, a lack of a cohesive theoretical framework, and the need for continuous research to capture emerging trends. The temporal dynamics of IDBs in information security, driven by rapid technological advancements and evolving organizational practices, underscore the need for continuous research. Despite these challenges, the review is a resource for researchers, practitioners, and policymakers to understand the intricacies of insider threats and deviant behaviors. Future research should prioritize interdisciplinary collaboration and adopt a comprehensive approach incorporating criminological, sociological, and psychological perspectives. This approach will provide a nuanced understanding of the interrelated elements affecting insider threats and deviant behaviors, emphasizing the need for strategies considering individual, organizational, and societal dimensions.

References

Adler, N. E., & Ostrove, J. M. (1999). Socioeconomic status and health: What we know and what we don't. *Annals of the New York Academy of Sciences*, *896*(1), 3–15.

Adolphs, R. (2013). The biology of fear. *Current Biology*, *23*(2), R79–R93.

Agnew, R. (1991). A longitudinal test of social control theory and delinquency. *Journal of Research in Crime and Delinquency*, *28*(2), 126–156.

Agnew, R. (1992). Foundation for a general strain theory of crime and delinquency. *Criminology*, *30*(1), 47–88.

Ahmad, A., Maynard, S. B., & Park, S. (2014). Information security strategies: Towards an organizational multi-strategy perspective. *Journal of Intelligent Manufacturing*, *25*, 357–370.

Ajzen, I. (1991). The theory of planned behavior. *Organizational Behavior and Human Decision Processes*, *50*(2), 179–211.

Albinson, N., Balaji, S., & Chu, Y. (2019). *Building digital trust: Technology can lead the way*. https://www2.deloitte.com/content/dam/insights/us/articles/6320_Building-digital-trust/DI_Building-digital-trust.pdf. Accessed 3/4/2024

Albrecht, W. S., Albrecht, C., & Albrecht, C. C. (2008). Current trends in fraud and its detection. *Information Security Journal: A Global Perspective*, *17*(1), 2–12.

Albrecht, W. S., Howe, K. R., & Romney, M. B. (1984). *Deterring fraud: The internal auditor's perspective*. Institute of Internal Auditors Research Foundation. https://cir.nii.ac.jp/crid/1130282272831048320

Al-Mukahal, H. M., & Alshare, K. (2015). An examination of factors that influence the number of information security policy violations in Qatari organizations. *Information & Computer Security*, *23*(1), 102–118.

Alonso-Betanzos, A., Sánchez-Maroño, N., Fontenla-Romero, O., Polhill, J. G., Craig, T., Bajo, J., & Corchado, J. M. (2017). *Agent-based modeling of sustainable behaviors*. Springer.

Alshare, K. A., Lane, P. L., & Lane, M. R. (2018). Information security policy compliance: A higher education case study. *Information & Computer Security*, *26*(1), 91–108.

Arduin, P.-E., & Vieru, D. (2017). Workarounds as means to identify insider threats to information systems security. *Americas Conference on Information Systems*.

Ashforth, B. E., Kreiner, G. E., & Fugate, M. (2000). All in a day's work: Boundaries and micro role transitions. *Academy of Management Review*, *25*(3), 472–491.

Aurigemma, S., & Mattson, T. (2017). Deterrence and punishment experience impacts on ISP compliance attitudes. *Information & Computer Security*, *25*(4), 421–436.

Bandura, A. (1971). *Social learning theory.* General Learning Press.

Bandura, A. (1977). Self-efficacy: Toward a unifying theory of behavioral change. *Psychological Review*, *84*(2), 191.

Bandura, A. (1986). *Social foundations of thought and action*. Prentice-Hall.

Bandura, A. (1988). Organisational applications of social cognitive theory. *Australian Journal of Management*, *13*(2), 275–302.

Bandura, A. (1999). Moral disengagement in the perpetration of inhumanities. *Personality and Social Psychology Review*, *3*(3), 193–209.

Bandura, A., & Wessels, S. (1997). *Self-efficacy*. Cambridge University Press.

Bansal, G., Hodorff, K., & Marshall, K. (2016). Moral beliefs and organizational information security policy compliance: The role of gender. *MWAIS 2016 Proceedings. 11.* https://aisel.aisnet.org/mwais2016/11

Barlow, J. B., Warkentin, M., Ormond, D., & Dennis, A. (2018). Don't even think about it! The effects of antineutralization, informational, and normative communication on information security compliance. *Journal of the Association for Information Systems*, *19*(8), 3.

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*, 145–159.

Baskerville, R., Hee Park, E., & Kim, J. (2014). An emote opportunity model of computer abuse. *Information Technology & People*, *27*(2), 155–181.

Beaudry, A., & Pinsonneault, A. (2010). The other side of acceptance: Studying the direct and indirect effects of emotions on information technology use. *MIS Quarterly*, *34*(4), 689–710.

Beccaria, C. (1963). On crimes and punishments (H. Paolucci, Trans.). Bobbs-Merrill

Bishop, M., & Gates, C. (2008). Defining the insider threat. *Proceedings of the 4th Annual Workshop on Cyber Security and Information Intelligence Research: Developing Strategies to Meet the Cyber Security and Information Intelligence Challenges Ahead*.

Boal, K. B., & Cummings, L. (1981). Cognitive evaluation theory: An experimental test of processes and outcomes. *Organizational Behavior and Human Performance*, *28*(3), 289–310.

Box, D., & Pottas, D. (2014). A model for information security compliant behaviour in the healthcare context. *Procedia Technology*, *16*, 1462–1470.

Boxall, P., & Macky, K. (2009). Research and theory on high-performance work systems: Progressing the high-involvement stream. *Human Resource Management Journal*, *19*(1), 3–23.

Brackney, R. C., & Anderson, R. H. (2004). *Understanding the insider threat: Proceedings of a March 2004 workshop*. Rand.

Brehm, S. S., & Brehm, J. W. (2013). *Psychological reactance: A theory of freedom and control*. Academic Press.

Briz-Ponce, L., Pereira, A., Carvalho, L., Juanes-Méndez, J. A., & García-Peñalvo, F. J. (2017). Learning with mobile technologies–Students' behavior. *Computers in Human Behavior*, *72*, 612–620.

Broeder, P. (2021). Informed communication in high context and low context cultures. *Journal of Education, Innovation, and Communication*, *3*(1), 13–24.

Brown, I. T. (2002). Individual and technological factors affecting perceived ease of use of web-based learning technologies in a developing country. *The Electronic Journal of Information Systems in Developing Countries*, *9*(1), 1–15.

Bulgurcu, B., Cavusoglu, H., & Benbasat, I. (2010). Information security policy compliance: An empirical study of rationality-based beliefs and information security awareness. *MIS Quarterly*, *34*(3), 523–548.

Burns, A., Roberts, T. L., Posey, C., & Lowry, P. B. (2019). The adaptive roles of positive and negative emotions in organizational insiders' security-based precaution taking. *Information Systems Research*, *30*(4), 1228–1247.

Burns, A., Roberts, T. L., Posey, C., Bennett, R. J., & Courtney, J. F. (2015). Assessing the role of security education, training, and awareness on insiders' security-related behavior: An expectancy theory approach. *2015 48th Hawaii International Conference on System Sciences* (pp. 3930–3940).

Burns, A., Roberts, T. L., Posey, C., Lowry, P. B., & Fuller, B. (2023). Going beyond deterrence: A middle-range theory of motives and controls for insider computer abuse. *Information Systems Research*, *34*(1), 342–362.

Chen, H., Chau, P. Y., & Li, W. (2019). The effects of moral disengagement and organizational ethical climate on insiders' information security policy violation behavior. *Information Technology & People*, *32*(4), 973–992.

Chen, Y., Galletta, D. F., Lowry, P. B., Luo, X., Moody, G. D., & Willison, R. (2021). Understanding inconsistent employee compliance with information security policies through the lens of the extended parallel process model. *Information Systems Research*, *32*(3), 1043–1065.

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

Chia, P. A., Maynard, S. B., & Ruighaver, A. B. (2002). Understanding organizational security culture. *Proceedings of PACIS2002. Japan*, *158*.

Chu, A. M., Chau, P. Y., & So, M. K. (2015). Developing a typological theory using a quantitative approach: A case of information security deviant behavior. *Communications of the Association for Information Systems*, *37*(1), 25.

Clausen, J. A., & Huffine, C. L. (1975). Sociocultural and social-psychological factors affecting social responses to mental disorder. *Journal of Health and Social Behavior*, *16*(4), 405–420.

Cohen, L. E., & Felson, M. (1979). Social change and crime rate trends: A routine activity approach. In *Classics in environmental criminology* (pp. 203–232). Routledge.

Colwill, C. (2009). Human factors in information security: The insider threat–Who can you trust these days? *Information Security Technical Report*, *14*(4), 186–196.

Connolly, L. Y., Lang, M., Gathegi, J., & Tygar, D. J. (2017). Organisational culture, procedural countermeasures, and employee security behaviour: A qualitative study. *Information & Computer Security*, *25*(2), 118–136.

Connolly, L., Lang, M., & Tygar, J. D. (2015). Investigation of employee security behaviour: A grounded theory approach. *ICT Systems Security and Privacy Protection: 30th IFIP TC 11 International Conference, SEC 2015, Hamburg, Germany, May 26-28, 2015, Proceedings 30* (pp. 283–296).

Cram, W. A., Proudfoot, J. G., & D'Arcy, J. (2017). *Organizational information security policies: A review and research framework*. *European Journal of Information Systems*, *26*(6), 605–641.

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*, 90–101.

Cybersecurity Insiders. (2023). *Insider threat report 2023*. https://www.cybersecurity-insiders.com/portfolio/insider-threat-report-prospectus/ Accessed 20/02/2023

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. (2005). Deterring information systems misuse: The impact of three security countermeasures. *The Fourth Security Conference, Las Vegas, NV*.

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

D'Arcy, J., & Teh, P.-L. (2019). Predicting employee information security policy compliance on a daily basis: The interplay of security-related stress, emotions, and neutralization. *Information & Management*, *56*(7), 103151.

D'Arcy, J., Herath, T., & Shoss, M. K. (2014). Understanding employee responses to stressful information security requirements: A coping perspective. *Journal of Management Information Systems*, *31*(2), 285–318.

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.

Dang, D. (2014). Predicting insider's malicious security behaviours: A general strain theory-based conceptual model. *Proceedings of the International Conference on Information Resources Management (CONF-IRM 2014)*.

Davis, F. D. (1989). Perceived usefulness, perceived ease of use, and user acceptance of information technology. *MIS Quarterly*, *13*(3), 319–340.

Davis, F. D., Bagozzi, R. P., & Warshaw, P. R. (1989). User acceptance of computer technology: A comparison of two theoretical models. *Management Science*, *35*(8), 982–1003.

Dewe, P. (1991). Primary appraisal, secondary appraisal and coping: Their role in stressful work encounters. *Journal of Occupational Psychology*, *64*(4), 331–351.

Dhillon, G., Abdul Talib, Y. Y., & Picoto, W. N. (2020). The mediating role of psychological empowerment in Information Security Compliance Intentions. *Journal of the Association for Information Systems*, *21*(1).

Digman, J. M. (1997). Higher-order factors of the Big Five. *Journal of Personality and Social Psychology*, *73*(6), 1246.

Dijk, J. J. van. (1994). Understanding crime rates: On the interactions between the rational choices of victims and offenders. *The British Journal of Criminology*, *34*(2), 105–121.

Eccles, J. S., & Wigfield, A. (2002). Motivational beliefs, values, and goals. *Annual Review of Psychology*, *53*(1), 109–132.

Eccles, J. S., & Wigfield, A. (2020). From expectancy-value theory to situated expectancy-value theory: A developmental, social cognitive, and sociocultural perspective on motivation. *Contemporary Educational Psychology*, *61*, 101859.

Fan, J., & Zhang, P. (2011). Study on e-government information misuse based on General Deterrence Theory. *ICSSSM11*.

Farshadkhah, S., Van Slyke, C., & Fuller, B. (2021). Onlooker effect and affective responses in information security violation mitigation. *Computers & Security*, *100*, 102082.

Fish, S. (1985). Consequences. *Critical Inquiry*, *11*(3), 433–458.

Fishbein, M. (1979). A theory of reasoned action: Some applications and implications. *Nebraska Symposium on Motivation*, *27*, 65–116.

Fleischman, G. M., Valentine, S. R., Curtis, M. B., & Mohapatra, P. S. (2023). The influence of ethical beliefs and attitudes, norms, and prior outcomes on cybersecurity investment decisions. *Business & Society*, *62*(3), 488–529.

Foa, E. B., & Kozak, M. J. (1986). Emotional processing of fear: Exposure to corrective information. *Psychological Bulletin*, *99*(1), 20.

Folger, R., & Cropanzano, R. (2001). Fairness theory: Justice as accountability. In J. Greenberg, & R. Cropanzano, (Eds.), *Advances in organizational justice* (pp. 1–55). Stanford University Press.

Gheyas, I. A., & Abdallah, A. E. (2016). Detection and prediction of insider threats to cyber security: A systematic literature review and meta-analysis. *Big Data Analytics*, *1*(1), 6.

Gibbs, J. P. (1968). Crime, punishment, and deterrence. *The Southwestern Social Science Quarterly*, *48*(4), 515–530.

Green, D. (2014). Insider threats and employee deviance: Developing an updated typology of deviant workplace behaviors. *Issues in Information Systems*, *15*(2), 185–189.

Greenberg, J. (1987). A taxonomy of organizational justice theories. *Academy of Management Review*, *12*(1), 9–22.

Greenwald, G., MacAskill, E., & Poitras, L. (2013). Edward Snowden: The whistleblower behind the NSA surveillance revelations. *The Guardian*, *9*(6), 2.

Gresham, S., & David, M. (1957). Techniques of neutralization: A theory of delinquency. *American Sociological Review*, *22*(6), 664–670.

Griffith, D. S. (1990). The computer fraud and abuse act of 1986: A measured response to a growing problem. *Vanderbilt Law Review*, *43*, 453.

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

Gutierrez, A., Boukrami, E., & Lumsden, R. (2015). Technological, organisational and environmental factors influencing managers' decision to adopt cloud computing in the UK. *Journal of Enterprise Information Management*, *28*(6), 788–807.

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

Hackbarth, G., Grover, V., & Mun, Y. Y. (2003). Computer playfulness and anxiety: Positive and negative mediators of the system experience effect on perceived ease of use. *Information & Management*, *40*(3), 221–232.

Hall, E. T. (1976). *Beyond culture.* Anchor.

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.

Hedström, K., Karlsson, F., & Kolkowska, E. (2013). Social action theory for understanding information security non-compliance in hospitals: The importance of user rationale. *Information Management & Computer Security*, *21*(4), 266–287.

Herath, T., & Rao, H. R. (2009a). Encouraging information security behaviors in organizations: Role of penalties, pressures and perceived effectiveness. *Decision Support Systems*, *47*(2), 154–165.

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

Herath, T., Yim, M.-S., D'Arcy, J., Nam, K., & Rao, H. R. (2018). Examining employee security violations: Moral disengagement and its environmental influences. *Information Technology & People*, *31*(6), 1135–1162.

Hina, S., Selvam, D. D. D. P., & Lowry, P. B. (2019). Institutional governance and protection motivation: Theoretical insights into shaping employees' security compliance behavior in higher education institutions in the developing world. *Computers & Security*, *87*, 101594.

Hirschi, T. (1969). *Causes of delinquency.* University of California Press.

Hirschi, T. (2017). *Causes of delinquency*. Routledge.

Hofstede, G. (1984). *Culture's consequences: International differences in work-related values* (Vol. 5). Sage.

Hofstede, G., & McCrae, R. R. (2004). Personality and culture revisited: Linking traits and dimensions of culture. *Cross-Cultural Research*, *38*(1), 52–88.

Hogarth, R. M., & Reder, M. W. (1987). *Rational choice: The contrast between economics and psychology.* University of Chicago Press.

Hooper, V., & Blunt, C. (2020). Factors influencing the information security behaviour of IT employees. *Behaviour & Information Technology*, *39*(8), 862–874.

Hope, P., McGraw, G., & Anton, A. I. (2004). Misuse and abuse cases: Getting past the positive. *IEEE Security & Privacy*, *2*(3), 90–92.

Hovav, A., & D'Arcy, J. (2012). Applying an extended model of deterrence across cultures: An investigation of information systems misuse in the US and South Korea. *Information & Management*, *49*(2), 99–110.

Hsu, J. S.-C., Shih, S.-P., Hung, Y. W., & Lowry, P. B. (2015). The role of extra-role behaviors and social controls in information security policy effectiveness. *Information Systems Research*, *26*(2), 282–300.

Hu, Q., Dinev, T., Hart, P., & Cooke, D. (2012). Managing employee compliance with information security policies: The critical role of top management and organizational culture. *Decision Sciences*, *43*(4), 615–660.

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

Humphrey, J. A., & Palmer, S. (2013). *Deviant behavior: Patterns, sources, and control*. Springer Science & Business Media.

Hunker, J., & Probst, C. W. (2011). Insiders and insider threats-an overview of definitions and mitigation techniques. *Journal of Wireless Mobile Networks, Ubiquitous Computing, and Dependable Applications*, *2*(1), 4–27.

IBM Security, & Ponemon Institute. (2023). *Cost of a data breach report 2023*. https://www.ibm.com/reports/data-breach.Accessed 24/10/2023

Ifinedo, P. (2012). Understanding information systems security policy compliance: An integration of the theory of planned behavior and the protection motivation theory. *Computers & Security*, *31*(1), 83–95.

Ifinedo, P. (2014). Social cognitive determinants of non-malicious, counterproductive computer security behaviors (CCSB): An empirical analysis. *Proceedings of the 8th Mediterranean Conference on Information Systems, Verona, Italy, September 03-05*. https://aisel.aisnet.org/mcis2014/18

Ifinedo, P. (2015). Effects of organizational citizenship behavior and social cognitive factors on employees' non-malicious counterproductive computer security behaviors: An empirical analysis. *CONF-IRM 2015 Proceedings. 36.* https://aisel.aisnet.org/confirm2015/36

Ifinedo, P. (2019). Investigating employee engagement in nonmalicious, end-user computing and information security deviant behavior. *AMCIS 2019 Proceedings. 8*. https://aisel.aisnet.org/amcis2019/info_security_privacy/info_security_privacy/8

Ifinedo, P. (2022). Exploring personal and environmental factors that can reduce nonmalicious information security violations. *Information Systems Management*, *40*(4), 1–21.

Ifinedo, P. (2023). Exploring personal and environmental factors that can reduce nonmalicious information security violations. *Information Systems Management*, *40*(4), 316–336.

Ifinedo, P., & Idemudia, E. C. (2017). Factors influencing employees' participation in non-malicious, information systems security deviant behavior: Focus on formal control mechanisms and sanctions. *AMCIS 2017 Proceedings. 21.* https://aisel.aisnet.org/amcis2017/InformationSystems/Presentations/21

Jiang, R. (2022). Exploring employees' computer fraud behaviors using the fraud triangle theory. *Pacific Asia Journal of the Association for Information Systems*, *14*(4), 4.

Jiang, R., & Zhang, J. (2023). The impact of work pressure and work completion justification on intentional nonmalicious information security policy violation intention. *Computers & Security*, *130*, 103253.

Johnston, A. C., Warkentin, M., & Siponen, M. (2015). An enhanced fear appeal rhetorical framework. *MIS Quarterly*, *39*(1), 113–134.

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.

Jones, A., & Colwill, C. (2008). Dealing with the malicious insider. *6th Australian Information Security Management Conference, Edith Cowan University, Perth, Western Australia*.

Kahneman, D. (1979). Prospect theory: An analysis of decisions under risk. *Econometrica*, *47*, 278.

Kahneman, D., & Tversky, A. (2013). Prospect theory: An analysis of decision under risk. In *Handbook of the fundamentals of financial decision making: Part I* (pp. 99–127). World Scientific.

Kanter, J. W., Manos, R. C., Bowe, W. M., Baruch, D. E., Busch, A. M., & Rusch, L. C. (2010). What is behavioral activation?: A review of the empirical literature. *Clinical Psychology Review*, *30*(6), 608–620.

Kanter, R. (1993). *Men and women of the corporation, 2nd ed, 1977*. BasicBooks.

Kanter, R. M. (1977). *Men and women of the corporation.* BasicBooks.

Kanter, R. M. (2008). *Men and women of the corporation: New edition*. BasicBooks.

Karjalainen, M., Siponen, M., & Sarker, S. (2020). Toward a stage theory of the development of employees' information security behavior. *Computers & Security*, *93*, 101782.

Karlsson, F., & Hedström, K. (2019). Value-Based Compliance Theory. In S. Jajodia, P. Samarati, & M. Yung (Eds.), *Encyclopedia of cryptography, security and privacy* (pp. 1–5). Springer.

Katz, A. M. (1976). Government information leaks and the First Amendment. *California Law Review, 64*, 108.

Katz, D. (1964). The motivational basis of organizational behavior. *Behavioral Science*, *9*(2), 131–146.

Khatib, R., & Barki, H. (2020). An activity theory approach to information security non-compliance. *Information & Computer Security*, *28*(4), 485–501.

Kidwell, B., & Jewell, R. D. (2008). The influence of past behavior on behavioral intent: An information-processing explanation. *Psychology & Marketing*, *25*(12), 1151–1166.

Kim, J. J., Park, E. H. E., & Baskerville, R. L. (2016). A model of emotion and computer abuse. *Information & Management*, *53*(1), 91–108.

Kohlberg, L. (1963). Moral development and identification. *Teachers College Record*, *64*(9).

Kohlberg, L. (1971). Stages of moral development. *Moral Education*, *1*(51), 23–92.

Kraemer, S., & Carayon, P. (2007). Human errors and violations in computer and information security: The viewpoint of network administrators and security specialists. *Applied Ergonomics*, *38*(2), 143–154.

Kuo, K.-M., Talley, P. C., & Huang, C.-H. (2020). A meta-analysis of the deterrence theory in security-compliant and security-risk behaviors. *Computers & Security*, *96*, 101928.

Kuutti, K. (1996). Activity theory as a potential framework for human-computer interaction research. *Context and Consciousness: Activity Theory and Human-Computer Interaction*, *1744*, 9–22.

Laffier, J., & Rehman, A. (2023). Deepfakes and harm to women. *Journal of Digital Life and Learning*, *3*(1), 1–21.

Lazarus, R. S. (1991). Progress on a cognitive-motivational-relational theory of emotion. *American Psychologist*, *46*(8), 819.

Lazarus, R. S., & Folkman, S. (1984). *Stress, appraisal, and coping*. Springer.

Lee, J., & Lee, Y. (2002). A holistic model of computer abuse within organizations. *Information Management & Computer Security*, *10*(2), 57–63.

Lee, S. M., Lee, S.-G., & Yoo, S. (2004). An integrative model of computer abuse based on social control and general deterrence theories. *Information & Management*, *41*(6), 707–718.

Li, H., Luo, X. R., & Chen, Y. (2021). Understanding information security policy violation from a situational action perspective. *Journal of the Association for Information Systems*, *22*(3),5.

Liang, H., & Xue, Y. L. (2010). Understanding security behaviors in personal computer usage: A threat avoidance perspective. *Journal of the Association for Information Systems*, *11*(7), 1.

Liang, H., Xue, Y., Pinsonneault, A., & Wu, Y. A. (2019). What users do besides problem-focused coping when facing IT security threats: An emotion-focused coping perspective. *MIS Quarterly*, *43*(2), 373–394.

Lin, C., & Kunnathur, A. S. (2013). Toward developing a theory of end user information security competence. *AMCIS 2013 Proceedings*. *1*. https://aisel.aisnet.org/amcis2013/ISSecurity/GeneralPresentations/1

Lindenberg, S., & Steg, L. (2007). Normative, gain and hedonic goal frames guiding environmental behavior. *Journal of Social Issues*, *63*(1), 117–137.

Lowry, P. B., Posey, C., Bennett, R. (Becky) J., & Roberts, T. L. (2015). Leveraging fairness and reactance theories to deter reactive computer abuse following enhanced organisational information security policies: An empirical study of the influence of counterfactual reasoning and organisational trust. *Information Systems Journal*, *25*(3), 193–273.

Luo, X. R., Li, H., Hu, Q., & Xu, H. (2020). Why individual employees commit malicious computer abuse: A routine activity theory perspective. *Journal of the Association for Information Systems*, *21*(6), 5.

Maalem Lahcen, R. A., Caulkins, B., Mohapatra, R., & Kumar, M. (2020). Review and insight on the behavioral aspects of cybersecurity. *Cybersecurity*, *3*, 1–18.

Maasberg, M., Warren, J., & Beebe, N. L. (2015). The dark side of the insider: Detecting the insider threat through examination of dark triad personality traits. *2015 48th Hawaii International Conference on System Sciences* (pp. 3518–3526).

McCormac, A., Zwaans, T., Parsons, K., Calic, D., Butavicius, M., & Pattinson, M. (2017). Individual differences and information security awareness. *Computers in Human Behavior*, *69*, 151–156.

McLeod, A., & Dolezel, D. (2022). Information security policy non-compliance: Can capitulation theory explain user behaviors? *Computers & Security*, *112*, 102526.

Milgram, S. (1963). Behavioral study of obedience. *The Journal of Abnormal and Social Psychology*, *67*(4), 371.

Milgram, S. (1974). *Obedience to authority: An experimental view.* Harper-Collins.

Moody, G. D., Siponen, M., & Pahnila, S. (2018). Toward a unified model of information security policy compliance. *MIS Quarterly*, *42*(1), 285-311.

Mou, J., Cohen, J. F., Bhattacherjee, A., & Kim, J. (2022). A test of protection motivation theory in the information security literature: A meta-analytic structural equation modeling approach. *Journal of the Association for Information Systems*, *23*(1), 196–236.

Mullen, P. (2023). *7 real-life insider threat examples*. https://acdsglobal.com/resources/blog/7-real-life-insider-threat-examples. Accessed 10/04/2024

Myyry, L., Siponen, M., Pahnila, S., Vartiainen, T., & Vance, A. (2009). What levels of moral reasoning and values explain adherence to information security rules? An empirical study. *European Journal of Information Systems*, *18*(2), 126–139.

Nasaescu, E., Marín-López, I., Llorent, V. J., Ortega-Ruiz, R., & Zych, I. (2018). Abuse of technology in adolescence and its relation to social and emotional competencies, emotions in online communication, and bullying. *Computers in Human Behavior*, *88*, 114–120.

Nehme, A. (2021). *Coping with information security fear appeals: A drive theory perspective* [PhD Thesis, Iowa State University].

Nehme, A., & George, J. (2020). Taking it out on IT: A mechanistic model of abusive supervision and computer abuse. *Hawaii International Conference on System Sciences*.

Öğütçü, G., Testik, Ö. M., & Chouseinoglou, O. (2016). Analysis of personal information security behavior and awareness. *Computers & Security*, *56*, 83–93.

Organ, D. W. (1988). *Organizational citizenship behavior: The good soldier syndrome.* (pp. xiii, 132). Lexington Books/D. C. Heath and Com.

Organ, D. W. (2014). Organizational citizenship behavior: It's construct clean-up time. In *Organizational citizenship behavior and contextual performance* (pp. 85–97). Psychology Press.

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

Page, M. J., McKenzie, J. E., Bossuyt, P. M., Boutron, I., Hoffmann, T. C., Mulrow, C. D., Shamseer, L., Tetzlaff, J. M., Akl, E. A., Brennan, S. E., & others. (2021). The PRISMA 2020 statement: An updated guideline for reporting systematic reviews. *International Journal of Surgery*, *88*, 105906.

Popken, B. (2018). *Facebook fires engineer who allegedly used access to stalk women*. https://www.nbcnews.com/tech/social-media/facebook-investigating-claim-engineer-used-access-stalk-women-n870526.

Posey, C., Roberts, T. L., & Lowry, P. B. (2015). The impact of organizational commitment on insiders' motivation to protect Organizational Information Assets. *Journal of Management Information Systems*, *32*(4), 179–214.

Puleo, A. J. (2006). Mitigating insider threat using human behavior influence models. *Theses and Dissertations*, *3455*.

Rajab, M., & Eydgahi, A. (2019). Evaluating the explanatory power of theoretical frameworks on intention to comply with information security policies in higher education. *Computers & Security*, *80*, 211–223.

Ratliff, K. M., & Hicks, S. J. (1998). Intrinsic and extrinsic motivational factors and Type A behavior pattern. *Modern Psychological Studies*, *6*(2), 2.

Rawls, J. (1971). *A theory of justice.* Harvard University Press.

Reeve, J. (2018). *Understanding motivation and emotion*. John Wiley & Sons.

Rentrop, C., & Zimmermann, S. (2012). Shadow IT. *Management and Control of Unofficial IT. ICDS* (pp. 98–102).

Richardson, R. (2008). CSI computer crime and security survey. *Computer Security Institute*, *1*, 1–30.

Roberts, R., Flin, R., Millar, D., & Corradi, L. (2021). Psychological factors influencing technology adoption: A case study from the oil and gas industry. *Technovation*, *102*, 102219.

Robinson, S. L., & Bennett, R. J. (1995). A typology of deviant workplace behaviors: A multidimensional scaling study. *Academy of Management Journal*, *38*(2), 555–572.

Rogers, R. W. (1975). A protection motivation theory of fear appeals and attitude change1. *The Journal of Psychology*, *91*(1), 93–114.

Rogers, R. W. (1983). Cognitive and physiological processes in fear appeals and attitude change: A revised theory of protection motivation. *Social psychology: A source book* (pp. 153–176). Guilford.

Rogers, R. W., & Deckner, C. W. (1975). Effects of fear appeals and physiological arousal upon emotion, attitudes, and cigarette smoking. *Journal of Personality and Social Psychology*, *32*(2), 222.

Rogers, R. W., & Prentice-Dunn, S. (1997). *Protection motivation theory.* D. S. Gochman (Ed.), *Handbook of health behavior and research, 1* (pp. 1–13). Springer.

Romney, M. (1995). Computer fraud-What can be done about it? *The CPA Journal*, *65*(5), 30.

Roszkowska, P., & Melé, D. (2021). Organizational factors in the individual ethical behaviour. The notion of the "organizational moral structure." *Humanistic Management Journal*, *6*, 187–209.

Ryan, R. M., & Deci, E. L. (2000). Self-determination theory and the facilitation of intrinsic motivation, social development, and well-being. *American Psychologist*, *55*(1), 68.

Sadeghi, B., Richards, D., Formosa, P., McEwan, M., Bajwa, M. H. A., Hitchens, M., & Ryan, M. (2023). Modelling the ethical priorities influencing decision-making in cybersecurity contexts. *Organizational Cybersecurity Journal: Practice, Process and People*, *3*(2), 127–149.

Safa, N. S., Maple, C., Watson, T., & Von Solms, R. (2018). Motivation and opportunity based model to reduce information security insider threats in organisations. *Journal of Information Security and Applications*, *40*, 247–257.

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

Salancik, G. R., & Pfeffer, J. (1978). A social information processing approach to job attitudes and task design. *Administrative Science Quarterly*, 224–253.

Scherer, K. R., Schorr, A., & Johnstone, T. (2001). *Appraisal processes in emotion: Theory, methods, research*. Oxford University Press.

Schmideberg, M. (1946). Psychological factors underlying criminal behavior. *Journal of Criminal Law and Criminology*, *37*(6), 458-476.

Schoenherr, J. R., & Thomson, R. (2020). Insider threat detection: A solution in search of a problem. *2020 International Conference on Cyber Security and Protection of Digital Services (Cyber Security)*.

Schryen, G. (2015). Writing qualitative is literature reviews—Guidelines for synthesis, interpretation, and guidance of research. *Communications of the Association for Information Systems*, *37*(1), 12.

Schwartz, S. H. (1992). Universals in the content and structure of values: Theoretical advances and empirical tests in 20 countries. In *Advances in experimental social psychology* (Vol. 25, pp. 1–65). Elsevier.

Shropshire, J., Warkentin, M., & Sharma, S. (2015a). Personality, attitudes, and intentions: Predicting initial adoption of information security behavior. *Computers & Security*, *49*, 177–191.

Shropshire, J., Warkentin, M., & Sharma, S. (2015b). Personality, attitudes, and intentions: Predicting initial adoption of information security behavior. *Computers & Security*, *49*, 177–191.

Sikolia, D., & Biros, D. (2016). Motivating employees to comply with information security policies. *Journal of the Midwest Association for Information Systems (JMWAIS)*, *2016*(2), 2.

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.

Simpson, E. H., & Balsam, P. D. (2016). *The behavioral neuroscience of motivation: An overview of concepts, measures, and translational applications*. Springer.

Siponen, M. T. (2000). A conceptual foundation for organizational information security awareness. *Information Management & Computer Security*, *8*(1), 31–41.

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

Siponen, M., Mahmood, M. A., & Pahnila, S. (2014). Employees' adherence to information security policies: An exploratory field study. *Information & Management*, *51*(2), 217–224.

Siponen, M., Pahnila, S., & Mahmood, M. A. (2010). Compliance with information security policies: An empirical investigation. *Computer*, *43*(2), 64–71.

Son, J.-Y. (2011). Out of fear or desire? Toward a better understanding of employees' motivation to follow IS security policies. *Information & Management*, *48*(7), 296–302.

Srivratanakul, T., Clark, J. A., & Polack, F. (2004). *Writing effective security abuse cases*. Department of Computer Science.

Steele, S., & Wargo, C. (2007). An introduction to insider threat management. *Information Systems Security*, *16*(1), 23–33.

Steg, L., Bolderdijk, J. W., Keizer, K., & Perlaviciute, G. (2014). An integrated framework for encouraging pro-environmental behaviour: The role of values, situational factors and goals. *Journal of Environmental Psychology*, *38*, 104–115.

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

Sykes, G. M., & Matza, D. (2017). Techniques of neutralization: A theory of delinquency. In *Delinquency and drift revisited, volume 21* (pp. 33–41). Routledge.

Tetlock, P. E. (1983). Accountability and complexity of thought. *Journal of Personality and Social Psychology*, *45*(1), 74.

Theoharidou, M., Kokolakis, S., Karyda, M., & Kiountouzis, E. A. (2005). The insider threat to information systems and the effectiveness of ISO17799. *Computers & Security, 24(6),* 472-484.

Trang, S. (2018). When does deterrence work? A moderation meta-analysis of employees™ information security policy behavior. *ICIS 2018 Proceedings. 4.* https://aisel.aisnet.org/icis2018/security/Presentations.

Trang, S., & Brendel, B. (2019). A meta-analysis of deterrence theory in information security policy compliance research. *Information Systems Frontiers*, *21*, 1265–1284.

Trieu, V.-H., Cooper, V., & Pallegedara, D. (2021). Employee's unauthorized disclosure of organizational information on social media: The role of emotions and boundary permeability. *Proceedings of the 42nd International Conference on Information Systems (ICIS 2021)*.

Trinkle, B. S., Warkentin, M., Malimage, K., & Raddatz, N. (2021). High-risk deviant decisions: Does neutralization still play a role? *Journal of the Association for Information Systems*, *22*(3), 3.

Tsohou, A., Karyda, M., & Kokolakis, S. (2015). Analyzing the role of cognitive and cultural biases in the internalization of information security policies: Recommendations for information security awareness programs. *Computers & Security*, *52*, 128–141.

Tyler, T., Dienhart, J., & Thomas, T. (2008). The ethical commitment to compliance: Building value-based cultures. *California Management Review*, *50*(2), 31–51.

United States Department of Justice. (2020a). *Former employee of medical packaging company sentenced to federal prison for disrupting PPE shipments*. https://www.justice.gov/usao-ndga/pr/former-

employee-medical-packaging-company-sentenced-federal-prison-disrupting-ppe.Accessed 14/5/2024

United States Department of Justice. (2020b). *San Jose man sentenced to two years imprisonment for damaging Cisco's network*. https://www.justice.gov/usao-ndca/pr/san-jose-man-sentenced-two-years-imprisonment-damaging-cisco-s-network.Accessed 14/05/2024

Van Slyke, C., & Belanger, F. (2020). Explaining the interactions of humans and artifacts in insider security behaviors: The mangle of practice perspective. *Computers & Security*, *99*, 102064.

Vance, A., & Siponen, M. T. (2012a). IS security policy violations: A rational choice perspective. *Journal of Organizational and End User Computing*, *24*(1), 21–41.

Vance, A., & Siponen, M. T. (2012b). IS security policy violations: A rational choice perspective. *Journal of Organizational and End User Computing*, *24*(1), 21–41.

Vance, A., Lowry, P. B., & Eggett, D. (2013a). Using accountability to reduce access policy violations in information systems. *Journal of Management Information Systems*, *29*(4), 263–290.

Vance, A., Lowry, P. B., & Eggett, D. (2013b). Using accountability to reduce access policy violations in information systems. *Journal of Management Information Systems*, *29*(4), 263–290.

Velazquez, L. (2020). *Examining information security policy violations, rationalization of deviant behaviors, and preventive strategies* [PhD Thesis, Northcentral University].

Vroom, V. H. (2005). On the origins of expectancy theory. In *Great minds in management: The process of theory development* (pp. 239–258). Oxford.

Wall, J. D., & Buche, M. W. (2017). To fear or not to fear? A critical review and analysis of fear appeals in the information security context. *Communications of the Association for Information Systems*, *41*(1), 13.

Warkentin, M., & Willison, R. (2009). Behavioral and policy issues in information systems security: The insider threat. *European Journal of Information Systems*, *18*(2), 101–105.

Warkentin, M., Walden, E., Johnston, A. C., & Straub, D. W. (2016). Neural correlates of protection motivation for secure IT behaviors: An fMRI examination. *Journal of the Association for Information Systems*, *17*(3), 1.

Warkentin, M., Willison, R., & Johnston, A. C. (2011). The role of perceptions of organizational injustice and techniques of neutralization in forming computer abuse intentions. *Americas Conference on Information Systems.*

Watson, R. T., & Webster, J. (2020). Analysing the past to prepare for the future: Writing a literature review a roadmap for release 2.0. *Journal of Decision Systems*, *29*(3), 129–147.

Weber, M. (1978). *Economy and society: An outline of interpretive sociology. Chapters VIII to XVI*. University of California Press.

Weber, M. (1991). *The nature of social action in Runciman, WG Weber: Selections in translation*. Cambridge University Press.

Weiss, H. M., & Cropanzano, R. (1996). Affective events theory. *Research in Organizational Behavior*, *18*(1), 1–74.

Wikström, P.-O. H. (2014). Why crime happens: A situational action theory. In G. Manzo (Ed.), *Analytical sociology* (pp. 71–94). Wiley.

Wikström, P.-O. H., Oberwittler, D., Treiber, K., & Hardie, B. (2017). Situational action theory. In *developmental and life-course criminological theories* (pp. 125–170). Routledge.

Wiley, A., McCormac, A., & Calic, D. (2020). More than the individual: Examining the relationship between culture and information security awareness. *Computers & Security*, *88*, 101640.

Willison, R. (2006). Understanding the perpetration of employee computer crime in the organisational context. *Information and Organization*, *16*(4), 304–324.

Willison, R., & Backhouse, J. (2006). Opportunities for computer crime: Considering systems risk from a criminological perspective. *European Journal of Information Systems*, *15*(4), 403–414.

Willison, R., & Lowry, P. B. (2018). Disentangling the motivations for organizational insider computer abuse through the rational choice and life course perspectives. *ACM SIGMIS database: The database for advances in information systems*, *49*(SI), 81–102.

Willison, R., Lowry, P. B., & Paternoster, R. (2018). A tale of two deterrents: Considering the role of absolute and restrictive deterrence in inspiring new directions in behavioral and organizational security. *Journal of the Association for Information Systems*, *19*(12), 1187–1216.

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.

Workman, M., & Gathegi, J. (2007). Punishment and ethics deterrents: A study of insider security contravention. *Journal of the American Society for Information Science and Technology*, *58*(2), 212–222.

Xu, F., Luo, X. R., & Hsu, C. (2020). Anger or fear? Effects of discrete emotions on employee's computer-related deviant behavior. *Information & Management*, *57*(3), 103180.

Yayla, A. (2011). Controlling insider threats with information security policies. *ECIS 2011 Proceedings. 242.* https://aisel.aisnet.org/ecis2011/242

Yazdanmehr, A., & Wang, J. (2023). Can peers help reduce violations of information security policies? The role of peer monitoring. *European Journal of Information Systems*, *32*(3), 508–528.

Yazdanmehr, A., Li, Y., & Wang, J. (2023). Employee responses to information security related stress: Coping and violation intention. *Information Systems Journal*, *33*(3), 598–639.

Zwilling, M., Klien, G., Lesjak, D., Wiechetek, Ł., Cetin, F., & Basim, H. N. (2022). Cyber security awareness, knowledge and behavior: A comparative study. *Journal of Computer Information Systems*, *62*(1), 82–97.

About the Authors

Emmanuel Anti is a doctoral student and a project researcher in the School of Technology and Innovations at the University of Vaasa, Finland. His research interests include insider threats and behavioral research in information and cybersecurity**.**

Tero Vartiainen is professor of information systems in the School of Technology and Innovations at the University of Vaasa, Finland. His research and development activities are based on an interpretive approach and consider cybersecurity, computer ethics, project management, and IT services. His articles have been published in IS journals such as Information Systems Journal, Communications for Association of Information Systems, and European Journal of Information Systems.