Emmanuel Anti

Insider Deviant Behavior in Cybersecurity

ACTA WASAENSIA 570

University of Vaasa
VAASAN YLIOPISTO

ISBN 978-952-395-230-0 (print)
978-952-395-231-7 (online)

ISSN 0355-2667 (Acta Wasaensia 570, print)
2323-9123 (Acta Wasaensia 570, online)

URN https://urn.fi/URN:ISBN:978-952-395-231-7

PunaMusta Oy, Joensuu, 2025.

ACADEMIC DISSERTATION

To be presented, with the permission of the Board of the School of Technology and Innovations of the University of Vaasa, for public examination on the 2nd of December, 2025, at noon.

Article based dissertation, School of Technology and Innovations, Information Systems

Author	Emmanuel Anti https://orcid.org/0009-0007-3802-4875
Supervisors	Professor Tero Vartiainen University of Vaasa. School of Technology and Innovations, Information Systems Science. Associate Professor Rebekah Rousi University of Vaasa. School of Marketing and Communication, Communication Studies.
Custos	Professor Tero Vartiainen University of Vaasa. School of Technology and Innovations, Information Systems Science.
Reviewers	Professor Carol Hsu University of Sydney. Business Information Systems. Professor Marko Niemimaa University of Agder. Department of Information Systems.
Opponent	Associate Professor Wael Soliman University of Agder. Department of Information Systems.

Tiivistelmä

Sisätoimijan poikkeava käyttäytyminen (insider deviant behavior, IDB) tieto- ja kyberturvallisuudessa on monimutkainen ja jatkuva haaste organisaatioille ja yhteiskunnalle. Perinteiset teknisiin, kriminologisiin, psykologisiin ja sosiologisiin teorioihin pohjaavat lähestymistavat eivät tavoita sisäuhkien kompleksisuutta käytännön konteksteissa. Tämä väitöskirja kokoaa neljän tutkimusartikkelin löydökset ja esittää ihmiskeskeisen viitekehyksen IDB-ilmiöiden ymmärtämiseksi ja hillitsemiseksi.

Tutkimus tunnistaa 46 teoriaa, jotka selittävät sisäpiiriläisten käyttäytymistä, mutta jotka ovat keskenään pirstaleisia psykologisten, organisatoristen, sosiokulttuuristen ja päätöksenteon näkökulmien välillä. Se kritisoi näiden teorioiden rajoituksia ja korostaa monitieteisen lähestymistavan tarvetta, jossa huomioidaan myös kontekstuaaliset, eettiset ja emotionaaliset tekijät. Erityisesti tutkimus tuo esiin käsitteen kognitiivinen poikkeavuus – usein sivuutetun mutta keskeisen sisäpiiriläistoiminnan edeltäjän – ja osoittaa, kuinka ajatukset ja asenteet voivat johtaa poikkeavaan käyttäytymiseen.

Tutkimus tarkastelee myös tekoälyn (AI) häiritsevää vaikutusta ja sitä, miten kehittyvät teknologiat muuttavat käsityksiä autonomiasta, oikeudenmukaisuudesta, valvonnasta ja stressistä – tekijöistä, jotka kytkeytyvät IDB-ilmiöihin. Ennaltaehkäiseväksi strategiaksi väitöskirja ehdottaa muotoiluajatteluun perustuvaa DESTIC-viitekehystä, jossa painottuvat empatia, yhteistyö ja iteratiivinen ongelmanratkaisu. Tämä osallistava malli painottaa kontekstiherkkiä ja eettisesti perusteltuja turvallisuusstrategioita.

Tutkimus siirtyy pois perinteisestä näkemyksestä, jossa sisäpiiriläiset nähdään joko täysin rationaalisina toimijoina tai pelkkinä sosioteknisinä riskeinä. Se puolustaa dynaamisia malleja, jotka huomioivat organisatorisen identiteetin, emotionaaliset kokemukset ja teknologiset realiteetit. Vaikka painopiste on tahallisessa poikkeavuudessa ja kehitetty viitekehys esitellään konseptuaalisella tasolla, tutkimus luo perustan tulevalle monitieteiselle, eettisesti tietoiselle ja käytännönläheiselle tutkimukselle digitaalisessa työympäristössä.

Asiasanat: sisätoimijan poikkeava käyttäytyminen (IDB), kyberturvallisuus, tekoäly (AI), teoreettiset viitekehykset, muotoiluajattelu (DT), tietoturva.

Abstract

Insider deviant behavior (IDB) in information and cybersecurity is a persistent challenge for organisations and society. Traditional approaches grounded in technocentric, criminological, psychological, and sociological theories provide fragmented explanations that do not fully capture the complexity of insider threats in practice. This dissertation synthesises findings from four research articles to propose a human-centered framework for understanding and mitigating IDBs, emphasising empathy and ethics in cybersecurity.

The study maps the theoretical landscape and identifies 46 theories that attempt to explain insider behaviour. These theories remain fragmented across psychological, organisational, sociocultural, and decision-making perspectives. The study critiques their limitations and calls for interdisciplinary integration that accounts for contextual, ethical, and emotional factors. This interdisciplinary approach, which draws from various fields, is crucial for a comprehensive understanding of insider deviant behavior.

The dissertation also addresses the disruptive role of artificial intelligence (AI) and how emerging technologies reshape notions of autonomy, justice, surveillance and stress – all of which are linked to insider deviance. As a mitigation strategy, it introduces a design thinking-based framework (DESTIC) built on empathy, collaboration, and iterative problem-solving. This participatory model promotes context-sensitive and ethically grounded security practices.

Moving beyond the traditional view of insiders as either rational actors or sociotechnical risks, the study argues for dynamic theoretical models that integrate organisational identity, emotional experience, and technological realities. Although focused primarily on intentional deviance and offering a conceptual application of the proposed framework, it provides a foundation for future interdisciplinary and ethically conscious research relevant to the digital workplace.

Keywords: Insider Deviant Behavior (IDB), Cybersecurity, Artificial Intelligence (AI), Theoretical Frameworks, Design Thinking (DT), Informational Security.

ACKNOWLEDGEMENT

First and foremost, I thank God for His grace, guidance, and unwavering mercy throughout this journey. His wisdom and strength carried me through moments of doubt and exhaustion, and His presence consistently offered hope and resilience. I am deeply thankful.

I am deeply thankful to my family, whose unwavering support and love have been the foundation of my academic journey. Their encouragement, patience, and practical help made it possible for me to study in Finland. Through every challenge and success, their belief in me has been my anchor. This achievement is as much theirs as it is mine.

I extend my deepest thanks to Professor Tero Vartiainen and Associate Professor Rebekah Rousi for their exceptional guidance and support. From the outset, they welcomed my ideas with openness and respect, providing invaluable guidance, constructive feedback, and ongoing encouragement. Their intellectual input and time commitment greatly influenced my growth as a researcher and helped me produce several publications. I am especially thankful for their assistance in obtaining project funding, which allowed me to focus more on my research with fewer constraints. It has been a privilege to work under their mentorship.

I also thank my external examiners, Professor Carol Hsu (University of Sydney) and Professor Marko Niemimaa (University of Agder), for their insightful and constructive feedback. Their comments not only improved the quality of this dissertation but also encouraged me to think more critically, expanding the scope and depth of my research in meaningful ways.

I sincerely thank Dang Duong for his consistent encouragement, collaboration, and generosity in co-authoring several of my articles. His willingness to share knowledge, offer guidance, and work closely with me played a key role in turning ideas into meaningful contributions.

I am grateful to Sayawu Diaba and Truth Lumor for their unwavering guidance and support, especially during the most challenging times of my academic journey. Their encouragement reminded me that I was never alone in facing challenges, and their assistance helped me stay focused and resilient.

This PhD reflects the belief, kindness, and support of many. Every gesture, spoken or silent, helped me reach this moment. Thank you.

Contents

Figures

Tables

Abbreviations

AI	Artificial Intelligence
AIPI	AI-Induced Perceived Inequity
AIWC	AI-Induced Workload Change
AIWS	AI-Induced Work Strain
DESTIC	Design Thinking for Insider Threat in Cybersecurity
DT	Design Thinking
IDB	Insider Deviant Behavior
IT	Information Technology
IS	Information Security
ISS	Information Systems Security
MCA	Malicious Computer Abuse

Articles

[1] 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), 4. *Published.* https://doi.org/10.17705/1CAIS.05501 © 2024 by the Association for Information Systems.

[2] Anti, E., Vartiainen, T., Rousi, R., & Dang, D. Limitations of Theories on Insider Deviant Behavior Research in Information Security: A Theoretical Review and Research Agenda. *Unpublished.*

[3] Anti, E., & Dang, D. (2025). Impact of Artificial Intelligence on Employee Strain and Insider Deviance in Cybersecurity. *PACIS 2025 Proceedings. Published.* https://aisel.aisnet.org/pacis2025/security/security/19. © The Authors.

[4] Anti, E., & Rousi, R. (2025). Mitigating Insider Threats in Cybersecurity: A Design Thinking Approach. *The Annual Symposium of Computer Science*. *Accepted.* © The Authors, CC BY.

In all four articles in this dissertation, I served as the first author and led the research process, including the design, conceptual development, and coordination of writing and analysis. The nature of each article and my contributions are summarized as follows:

Article 1: As the first author, I designed the review protocol, conducted the literature search and analysis, and co-wrote the manuscript with my co-author.

Article 2: As the first author, I designed the review framework, led the analysis, and coordinated contributions from co-authors, who supported data interpretation and provided general editorial feedback.

Article 3: I was the first author of this research-in-progress paper. I led the research design and literature review, jointly developed the

methodology, analyzed preliminary data, and co-wrote the paper with my co-author.

Article 4: As the first author of this paper proposing a design thinking-based framework for mitigating insider threats, I led the literature review, while my co-author led the conceptual development and study design; we co-wrote the paper.

1 INTRODUCTION

In today's digital world, it is essential for organizations in all industries to safeguard sensitive data against unauthorized access, misuse, exposure, tampering, disruption, or loss (Miryala & Gupta, 2022; Xu et al., 2024). The rapid expansion of digital assets, rising cyber threats like data breaches and ransomware, and growing dependence on IT and telecommunications have intensified concerns over privacy, security, and service disruptions (Bélanger & Crossler, 2011; Loch et al., 1992; Miryala & Gupta, 2022). In information security, the spread of data across various systems increases the risk of breaches, making it more challenging to ensure secure behavior among organizational insiders (Balozian et al., 2023). While significant advancements have been made in developing sophisticated cybersecurity tools and technologies to safeguard these assets, one of the most persistent and challenging threats comes from within the organization itself: the insider (Colwill, 2009; Hunker & Probst, 2011; Mady et al., 2023; Mazzarolo & Jurcut, 2019).

Threats originating from insiders can involve current or former employees, contractors, or business partners (Mills et al., 2017; Predd et al., 2008). Unlike external attackers, insiders possess legitimate access to sensitive systems and data, making their harmful actions more difficult to detect and mitigate (Bishop & Gates, 2008; Nurse et al., 2014). Deviant behaviors are often precursors to insider threats, as organizational insiders often engage in harmful actions that can compromise an organization's digital assets (Ifinedo, 2017; Torres & Crossler, 2024). Organizations are increasingly worried about 'malicious insiders' who act against the organization's best interests, leveraging their knowledge of the organization's systems and data (Schoenherr & Thomson, 2020). Furthermore, insider threats, ranging from fraud to sabotage, are particularly challenging to manage due to the perpetrator's authorized access, which amplifies their potential impact (Prabhu & Thompson, 2022).

A survey by Cybersecurity Insiders (2024) indicates that from 2019 to 2024, insider attacks saw a significant rise, with organizations reporting such incidents increasing from 66% to 76%. Concern over malicious insiders rose from 60% to 74%, with financial gain as the top motivation. A striking 90% of respondents found insider attacks more challenging to detect than external threats. The survey further indicated that ransomware attacks by insiders were on the rise, affecting 76% of organizations. In comparison, information disclosure (56%) and unauthorized data operations (48%) were seen as major concerns of most organizations (Cybersecurity Insiders, 2024). Additionally, the survey revealed that hybrid work risks were a concern for 70% of participants, while 75% expressed concern about new technologies, such as

AI. However, only 16% of organizations consider themselves highly effective at handling insider threats, up from 11% in 2019 (Cybersecurity Insiders, 2024). The data by Cybersecurity Insiders (2024) also shows that 66% of organizations feel vulnerable to insider attacks, while 41% have only partially implemented insider threat programs, highlighting weaknesses in threat monitoring and management. Further, only 29% of organizations feel fully equipped with the right tools, exposing a significant security shortfall.

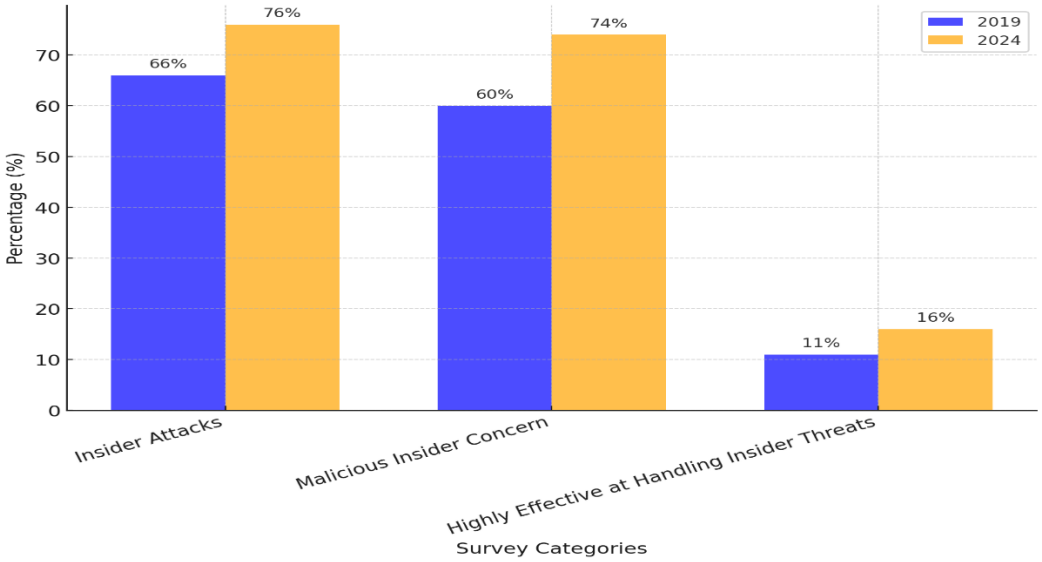

Figure 1. Insider Threat Statistics 2019 to 2024 (Cybersecurity Insiders, 2024)

Figure 1 summarizes the growing prevalence of insider attacks, highlighting increased organizational concern about malicious insiders. Financial gain is identified as the primary motivation, and insider threats are widely viewed as more difficult to detect than external ones.

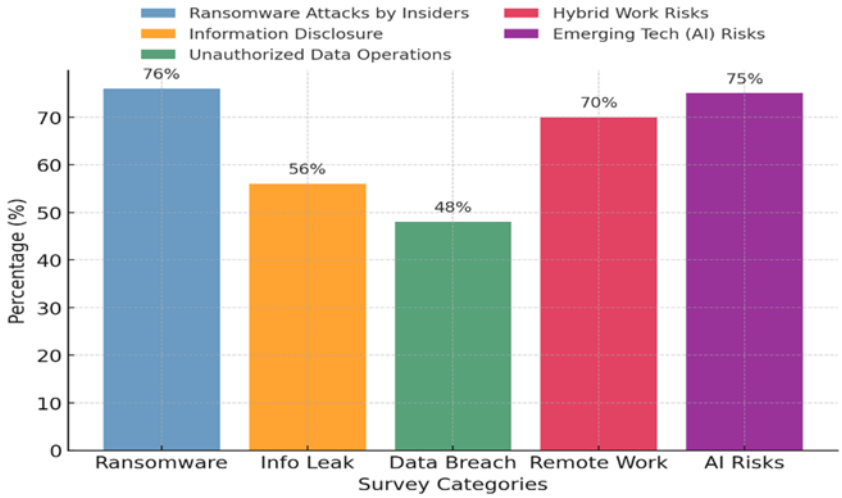

Figure 2. Insider Threat Statistics 2024 (Cybersecurity Insiders, 2024)

Figure 2 further highlights the increasing impact of insider threats, with a rise in ransomware attacks and growing concern over information disclosure and unauthorized data operations. Hybrid work environments and emerging technologies, such as AI, are introducing new layers of risk. Despite these challenges, only a small number of organizations feel confident in their ability to manage insider threats effectively.

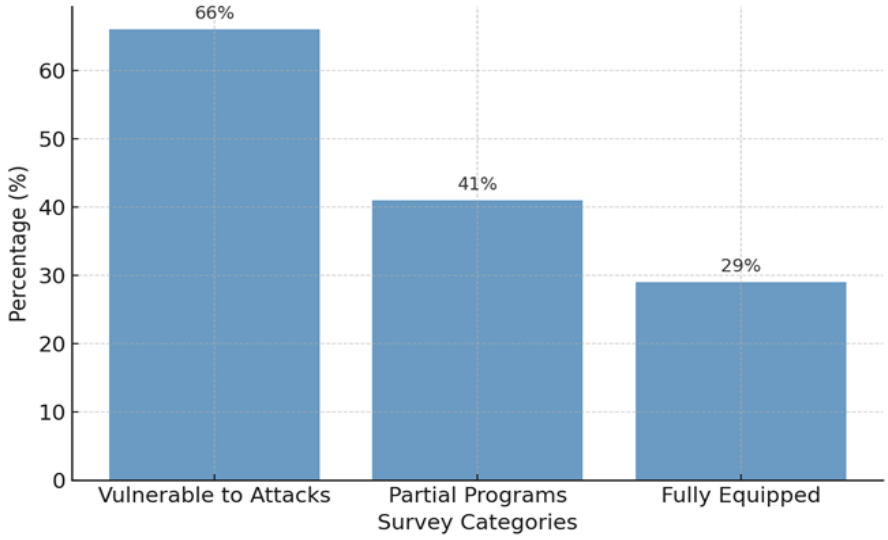

Figure 3. Insider Threat Program Maturity in Organizations 2024

Figure 3 also reflects a widespread sense of vulnerability among organizations to insider attacks. Many have only partially implemented insider threat programs, revealing gaps in monitoring and management. Additionally, few organizations feel

fully equipped with the necessary tools, pointing to a significant shortfall in security preparedness.

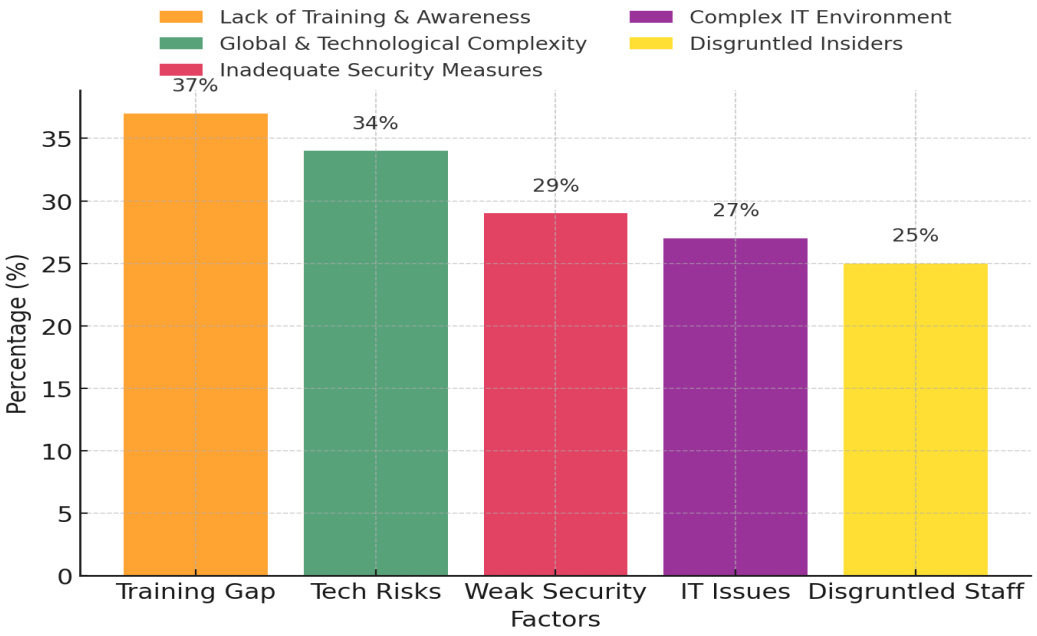

Figure 4. The Main Drivers Behind Increased Insider Attacks

The data suggests that while awareness of insider threats has increased, detection and prevention remain major challenges. Organizations are struggling to keep up with evolving threats, and while some improvements in preparedness have been made, most remain vulnerable due to incomplete security programs, behavioral insights, and insufficient tools. This highlights the need to understand insider behaviors in order to develop stronger security policies, more effective threat programs, and advanced monitoring for effective insider threat management.

Green (2014) notes that deviant actions, often triggered by workplace issues such as conflict or demotion, can lead to insider threats, including unauthorized access or manipulation of information systems, both of which are common forms of organizational misconduct. Humphrey and Palmer (2013) explain deviant behaviors as actions that deviate from accepted norms and policies. In cybersecurity, deviant behavior includes insider actions that may lead to security breaches (Green, 2014). Therefore, insider threats and deviant behaviors, whether driven by malicious intent, negligence, or unintentional errors, have become a significant concern for both public and private organizations, as well as cybersecurity professionals.

The study of insider threats and deviant behaviors in information systems and cybersecurity integrates several disciplines, including criminology, psychology, and

sociology, each providing theoretical frameworks to explain the reasons for insiders' engagement in deviant behavior. However, while these theories offer valuable insights, they often fail to fully capture the complexity of insider deviant behavior in modern information and cybersecurity contexts. Furthermore, as insider threats continue to be an evolving and growing risk, this thesis critically analyzes existing theories, identifies their limitations, and examines the influence of emerging technologies such as AI on insider deviant behaviors. Additionally, it examines how these technologies influence mitigation strategies and proposes strategies to address these evolving threats.

1.1 Problem statement

Insider deviant behavior (IDB) in cybersecurity is a complex phenomenon that is influenced by a variety of factors, including individual motivations and intentions (Lowry et al., 2015; Luo et al., 2020), organizational culture (Box & Pottas, 2014; Hina et al., 2019), and social dynamics (J. Lee & Lee, 2002; Yazdanmehr & Wang, 2023). Despite implementing advanced technologies to detect and prevent insider threats and deviant behaviors (Hunker & Probst, 2011; Liu et al., 2018; Sarkar, 2010), organizations are increasingly facing a surge in such incidents, leading to significant financial losses and damage to their reputations. The persistent rise in insider threats and deviant behaviors underscores a pressing disparity in current approaches, as many existing criminological, psychological, and sociological theories inadequately address the dynamic, evolving, and multifaceted nature of IDBs in current cybersecurity contexts.

Additionally, many organizations struggle to translate these theoretical insights into effective, proactive strategies for mitigating IDBs. Therefore, in this dissertation, I pose the following questions:

1. What is the current state of criminological, sociological, and psychological theories used to explain insider deviant behavior in cybersecurity research?

2. How can criminological, psychological, and sociological theories be critically analyzed and synthesized to better mitigate insider deviant behavior in information and cybersecurity?

This dissertation seeks to tackle the following fundamental issues: (1) the explanatory ability of current theories regarding IDBs; (2) the limitations of these theories in comprehensively understanding IDBs within cybersecurity; and (3) using theoretical frameworks to understand how emerging technologies like AI impact IDBs, thereby bridging the gap between theory and practice.

1.2 Objectives

This dissertation examines IDB in the context of information and cybersecurity, proposing practical solutions. These specific objectives are:

1. To conduct a systematic literature review of the current state of criminological, psychological, and sociological theories applied to understand IDB in information and cybersecurity.

2. To critically analyze the limitations of these existing theoretical frameworks in explaining IDBs.

3. To develop a theoretical framework that serves as a guide to analyze the complexities of IDB in information and cybersecurity research.

4. To integrate theory and practice, offering organizations a comprehensive framework to understand and mitigate emerging technologies, such as AI's impact on employee strain and malicious insider deviance in cybersecurity.

1.3 Outline of the thesis

The subsequent sections of this dissertation are structured as follows. Chapter 2 examines the literature review and theoretical framework related to insider deviant behaviors (IDBs). The chapter provides a detailed overview of behavioral research in information security, including the application of theories from criminology, psychology, and sociology, as well as the influence of emerging technologies on insider deviance. Chapter 3 presents a synthesis of four research articles, outlining their key findings. Chapter 4 explores the theoretical and practical implications of the research and proposes directions for future research. The final section includes the full texts of the original articles.

To provide clarity on how each article contributes to the overall research goals, Table 1 maps each research question (RQ) to the corresponding article(s) and highlights the conceptual progression across the dissertation.

Table 1. Overview of Research Questions and Article Contributions

Research Question (RQ)	Article(s)	Contribution	Connection to Other Articles
How do psychological, sociological, and criminological theories explain insider deviant behavior? **Behavior in information security?**	Article 1	Identified and categorized 46 theories applied to offer explanations in IDB research.	Establishes the theoretical foundation and highlights the fragmented nature of existing theories in explaining IDBs, thereby prompting a critical evaluation of their theories and applications in Article 2.
What are the limitations of psychological, sociological, and criminological theories applied to IDB research in information security?	Article 2	Analyzes the limitations and methodological challenges of 66 theories applied in IDB research	Builds on Article 1 by reviewing theoretical limitations and their applications, emphasizing the need for empirical and context-aware research, setting the stage for Article 3
How do AI-driven PMTs and ADMSs influence employee strain, and how does this strain contribute to insider deviance?	Article 3	Offers empirical insights into how AI systems implemented at workplaces affect insider deviance in cybersecurity	Responds to the gaps identified in Articles 1 and 2 by introducing a new explanatory lens to technological strain to provide evidence of its impact on insider behavior.
How can design thinking be applied to develop effective proactive strategies for preventing insider threats, while offering a deeper understanding of previous cases?	Article 4	Introduces the DESTIC framework based on design thinking principles as a mitigation strategy for insider threats	Analyzes existing insider threat mitigation strategies, many of which are informed by the theories discussed in Articles 1, 2, and 3 to propose a proactive, human-centered approach to prevention.

2 LITERATURE REVIEW AND THEORETICAL BACKGROUND

This literature review begins with an overview of behavioral information security, emphasizing the role of human behavior in cybersecurity. It then focuses on IDBs as the central issue. To investigate the underlying causes of IDBs, the review draws on criminological, psychological, and sociological theories. The final sections examine how emerging technologies are reshaping insider threats and introduce design thinking as a multidisciplinary approach to their mitigation. Each section links theoretical insights to practical challenges and innovative responses.

2.1 Overview of Behavioral Information Security

Behavioral information security research emerged in the late 1980s and early 1990s. Denning's (1982) seminal work on cryptography and data security recognized the interplay between human behavior and technical systems. Further, Denning (1982) emphasized the importance of psychological acceptability, stating that security mechanisms must be easy to use so that they are applied correctly and not bypassed. This highlights the need for security frameworks that account for human vulnerabilities, arguing that technical safeguards are insufficient without understanding user behavior. Straub (1990) contributed to this field by exploring deterrence mechanisms, including monitoring systems and sanctions. The research by Straub (1990) demonstrated that behavioral deterrents could effectively reduce violations by influencing employees' cost-benefit analyses of engaging in malicious activities. These insights emphasized the need for a balanced approach integrating psychological principles with technical measures.

Harrington (1996) also contributed to IS security studies through an analysis of how ethical codes and the psychological tendency to deny responsibility influence judgments and intentions related to computer misuse. Harrington (1996) found that IS-specific codes of ethics directly influenced judgments and intentions regarding computer sabotage, whereas generic company codes had no significant impact on these judgments and intentions. The study also highlighted that responsibility denial was a key factor in all forms of computer abuse, suggesting that personality traits may interact with ethical codes to shape behavior. This progression marks a shift in focus within behavioral information security research, from encouraging compliance and ethical conduct to unpacking the complex psychological and situational factors that underlie deviant behaviors, particularly insider threats.

During the early 2000s, Siponen (2000) advanced the study of security policy compliance, emphasizing the role of organizational and cultural factors in shaping

secure behaviors. This study highlighted that effective leadership and a healthy organizational culture are crucial for fostering security awareness. They enhance intrinsic motivation and perceived usefulness, ensure that security guidelines are clear, relevant, and justified, and balance extrinsic motivators, such as fear appeals, with intrinsic motivation through guidance and support. Additionally, the study recommended a multifaceted strategy that combines education, active participation, and persuasive communication to enhance security awareness and user commitment effectively.

Schultz (2002) explored psychological and organizational factors behind malicious and negligent behaviors. According to Schultz (2002), insider attacks are more likely to occur when organizational authority structures break down, with attackers often driven by job dissatisfaction and a desire to "make a statement," while insider abuse is frequently associated with individuals who are introverted, struggle with stress or conflict, and experience workplace frustration. The study highlighted that addressing insider risks requires integrating technical measures with behavioral analytics, using multiple indicators for effective detection. It proposed a framework that supports proactive threat detection systems and insider threat management programs.

Von Solms (2001) complemented this focus by emphasizing the critical role of organizational governance and leadership. Von Solms (2001) asserts that information security should be a senior management and board-level responsibility, aligned with organizational objectives, supported by robust governance frameworks, and driven by leadership that fosters a security-conscious culture through behavior-focused policy development and enforcement. Further, Von Solms (2001) indicated that effective cybersecurity relies on robust governance frameworks and strong leadership that fosters a security-conscious culture through behavior-focused policy development and enforcement. Lee et al. (2004) also emphasized the need to view information security as a social and organizational issue, highlighting human factors like integrity, trust, and ethics.

Warkentin and Willison (2009) further extended this research by emphasizing the critical need to address insider threats by understanding the human element in organizations. They argue that research should focus on employees' compliance, the motivations behind breaches, and their perceptions of security policies, while advocating for comprehensive approaches that involve hiring, training, and motivation to enhance information security. Similarly, Lowry and Moody (2015) have advanced behavioral research on insider threats by demonstrating the importance of socio-organizational elements in conjunction with technical solutions. They highlight employees as significant security risks, and advocate for strategies that foster

compliance with information security policies by addressing employee motivations and behaviors.

These studies have significantly advanced the field of information and cybersecurity by addressing employee or insider behaviors. The studies emphasize the importance of user-centric policy design, prioritizing clarity, fairness, and leadership engagement to ensure compliance. Research on insider threats has underscored the necessity for a combination of behavioral analytics and technical controls to facilitate proactive risk management. Trust and transparent communication are also needed to enhance employee engagement, as they can help reduce resistance to security measures. Furthermore, integrating behavioral insights into cybersecurity has shifted the focus from purely technical defenses to holistic strategies, emphasizing human vulnerabilities and providing actionable frameworks for policies, training, and systems that align with human behavior.

Despite significant progress and the impact of behavioral research in information and cybersecurity, there are still deficiencies in explaining, predicting, and prescribing solutions for insider threats and behaviors. This is due to the complexity of human behavior, the fragmented integration of interdisciplinary theories, and the nuanced understanding of motivations and situational factors.

2.2 Deviant Behavior

Deviant behavior refers to actions or beliefs that contravene established norms, rules, or customs, with its interpretation varying across normative and situational contexts (Goode, 2022; Humphrey & Schmalleger, 2012). Normatively, deviant behavior involves widely recognized violations, such as theft or substance abuse. Situationally, it depends on the context, as in the case of inappropriate behavior in formal settings (Goode, 2022). Cognitive deviance, defined as unconventional beliefs that conflict with societal norms, often leads to social marginalization, criticism, or punishment (Goode, 2015; Pals & Engin, 2019). For instance, believing the Earth is flat despite overwhelming scientific evidence may be considered cognitive deviance, as it diverges from the consensus and incurs social consequences such as ridicule or exclusion. Hanimoglu (2018) elaborates that deviant behaviors often stem from individual actions that disrupt social, moral, or cultural values, characterized by persistence, self-destructive tendencies, or social harm. These behaviors pose significant threats to the social and physical survival of individuals in collective settings.

Roberson and Garrido (2015) and Robinson and Bennett (2024) describe workplace deviance as voluntary, norm-violating behavior threatening organizational well-

being, including theft, fraud, or unauthorized disclosures. While deviance can include beneficial norm violations (positive deviance)(Robinson & Bennett, 2024), which may benefit individuals or organizations depending on their intent and outcomes, this study examines both positive and harmful behaviors, with a particular focus on understanding how deviant behaviors can impact individuals and organizations. However, previous definitions largely exclude cognitive deviance, which this dissertation incorporates as a critical precursor to physical actions. For example, disrupting organizational operations through technical means involves a mental and physical process, analyzing systems, identifying weaknesses, formulating plans, and justifying the behavior.

This study argues that deviant behavior arises from deliberate cognitive and physical actions. Thus, deviant behavior refers to intentional mental or physical actions that violate the standards, rules, or policies of a social group or organization, potentially leading to either beneficial or harmful consequences(Anti & Vartiainen, 2024). This thesis broadens the concept of deviance to include deliberate mental and physical actions that violate organizational norms. It argues that cognitive deviance often precedes observable misconduct and should be integrated into definitions of IDB.

2.3 Insider Threats and Insider Deviant Behavior

An insider is a current or former employee, contractor, business partner, or any individual with authorized access to an organization's network, systems, or data (Brackney & Anderson, 2004; Costa et al., 2014). Insiders operate within an organization’s security boundary, leveraging their legitimate access to sensitive information and resources. This access can be intentionally or unintentionally misused, posing significant threats to the confidentiality, integrity, and availability of organizational information and systems (Pfleeger et al., 2009).

Malicious insider actions are deliberate and often involve data theft, fraud, sabotage, intellectual property theft, espionage, or disrupting critical IT services (Costa et al., 2014; Willison & Warkentin, 2013). In contrast, non-malicious insider actions, although unintentional, can also cause substantial damage, such as accidental data leaks and unintentional security policy violations (Pfleeger et al., 2009). Both forms of insider actions pose a threat to an organization’s data, processes, and resources, underscoring the complexity of addressing insider threats.

Rauf et al. (2023) emphasize that insiders, often disgruntled employees, rogue agents, or intrusive applications, are uniquely challenging to detect and mitigate due to their legitimate access to organizational resources. Bishop and Gates (2008) identify two core insider capabilities: the ability to breach security policies through authorized

access and the ability to violate access controls through unauthorized means. Similarly, Willison and Warkentin (2013) emphasize the risks posed by insiders, who possess detailed knowledge of internal systems and procedures, enabling them to exploit vulnerabilities and leak sensitive information through lawful or unlawful means.

In this dissertation, I argue that insiders, who are entrusted with legitimate access and extensive knowledge of organizational systems, are uniquely positioned to engage in deviant behavior that violates organizational norms and policies. Their behavior, whether malicious (such as theft, sabotage, and fraud) or non-malicious (like accidental data leaks or policy violations), reflects both cognitive and physical dimensions. While malicious actions are driven by deliberate intent, non-malicious actions often result from negligence, oversight, or lack of awareness. Therefore, IDB in this dissertation is defined as "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''(Anti & Vartiainen, 2024, p.4).

2.4 Criminology in Cybersecurity Research

Wolfgang (1963) defines criminology as the study of crime as a social phenomenon, focusing on the making, breaking, and societal reactions to laws, to develop verified principles and knowledge about crime and its treatment. Burke (2018) highlights that criminological theories delve into the causes and dynamics of criminal behavior by examining physiological, psychological, and social factors. These include individual motivations, environmental factors, and societal influences (Mensah, 2024). Mensah (2024) further indicates that criminological theories provide frameworks for understanding the details of criminal behaviors and their underlying causes, which include the complex motives, cultural influences, psychological triggers, and environmental elements that drive such behavior. In behavioral research, criminological theories are applied to analyze patterns of deviance, identify risk factors for criminality, and inform preventative measures (Leukfeldt & Yar, 2016).

Criminological theories are crucial for understanding insider threats and deviant behaviors in the context of information and cybersecurity. Deterrence theory (Beccaria, 1963; Gibbs, 1968), for example, posits that individuals make calculated decisions about engaging in harmful actions by weighing the potential benefits, such as financial gain or revenge, against the perceived risks, e.g., certainty, severity, and swiftness of detection and punishment. Therefore, Deterrence theory offers a valuable framework for understanding and mitigating insider threats in

cybersecurity through measures like stricter penalties or increased surveillance. Additionally, Paternoster and Simpson (1996) contributed to deterrence research by challenging traditional sanction-based models, demonstrating that personal moral codes, informal sanctions, and organizational moral climate are crucial in deterring corporate crime, often outweighing formal legal penalties. However, Siponen et al. (2022) note that while deterrence theory has been essential in shaping compliance-focused information security (IS) policies by emphasizing perceived sanctions, its effectiveness is limited by the lack of distinction between general and specific deterrence, insufficient consideration of dynamic factors, and unexplored assumptions. Similarly, Routine Activity Theory (Cohen & Felson, 1979) focuses on the convergence of motivated offenders, suitable targets, and the absence of capable guardians, highlighting how vulnerabilities in systems or sloppy oversight can create opportunities for insider threats. According to Luo et al. (2020), this theory has been effectively applied in IS to explain and prevent malicious computer abuse (MCA). However, its application faces challenges due to the complexity of cybercrimes, evolving threats, and the need for integration with other theories to comprehensively address employee behavior. Another relevant theory is the General Strain Theory (Agnew, 1985, 1992), which suggests that individuals under significant stress or pressure may turn to deviant behaviors as a coping mechanism. In a cybersecurity context, insiders facing workplace dissatisfaction, financial problems, or personal grievances may be more likely to engage in data theft or sabotage (Dang, 2014). These theories enable organizations to understand the root causes of IDBs better and inform the development of more comprehensive security strategies, such as addressing workplace grievances and enhancing internal surveillance and controls.

2.5 Psychology in Cybersecurity Research

According to Colman (2016), psychology is defined as the study or science of behavior, but this definition can be limiting, as it often overlooks the mental processes underlying behavior. Psychological theories serve as intellectual frameworks that provide accurate predictions of observed phenomena and offer practical tools for answering questions and solving problems within specific domains (Cacioppo et al., 2004). Psychological theories aim to explain how individuals think, feel, and behave by emphasizing subjective and personal factors (Kwon & Silva, 2020). These factors include attitudes, subjective norms, psychological distance, fear appeal, beliefs and values, reasons, interests, satisfaction, probabilities, risks, heuristics, and conflicting interests (Kwon & Silva, 2020). In behavioral research, psychological theories explain behaviors by identifying correlations between psychological variables and delinquent behavior, focusing on contingencies that maintain non-conforming, often labeled deviant behavior (Moore, 2011). Thus, these theories provide a foundation

for understanding and predicting human actions, offering insights into why people make certain decisions, how they respond to stimuli, and what factors influence their behaviors over time.

Psychological theories are crucial for understanding insider threats and deviant insider behaviors in the context of information and cybersecurity. Insiders who are employees or trusted individuals within an organization pose unique risks because they already have authorized access to systems and data (Homoliak et al., 2019; Yuan & Wu, 2021). Psychological models, such as the Fear Appeal Theory (Rogers, 1975; Rogers & Deckner, 1975) and the Rational Choice Theory (Hogarth & Reder, 1987), help explain how personal motives, peer influences, and environmental factors contribute to harmful actions like data theft, sabotage, or negligence. According to Mattson et al. (2023), fear can drive deviant behaviors by triggering maladaptive coping mechanisms, such as fear avoidance, disrupting rational decision-making, and promoting risk-averse actions perceived as necessary to mitigate the fear.

Similarly, Willison et al.(2018) explain that deviant behaviors are influenced by a rational evaluation of costs and benefits. This is where individuals weigh potential rewards against the likelihood and severity of sanctions, choosing deviance if the benefits outweigh the risks or avoiding it if the risks are too high. Furthermore, IDBs can stem from perceived injustices within the workplace or rationalizations for unethical actions, which can be studied under the framework of Neutralization Theory (Gresham & David, 1957; Sykes & Matza, 2017). Trinkle et al. (2021) also explain that neutralization influences deviant behaviors by allowing individuals to rationalize their actions through justifications that reduce guilt or shame, thereby diminishing the deterrent effect of even severe organizational sanctions. Applying these theories within cybersecurity research helps organizations identify and mitigate the risks associated with insider threats. Behavioral profiling, for example, can identify anomalies in user behavior that signal a potential danger. Furthermore, these theories inform the development of training programs and organizational policies designed to reduce risky behaviors by addressing the psychological factors that drive them.

While theories such as neutralization, rational choice, and fear appeals offer valuable insights into insider behaviors in information and cybersecurity, they face notable limitations in fully accounting for deviant actions. These limitations stem from several factors: uncertainty about when neutralization occurs in the decision-making process, the complexity of situational and emotional influences that are difficult to model, the assumption of purely rational behavior in rational choice theory, and the variability in individual fear responses and coping mechanisms. Collectively, these challenges hinder the ability of such theories to predict deviant behavior consistently.

2.6 Sociology in Cybersecurity Research

Giddens and Griffiths (2006) define sociology as the scientific study of human social life, groups, and societies. Sociological theories offer frameworks for understanding how social structures, institutions, and relationships shape individual behaviors and societal outcomes (Wahab et al., 2023). These theories examine factors such as social norms, group dynamics, power relations, and cultural expectations, which shape the actions and decisions of individuals within their social environments (Roos et al., 2015). In behavioral research, sociological theories emphasize the role of social interaction and the impact of external social forces on behavior, rather than focusing solely on individual motivations (Kwon & Silva, 2020). These theories are essential for understanding how social contexts and interactions shape individual and group behaviors. These social contexts and interactions can both encourage and discourage deviant behavior by shaping it through negative influences (e.g., peer pressure) and deterring it through positive influences (e.g., strong family ties or community support).

Within the realm of information and cybersecurity, sociological theories play a pivotal role in elucidating how social ties, cultural influences, and group interactions can either foster or deter insider threats and deviant actions. For instance, Social Control Theory (SCT) (Agnew, 1991; Hirschi, 1969, 2017) posits that robust social bonds within organizations can significantly reduce the likelihood of deviant behaviors. This means that individuals with strong attachments to their peers or the organization are less likely to engage in harmful actions. According to Yayla (2011), Social Control Theory suggests that weak bonds to an organization, such as low attachment, commitment, involvement, and a lack of belief in its values, increase the likelihood of insider threats. However, strengthening these bonds through socio-behavioral controls can help mitigate such risks. This understanding enables organizations to take proactive measures that foster strong social bonds, thereby reducing the risk of insider threats.

Lee et al. (2004) applied SCT to explain insider computer abuse and advocated for comprehensive security policies that align with organizational objectives. The study found that strengthening social bonds through organizational trust can deter insider computer abuse, as individuals with strong attachments, commitments, and involvement are less likely to engage in misconduct. Furthermore, Lee et al. (2004) emphasized that participation in meetings, personal relationships, and company loyalty all play key roles in mitigating insider threats. Sociological perspectives help to identify the broader social contexts that contribute to insider threats, such as toxic workplace cultures (Folger & Cropanzano, 2001; Rawls, 1971), power imbalances, or group dynamics (Hofstede, 1984; Hofstede & McCrae, 2004) that encourage risky

behaviors. By applying these theories, organizations can design more effective interventions, such as fostering a positive organizational culture, enhancing social accountability, and addressing the structural causes of dissatisfaction. This broader understanding helps mitigate insider threats and deviant behaviors by focusing on both the individual and the social factors that influence behavior.

It is essential to acknowledge that while sociological theories are valuable in understanding and mitigating deviant behaviors, they also have their limitations. According to Alshare et al. (2018) and Yayla (2011), these theories may not fully address the complex dynamics of individual perceptions, biases, and motivation. For instance, while procedural, distributive, and interactional justice are considered important, perceptions of fairness are subjective and influenced by personal factors. Additionally, interactional justice has been found to lack significant predictive power for certain behaviors, such as information security violations, suggesting limitations in its applicability. Moreover, these theories focus on socio-behavioral aspects and do not integrate effectively with technical controls and organizational policies, which are essential for a comprehensive approach to mitigating deviant behaviors.

While criminological, sociological, and psychological theories offer valuable insights into the drivers of IDBs, they often fall short in addressing two critical dimensions: the internal cognitive processes that individuals use to justify harmful actions, and the evolving role of technology in facilitating such behaviors.. Cognitive deviance, which can be manifested through mechanisms such as moral disengagement, denial of responsibility, or perceived injustice, offers a useful lens for understanding how individuals rationalize harmful actions, even within ethically sound environments (Chen et al., 2019). At the same time, emerging technologies as artificial intelligence (AI), quantum computing, and the Metaverse are reshaping the insider threat landscape by amplifying the scale, subtlety, and complexity of potential attacks. These technologies introduce new vectors for exploitation, automate malicious capabilities, and blur the boundaries between physical and digital environments. Addressing these evolving threats requires a multidisciplinary approach—one that integrates behavioral theory, cognitive insight, and technological awareness—to fully understand and mitigate the risks posed by modern insider threats.

2.7 Emerging Technologies and Insider Threats

Building on the theoretical understandings of insider behavior, this section examines how emerging technologies such as AI, quantum computing, and the Metaverse are expanding the capabilities and complexities of insider threats. Cybersecurity Insiders (2024) reports significant concerns about these technologies, emphasizing fears of

misuse and their potential to transform and amplify insider threats due to their advanced capabilities. According to a report by the World Economic Forum (2025), emerging technologies such as AI are expected to have a significant impact on cybersecurity, with 66% of organizations recognizing its importance. However, only 37% have implemented safeguards for the secure deployment of AI. Additionally, 47% of organizations are concerned about adversarial advances from generative AI, while vulnerabilities introduced by quantum, decentralized, and satellite technologies further complicate cybersecurity strategies (World Economic Forum, 2025). IBM (2024) highlights that AI and automation are revolutionizing cybersecurity by enabling large-scale attacks for bad actors while equipping defenders with tools to identify and automate responses to threats quickly. For example, deepfakes, hyper-realistic synthetic media created using advanced AI techniques, can take various forms—text, audio, images, or videos—capable of mimicking writing styles, altering voices, swapping faces, or generating seemingly authentic content, posing significant risks as reliance on digital identities continues to grow (Tong et al., 2024; Vasist & Krishnan, 2022).

Deepfake technology, initially popularized for creating fake videos of public figures, has expanded to broader applications, raising concerns about security and trust in digital interactions (Seymour et al., 2021). Deepfakes simulating realistic faces and voices pose risks to authentication processes, enabling malicious actors to impersonate individuals and compromising information integrity (Seymour et al., 2021; Tong et al., 2024). According to Almuthaybiri et al. (2024), deepfakes can threaten an organization's brand, enabling threat actors to conduct social engineering attacks that compromise networks, communications, and sensitive information. Aside from the threats posed by AI, many organizations are leveraging it to streamline operations, reduce bottlenecks, free up human resources, and enhance efficiency and performance (Mikalef et al., 2023).

However, adopting and integrating AI technologies can pose challenges for employees, including skill gaps, job insecurity, increased workloads, cognitive overload, shifts in organizational culture, and higher turnover rates (Mikalef et al., 2023). For example, the fear of job loss, uncertainty about the future, and diminished human interaction due to the prioritization of AI integration can increase stress and anxiety (Matsunaga, 2022). These challenges can inadvertently contribute to the emergence of insider threats and deviant behaviors. For instance, Castro (2019) highlights that Amazon's use of AI technologies such as Performance Management Tools (PMTs) to track worker productivity and automate warnings or terminations has resulted in thousands of annual job losses, indicating that such systems create pressure to meet high performance benchmarks, leading to stress, job dissatisfaction, and high employee turnover. When technologies such as AI are perceived as a threat,

individuals may cope through fear or anger, potentially leading to deviant actions that compromise organizational security (Kim et al., 2016; Yazdanmehr et al., 2023). For example, employees who perceive unfairness in AI-driven hiring, discipline, or termination processes may resort to sabotage or other harmful actions as a form of financial or emotional retaliation.

The threats posed by insiders regarding emerging technologies, such as AI, highlight the need for a multidisciplinary approach to understanding and mitigating these risks by merging technical defenses with behavioral science, ethics, and organizational strategy. Applying theories in the same vein as General Strain Theory (Agnew, 1985, 1992), for instance, can help explain how stressors, such as job insecurity or performance pressures, drive deviant behaviors. The Fraud Triangle Theory (Albrecht et al., 1984, 2008) can provide insights into the elements of opportunity, pressure, and rationalization that contribute to unethical or deviant actions. Together, these frameworks can provide a comprehensive lens for exploring the psychological, social, and situational factors that influence insider threats, enabling organizations to develop more effective strategies to safeguard against these risks. Without this integration, mitigation strategies risk overlooking the human factors that drive deviance.

As emerging technologies introduce increasingly complex and evolving challenges in managing insider threats, traditional mitigation approaches, whether grounded in technical solutions or theoretical models, are often insufficient when used alone. This underscores the need for a practical and multidisciplinary approach that combines human-centered insights with iterative problem-solving. The following section introduces Design Thinking as a promising framework that addresses this gap, offering innovative and user-focused strategies for understanding and mitigating insider deviant behaviors.

2.8 Design Thinking as a Practical Approach to Insider Threat Mitigation

In response to the challenges of mitigating insider threats, this section examines Design Thinking as a novel and human-centered approach that complements existing technical and socio-technical methods. Insider threat mitigation in information and cybersecurity has been approached through technical, socio-technical, and sociological approaches, each with its benefits and drawbacks. Technical methods, such as IDS and deep learning, can detect suspicious behavior but struggle with identifying intent and adaptive threats (Elmrabit, 2018; Yuan & Wu, 2021). Socio-technical strategies integrate policies and human factors but face high costs and

limited applicability (Saxena et al., 2020). Sociological and psychological approaches to motivation and culture utilize deterrence and behavioral theories, but are often resource-intensive and subjective (Khan et al., 2021; Safa et al., 2018). None of these approaches has delivered a cohesive, practical, and multi-layered strategy for mitigating insider deviance, highlighting the need for a novel approach like Design Thinking (DT). What sets Design Thinking apart from traditional insider threat responses is its emphasis on understanding user motivations and co-creating solutions based on real-world feedback. While most existing approaches prioritize prevention or detection, Design Thinking focuses on empathy, iteration, and contextual understanding. This makes it particularly well-suited to addressing the fluid and context-specific nature of insider deviance.

DT is an iterative, user-centered process that combines analytical and creative approaches to redefine problems, challenge assumptions, and develop innovative solutions through experimentation, prototyping, feedback, and redesign. It is both a science of understanding design cognition (i.e., that which is also present in IDB) and a hands-on methodology for identifying alternative strategies and solving complex problems effectively (Dam & Siang, 2021; Razzouk & Shute, 2012). DT, at its core, focuses on design practices such as framing and frame creation, utilizing creativity, innovation, deep user understanding, and experimentation to tackle complex problems and develop effective, practical solutions (Dorst, 2011). Further, DT, increasingly applied across several fields such as IT, business, education, medical, and behavioral research, is a multifaceted framework for addressing complex, human-centered issues by using intuitive and emotional insights to investigate human behaviors and motives (Dam & Siang, 2021; Dorst, 2011; Micheli et al., 2019; Razzouk & Shute, 2012).

DT has been effectively applied in cybersecurity studies to address various challenges. Dorasamy et al. (2019) employed the five stages of DT—Empathy, Define, Ideate, Prototype, and Test to address low cybersecurity awareness among working youths in an IoT environment. The study identified a lack of knowledge as the core problem. It developed an interactive cybersecurity e-brochure cum playbook, refined through feedback from the target group, to enhance awareness and preparedness. Similarly, Ashenden et al. (2021) applied DT to develop cyber deception techniques, focusing on problem understanding, ideation, and prototyping. Using provocations from deception activities to stimulate ideas and journey mapping to refine them, an online DT workshop facilitated the integration of deception techniques from diverse contexts, resulting in more nuanced cyber deception tools. These studies highlight DT's versatility in addressing cybersecurity issues through innovative, user-centered solutions.

The application of DT in cybersecurity highlights how it can aid in developing interventions for insider threats and deviant behaviors by focusing on the user experience and motivations. Additionally, DT can enable researchers to explore how individuals interact with systems, processes, and environments, and how they influence their behavior. By emphasizing the iterative stages of DT (empathize, define, ideate, prototype, and test), it can be used to understand the underlying reasons behind certain behaviors (mindset, needs, and values), offering insights into how interventions might be designed to elicit positive behavioral changes (Dorasamy et al., 2019). DT can further encourage organizations to view security as both a technical and human-centered challenge. For instance, applying design thinking to research insider threats and deviant behaviors involves understanding the psychological and social factors that drive insiders to commit deviant acts, such as stress, dissatisfaction, or peer influence. Through empathy and iterative problem-solving, organizations can create more user-friendly systems, polices, and strategies to mitigate such harmful behaviors and promote a positive security culture.

3 SUMMARY OF THE ARTICLES

This chapter summarizes the articles included in this dissertation, outlining the research problems, methodologies employed, and synthesizing key findings and results.

3.1 Article 1: Explanations of Insider Deviant Behavior in Information Security: A Systematic Literature Review

Insider deviant behavior (IDB) in information security has become a critical issue for organizations due to the unique risks posed by insiders with privileged access and detailed knowledge of systems. Actions such as data theft, sabotage, and system abuse can lead to severe consequences, including the loss of sensitive information, reputational damage, financial losses, and disruptions to business operations. Addressing these threats requires a thorough understanding of the underlying motivations that drive insiders to engage in such behaviors (Schoenherr & Thomson, 2020). To date, information security researchers have drawn on psychological, sociological, and criminological theories to explain IDBs, providing valuable insights into the motivations and intentions behind these actions (Cram et al., 2017). However, these studies often present fragmented perspectives and face limitations in fully capturing the complexity of insider behaviors, particularly in the evolving landscape of information and cybersecurity.

In this study, we sought to address these gaps by systematically reviewing the theories applied in information security research on insider deviant behavior, examining key constructs, evaluating their explanatory power, and highlighting their limitations. The study also aimed to identify existing knowledge gaps and propose directions for future research. A comprehensive review of behavioral theories in information and cybersecurity was conducted, offering a more holistic understanding of the motivations and intentions that drive IDB. By synthesizing insights from multiple disciplines, this study contributed to a broader and more nuanced understanding of the motivations and intentions behind insider threats and deviant behaviors, helping organizations develop more effective strategies to prevent, detect, and mitigate IDBs.

Method

In this article, we conducted a systematic literature review to address the question: How do psychological, sociological, and criminological theories explain insider deviant behavior in information security? To address our research question, we

adhered to the PRISMA (Preferred Reporting Items for Systematic Reviews and Meta-Analyses) guidelines (Page et al., 2021), which involved identifying pertinent studies, applying eligibility criteria during the screening process, extracting relevant data, and synthesizing the findings.

This study targeted high-level IS journals and conferences, including the AIS Basket of 8 (e.g., EJIS, ISJ, ISR, JAIS, MISQ, JMIS), as well as proceedings such as ECIS, ICIS, HICSS, and AMCIS, and databases like Elsevier and Emerald. To ensure comprehensive coverage, our search was extended to include sources from both Scopus and Web of Science for interdisciplinary studies. We used Google Scholar to identify and cross-validate additional relevant papers beyond specialized sources.

We established criteria to select peer-reviewed, English-language empirical studies (1990–2023) focusing on criminological, sociological, or psychological theories related to information security, particularly insider deviant behavior (IDB). Short papers, opinion pieces, and studies on technical or external cybersecurity threats were excluded. Using keywords like "IS," "Information Security," and "cybersecurity," we ensured a comprehensive review. However, since most cybersecurity literature addressed technical threats or general management decisions, we narrowed our focus to information security for greater relevance to IDB.

We initially screened 448 articles by reviewing their titles and abstracts to ensure they met our inclusion criteria, including topic, language, and year. After removing duplicates and excluding conceptual papers, we conducted a full-text review to determine the eligibility of the remaining documents. Ultimately, 86 articles were included in our analysis based on their relevance and alignment with our research criteria.

Findings

We identified 46 theories, drawn from sociology, criminology, and psychology, that have been used to examine insider deviant behavior (IDB) within the context of information security. These theories were grouped into four categories: psychological and behavioral, organizational, sociocultural, and decision-making. Furthermore, the theoretical constructs were organized into eight key factors that influence motivations and intentions behind IDB: psychological, organizational, situational/environmental, sociocultural, coping and emotional, information processing and technology, ethical and value-based, and socioeconomic. This categorization offers a structured framework for understanding the underlying drivers of IDB in information security settings. Furthermore, we identified deviant behaviors typically studied in IS, including computer abuse, computer fraud, IS compliance and non-compliance, information systems misuse, security policy

violations (both malicious and non-malicious), shadow IT, unauthorized disclosure, computer crime, Information systems security (ISS) abuse, and access policy violations.

Our study contributes to the information systems literature by uncovering relationships among theories and factors, emphasizing overlapping constructs like fear, motivational values, coping mechanisms, stress responses, cultural dimensions, technological acceptance, and moral considerations in understanding IDB.

We explained that based on the literature, fear plays a significant role in shaping insider behaviors, influencing cognitive and emotional responses. Depending on individual perceptions of uncertainty and control, it can drive risk-averse behaviors, compliance with policies, or deviant actions. Motivation and values also intersect significantly, as intrinsic and extrinsic motivations, as well as personal and organizational values, determine individuals' intentions and behaviors. Aligned motivations and values foster compliance, while misalignment can lead to rationalized deviant actions.

The review highlighted how coping strategies and stress responses shed light on the ways individuals manage stressors in the workplace, such as unclear expectations or job insecurity. Negative emotional responses to these stressors may lead to maladaptive behaviors, including deviance, whereas adaptive coping strategies foster compliance and resilience. Cultural and societal dimensions influence insider behavior, such as norms, values, and communication styles. For instance, collectivism, power distance, and cultural attitudes toward authority shape employees' adherence to policies and their likelihood of engaging in deviant actions.

Technological acceptance is another critical factor, as perceptions of technology's usefulness and ease of use influence behavior (Tian et al., 2023). User-friendly systems enhance trust and reduce anxiety, fostering compliance and minimizing resistance to security measures. Ethical and moral factors serve as a foundation for decision-making, with individuals' beliefs and values guiding their evaluation of ethical dilemmas. These considerations help determine whether actions align with or deviate from organizational norms.

Together, these relationships demonstrate the interplay of psychological, cultural, and organizational factors in shaping insider behavior. Understanding these relationships offers a holistic framework for addressing IDB, enabling organizations to design targeted interventions that promote compliance, reduce deviance, and create a secure information security environment.

3.2 Article 2: Limitations of Theories in Insider Deviant Behavior Research in Information Security: A Theoretical Review and Research Agenda

Insider deviant behaviors (IDBs) in cybersecurity have become a major focus in research, as scholars seek to understand why employees comply or fail to comply with security policies. Theories from sociology, criminology, and psychology have been applied to explain these behaviors. Sociological theories emphasize social influences, criminological frameworks examine stressors and opportunities, and psychological models focus on individual cognition and emotions (Rottweiler et al., 2022). While these perspectives provide valuable insights, none offer a comprehensive explanation, prediction, or prescription for IDBs, underscoring the need for more integrative approaches.

Despite their contributions, these theories often fail to account for the complex situational and organizational factors influencing IDBs. Some models, such as Deterrence Theory (Beccaria, 1963; Gibbs, 1968), prioritize external controls but overlook internal decision-making processes, ethical considerations, and perceptions of legitimacy. Others, such as coping models, explain individual responses to security threats but overlook cultural and emotional dimensions, resulting in inconsistencies. As cybersecurity threats evolve, research highlights the need for adaptable, multidimensional frameworks that bridge these gaps.

Another limitation is that many theories assume static environments (settings with fixed security policies, roles, and infrastructures) and rational decision-making, failing to capture the dynamic nature of insider threats (Wall, 2017). Overlapping models create a fragmented research landscape, complicating efforts to develop a unified approach to IDB mitigation. Scholars are now exploring underutilized frameworks, such as cognitive decision-making and the legitimacy of security governance, to provide new perspectives.

In this study, we aimed to examine and address these theoretical limitations through a theoretical integrative review, advancing IDB research and developing action-guiding principles and recommendations to study IDB comprehensively. We also emphasize specific areas where additional research and theoretical integration are required. Integrating multiple perspectives into a comprehensive model can enhance understanding, prediction, and mitigation efforts. By refining existing theories and incorporating emerging insights, future research can develop more adaptive, context-sensitive security models that better address insider threats in complex organizational settings.

Method

In this study, we employed a Theoretical Integrative Review (TIR) (Battistone et al., 2023) to critically examine and synthesize the limitations of psychological, sociological, and criminological theories as they relate to IDB research within the field of information security. The TIR followed a structured three-stage process: planning, conducting, and reporting, based on established research methods of Keele (2007) and Webster & Watson (2002).

During the planning stage, we identified the need for a review based on Anti & Vartiainen (2024), Article 1, developed a review protocol, and evaluated its effectiveness. During the conducting stage, we systematically searched academic databases, selected relevant studies, and reviewed them according to rigorous inclusion and exclusion criteria. The reporting stage involved presenting our findings on the theoretical limitations of IDB research.

Our inclusion criteria focused on peer-reviewed studies published between 1990 and 2024 that examined employees' or insiders' behavior in information security through criminological, sociological, and psychological perspectives. Studies were excluded if they primarily addressed technical security threats, were short papers, or were opinion-based articles. Using targeted search terms, we searched key academic journals, including the AIS "Basket of 8", Elsevier, Emerald, and major IS conferences, alongside databases such as Scopus, Web of Science, and Google Scholar.

From an initial pool of 1,500 studies, we screened and refined the selection to 114 articles. Our analysis focused on identifying theories used in IDB research and critically assessing their limitations. We evaluated how these theories were applied and examined their explanatory, predictive, and prescriptive power gaps. This systematic approach allowed us to develop a research framework that addresses the theoretical limitations in IDB studies and enhances the understanding of insider behaviors in cybersecurity contexts. Thematic analysis was further applied to code and group the identified limitations into themes.

Findings

Based on an analysis of 114 articles, we evaluated the application of psychological, sociological, and criminological theories in IDB research within the context of information security, along with their associated limitations. We analyzed 66 theories and categorized their limitations into *explanation, prediction, and prescription*. We further coded and grouped the identified limitations into five (5) themes*: inconsistencies in research, neglect of influential factors, narrow focus, challenges in predicting behaviors, and data and methodological issues,* to enhance the study of IDBs

from various theoretical frameworks, providing a more nuanced discussion on how each limitation affects the applicability of findings across diverse contexts. We also identified ongoing studies that apply various theories. However, their limitations were not analyzed, as these studies are still in progress and were therefore excluded from this review. Table 1 highlights the identified themes.

Table 2. Identified Themes

Themes	Description	Solution
Inconsistencies in research	Identify and document contradictory findings, short-term focus, and restrictive frameworks.	Conduct meta-analyses and longitudinal studies to reconcile inconsistencies and develop comprehensive frameworks for understanding.
Neglect of influential factors	Include personality, cultural differences, and fear control processes in research designs.	Develop multi-dimensional models for these factors and their interactions with security behaviors.
Narrow focus	Broaden the scope to include diverse security threats, ethical concerns, and real-world applications.	Implement holistic approaches that integrate security threats and ethical considerations into the models.
Challenges in predicting behaviors	Address the complexity of interactions, limited generalizability, and need for integration with other frameworks.	Use advanced statistical methods and machine learning to improve predictive accuracy and integrate findings from multiple theoretical frameworks.
Data and methodological issues	Improve data collection methods, address biases, and enhance measurement techniques.	Employ mixed-methods research, including qualitative and quantitative approaches, to capture nuanced behaviors and improve data reliability.

Our findings reveal that the research on IDBs faces several theoretical limitations that do not allow for a comprehensive understanding of security behaviors.

The Inconsistencies in research stemming from studies presenting contradictory findings due to their short-term focus and the use of restrictive frameworks are major limitations. Results from research inconsistencies are often fragmented and conflicting, as their credibility heavily depends on the acceptance of theoretical frameworks. For example, the application of deterrence theory has yielded mixed results in cybersecurity research, where some studies suggest that sanctions deter certain behaviors but have little effect on non-malicious violations. Addressing these

inconsistencies requires conducting research through meta-analyses and longitudinal studies to reconcile differences and establish more inclusive, long-term frameworks.

Another notable limitation is the neglect of influential factors, such as personality traits, cultural differences, and fear control processes. These elements, when overlooked, weaken the theoretical explanatory power. Research is needed to identify these contextual and influential factors at the outset, in order to develop multidimensional models that incorporate them and examine how they interact with security behaviors.

Further, the narrow focus of existing research limits its applicability. By focusing on a limited range of security threats and ethical considerations, research into IDBs overlooks the full complexity of real-world scenarios. Broadening the scope to include diverse security threats and ethical concerns is crucial for creating holistic and applicable models.

Moreover, predicting security-related behaviors remains a significant challenge due to the complicated interplay of human interactions, limited generalizability, and the absence of integration with other theoretical frameworks. Advanced statistical methods and machine learning techniques are necessary to enhance predictive accuracy and effectively integrate findings across diverse approaches.

Lastly, data collection and methodological issues compromise the reliability of current IDB research. Biases in data collection and measurement techniques must be addressed through the development of improved methodologies. Employing mixed-methods research, which combines qualitative and quantitative approaches, promises a more nuanced understanding of behaviors, thereby enhancing the overall reliability and validity of the findings (Wilkes et al., 2021).

These findings reflect the current state of security behavior research as lacking the necessary rigor, especially considering the severity of the issue. Addressing inconsistencies, broadening the scope, incorporating key influencing factors, improving predictive methods, and strengthening data collection are essential steps toward developing more robust, valid, and comprehensive models.

Based on the findings, this study proposed a set of action-guiding principles to support research studying IDBs in information and cybersecurity. These flexible guidelines address major limitations in the field, including inconsistent findings, overlooked influential factors, limited research scope, difficulties in behavior prediction, and methodological shortcomings. The principles provide a structured approach that encompasses research perspectives, core principles, and key gaps,

along with practical recommendations. Designed to be adaptable, they help researchers navigate the complexity and evolving nature of cybersecurity threats.

This study outlined five core perspectives that guide IDB research in information and cybersecurity: theory, context, ethics, methods, and impact. Each perspective addresses a critical dimension often overlooked or underdeveloped in current research.

Theoretical development should be rooted in interdisciplinary synthesis. Instead of relying on isolated theoretical frameworks, research is encouraged to draw from psychology, sociology, organizational studies, criminology, and cybersecurity. This integration offers a more comprehensive and nuanced understanding of the complex factors that drive insider deviance.

Contextual embeddedness is equally essential. Research must reflect the specific organizational environments in which behaviors occur, taking into account the unique workplace cultures, norms, and structures. Without this, findings risk being overly generalized and detached from the realities they aim to represent.

Ethical reflexivity is a third pillar, emphasizing the moral responsibilities of research. Studies must critically assess how individuals are labeled as "insiders" or "threats," ensure privacy and informed consent, and remain aware of the broader impact on trust and fairness within organizations.

Methodological dynamism and integration call for flexible and robust research designs. Qualitative and quantitative methods, along with advanced tools such as simulations and machine learning, are essential for capturing the fluid and interactive nature of insider threats. This approach enables research to address both individual behaviors and systemic patterns effectively.

Finally, applied collaborative impact stresses the importance of relevance and real-world application, where research should be developed in collaboration with industry partners, ensuring that outcomes inform practical improvements in training, policy, and system design. Feedback loops with stakeholders further enhance the validity and usefulness of the findings.

3.3 Article 3: Impact of Artificial Intelligence on Employee Strain and Insider Deviance in Cybersecurity

In this study, we explored the psychological and behavioral impact of AI technologies, specifically Performance Monitoring Tools (PMTs) and Automated Decision-Making Systems (ADMSs), on employees concerning cybersecurity. Although literature has highlighted the advantages of implementing AI technologies, such as operational efficiency, enhanced decision-making, and digital transformations, these technologies also introduce unintended stressors that may negatively impact employees. These stressors may include constant surveillance, loss of autonomy, performance pressure, and perceptions of unfair treatment. The pressure emanating from such AI technologies can lead to emotional distress, job dissatisfaction, and, in some cases, insider deviance (malicious or unintentional behaviors) that can compromise organizational integrity and security.

Drawing on General Strain Theory (GST) (Agnew, 1985, 1992), this study examined the correlation between AI technologies, such as PMTs and ADMSs, and their impact on workplace strain and insider deviance. Furthermore, this study aimed to bridge the gap between cybersecurity and deviant behavior by examining how AI-induced workplace strains translate into deviant behaviors and insider threats, providing fresh insights that integrate information systems, organizational behavior, and cybersecurity research.

The growing reliance on AI technologies to monitor and evaluate workers has the potential to heighten employee anxiety and resentment, contributing to psychological and social strains that foster IDBs. Fears around job displacement and increased surveillance, amplified by public discourse like 'AI will steal our jobs', can intensify dissatisfaction and resistance to change. These conditions create a fertile ground for actions such as fraud, sabotage, unauthorized access, or system misuse by individuals with legitimate access to organizational systems.

Implementing AI systems, such as PMTs and ADMSs, involves restructuring organizational processes and decision-making hierarchies. These systems can displace human judgment, leading to employee concerns over accountability, loss of control, and job security. Additionally, AI technologies may create or exacerbate technostress, reduce meaningful social interactions, and promote digital dependency. Although AI is often presented as a tool for improving productivity, studies indicate that it can also create psychological strain, particularly when it imposes unrealistic benchmarks, reduces autonomy, or lacks transparency (Chuang et al., 2025; Leong et

al., 2025). Poorly managed implementation can provoke fear, resistance, and hostility, heightening insider deviance.

The GST, developed by Agnew (1985, 1992), explains how workplace stressors may lead to deviant behavior. GST posits that individuals who experience strain, defined as the inability to achieve valued goals, the removal of positive stimuli, or the exposure to negative stimuli, may develop negative emotions such as frustration, anger, or anxiety. These emotional responses can lead to deviant coping strategies.

In this study, GST is adapted to an AI-driven work context, identifying three core AI-related strains:

1. AI-Induced Work Strain (AIWS): Resulting from surveillance, job insecurity, and algorithm-driven decisions.

2. AI-Induced Workload Change (AIWC): Refers to shifts in job demands, task complexity, and cognitive load due to AI use.

3. AI-Induced Perceived Inequity (AIPI): Captures perceived unfairness in AI-driven decisions, such as evaluations or task assignments.

These strains were hypothesized to influence employee strain (ES) and insider deviance (ID). The theoretical model builds on GST by introducing technology-specific stressors and contextualizing deviance within the framework of cybersecurity threats.

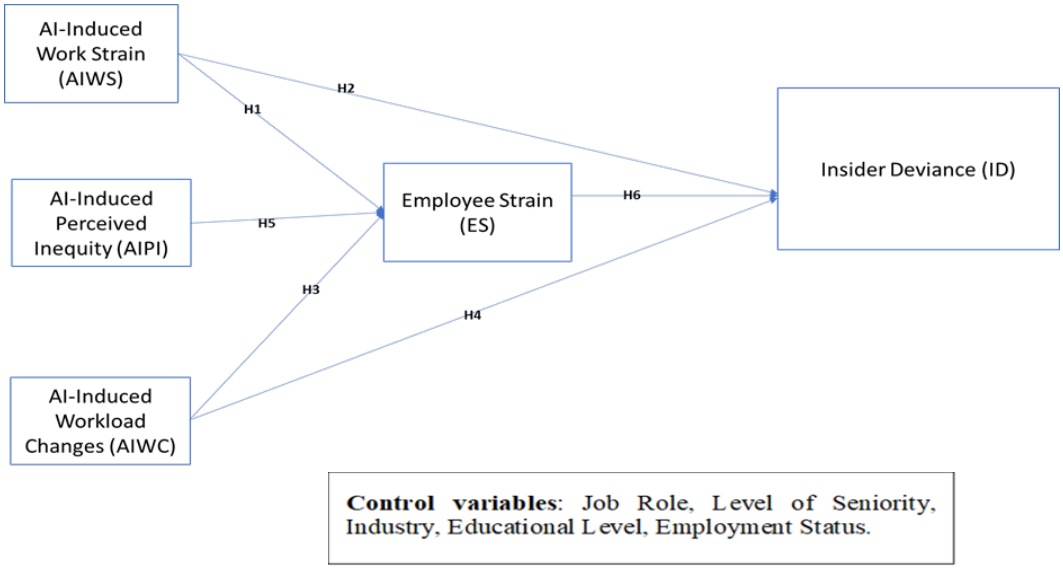

Figure 5. Research Model

Based on the research model, six hypotheses were proposed:

H1: AI-Induced Work Strain positively affects Employee Strain.

H2: AI-Induced Work Strain positively affects Insider Deviance.

H3: AI-Induced Workload Changes positively affect Employee Strain.

H4: AI-Induced Workload Changes positively affect Insider Deviance.

H5: AI-Induced Perceived Inequity positively affects Employee Strain.

H6: Employee Strain positively affects Insider Deviance.

Each construct drew on prior research and empirical findings. For example, AI-induced workload increases cognitive and emotional demands, while perceived inequity in algorithmic decisions may erode trust and heighten resistance.

Method

A quantitative research design was employed to test the proposed model, using regression analysis to evaluate the relationships among key variables. Data was collected using a structured survey that included validated items from the technostress, organizational justice, and workplace strain scales. The instrument was refined through expert reviews and a pilot study involving cybersecurity professionals and doctoral researchers. A stratified random sampling method was applied to target employees in North America and Europe (specifically the U.S. and Canada) to account for regional differences in AI adoption and the workplace. The target respondents were employees with direct experience using AI tools in their workplace or those who regularly interact with AI tools as part of their job responsibilities across technology, finance, healthcare, and manufacturing. A priori power analysis indicated a minimum sample size of 102. To enhance reliability and account for nonresponse or attrition, 150 responses were targeted. To minimize bias, the survey featured 7-point Likert-scale items, attention-check questions, and randomized item ordering. It also collected demographic and job-related information to control for confounding variables. AI-Induced Work Strain (AIWS), AI-Induced Perceived Inequity (AIPI), and AI-Induced Workload Changes (AIWC) were measured using adapted items from prior research (e.g., Anis & Emil, 2022; Jang et al., 2021; Nisafani et al., 2020). Employee Strain was assessed using workplace stress scales (D'Arcy & Teh, 2019; Yazdanmehr et al., 2023). Insider Deviance included items related to misuse of access, sabotage, or unauthorized activity (Dang, 2014; Guo et al., 2011).

Discussion and Expected Contributions.

Currently in the data analysis phase, this study is expected to demonstrate a strong correlation between AI-induced work strains and insider deviant behavior. We anticipate that the results will validate GST in the context of AI-driven workplace environments, particularly cybersecurity.

This study makes theoretical and practical contributions to understanding the impact of AI integration in organizational settings by applying GST. Theoretically, GST is extended to AI-specific workplace environments, which are yet to be fully explored. It introduced and operationalized three constructs: AI-induced work strain (AIW), AI-induced workload change (AIWC), and AI-induced perceived inequity (AIPI) as unique and relevant to the digital transformation and automation processes reshaping organizations. These constructs enable a more nuanced examination of how AI technologies impact employees, particularly in their emotional and behavioral responses when implemented in the workplace. Furthermore, this study presents a novel approach to linking AI-related stress to deviant behaviors, thereby advancing research in organizational behavior and cybersecurity.

Practically, this study's findings will help organizations mitigate insider threats when implementing AI technologies. Understanding these stressors driven by AI can help organizations develop more effective change management strategies and foster humane and transparent integration of AI technologies. Further, the findings will encourage fair AI governance and transparent decision-making processes to address employee concerns around autonomy, fairness, and control. The study will help organizations recognize the importance of investing in employee support systems, including targeted training programs and engagement initiatives, to mitigate psychological strain and enhance organizational trust.

3.4 Article 4: Mitigating Insider Threats in Cybersecurity: A Design Thinking Approach

Insider threats have become a growing concern in cybersecurity, representing one of an organization's most complex and costly challenges. Insiders, by virtue of their internal position and legitimate access, are more difficult to detect than external attackers and often pose a greater risk.. With an average cost of about USD 5 million per incident, recent statistics show that insider-related events now account for 7% of cybersecurity breaches (IBM & Ponemon Institute, 2024). From 2019 to 2024, the prevalence of insider threats rose significantly, driven by various motives (Cybersecurity Insiders, 2024). From policy violations and data theft to sabotage and

inadvertent breaches, these threats take many forms and can go undetected for hundreds of days, affecting organizations financially, legally, and reputationally.

Insider threats persist despite numerous countermeasures, including access control systems, user monitoring, and cybersecurity training. This ongoing vulnerability stems from the limitations of traditional approaches, which often fail to fully account for human motivations, organizational dynamics, and the evolving nature of threat behavior. Consequently, there is a growing call for adaptive, human-centered mitigation strategies that address both the psychological and technical aspects of insider threats and deviance in cybersecurity.

In this study, we present Design Thinking (DT) as a potential but underused framework in cybersecurity in response to this gap. Other methods have been adopted in information systems (IS) research to address the complexity of cybersecurity. Many of these approaches have involved systems thinking (Arnold & Wade, 2015; Zoto et al., 2019), which emphasizes understanding systems and their interrelationships as a whole. Systems thinking focuses primarily on structural analysis and the broader organizational ecosystem. However, DT stresses empathy, creativity, and iterative problem-solving grounded in user experience. Although its application in cybersecurity is still limited, some studies indicate its potential to enhance threat awareness, design educational tools, and improve user-centered defenses. However, a systematic approach to using DT for insider threat mitigation has yet to be developed.

This study bridges that gap by proposing DESTIC (Figure 1), a six-phase design thinking framework that integrates psychological, social, and organizational insights to understand and prevent insider threats. The literature indicates that while technical, socio-technical, and psychological approaches each offer value, they are often fragmented and insufficient when used in isolation.

Technical systems, such as intrusion detection and monitoring, struggle to distinguish between malicious and accidental behavior. Socio-technical models bring in human elements but can be costly and lack precision in understanding individual motivations. Psychological theories such as rational choice and deterrence offer behavioral insights but often assume homogeneity and fail without strong managerial enforcement.

By applying DT's structured, human-centered methodology, we aim to create a more holistic and actionable model for anticipating and mitigating insider threats. In doing so, it contributes a novel theoretical and practical approach to one of cybersecurity's most persistent challenges.

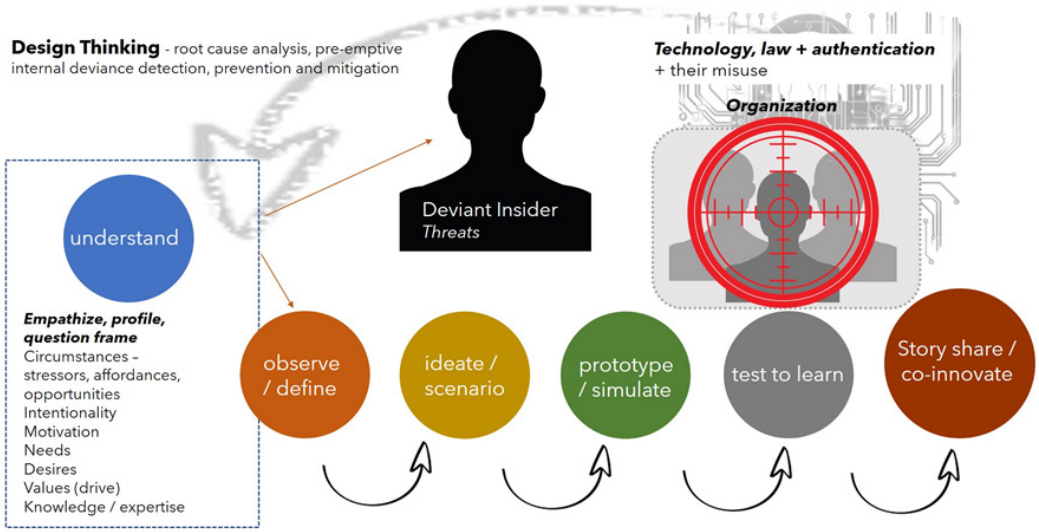

Figure 6. DESTIC Framework

Figure 5 highlights the Design Thinking for ITC framework (DESTIC), a six-stage DT model designed to uncover and mitigate insider deviance by integrating behavioral, organizational, and socio-technical insights. This framework outlines a process from developing an initial understanding of the situation (Understand stage) to observing and defining, ideating and scenario-building, prototyping and simulating, testing and learning, and finally, the official outward communication stage of story sharing and further co-innovation. The process can be implemented in iterative cycles, using each stage's increasing fidelity to generate more detailed strategic insights into what is happening. It can happen, where, and how it can be addressed.

Drawing on existing research, the framework begins by understanding deviant behaviors and their root causes, followed by the observation and definition of key organizational and psychological factors. The ideation phase encourages creative scenario-building to map potential threat pathways, which are then explored through prototyping and simulation exercises that model realistic outcomes. Testing involves expert and non-expert evaluations to refine scenarios and surface blind spots. Finally, the process culminates in storytelling and co-innovation, where findings are translated into actionable strategies and shared narratives that enhance awareness and support cultural change. These stages offer a dynamic, iterative approach to proactively addressing insider threats in complex organizational environments.

Method

This study employs a qualitative, exploratory methodology centered around the use of organizational design workshops to investigate insider threats through a human-centered Design Thinking (DT) lens.

The research is structured into three main phases over twelve months. The first phase focuses on planning, preparation, and recruitment, during which workshop materials and facilitation protocols are developed based on the DESTIC framework and established Design Thinking practices. Pilot testing will be conducted to refine the design before full implementation. Concurrently, partnerships will be established with four organizations in high-risk sectors in Finland, including finance, healthcare, and public institutions. Participant recruitment will target a multidisciplinary group of five to ten individuals per organization, comprising cybersecurity experts, IT professionals, human resources personnel, general employees, and behavioral and cognitive psychology specialists. This diverse stakeholder representation supports the generation of rich, contextual insights and aligns with the broader goals of information systems research, theory development, socio-technical system design, and practical innovation.

The second phase of the study will consist of intensive one-day design workshops held within each participating organization. These sessions will be structured into iterative sprints that cycle through ideation, prototyping, feedback, and refinement. Participants will engage directly with a variety of DT tools, including empathy mapping, journey mapping, root cause analysis, and persona development. To deepen understanding of insider threat behavior and organizational vulnerabilities, the workshops also incorporate forensic-style inquiry sessions and facilitated focus groups. This approach allows participants not only to reframe issues but also to co-create potential interventions. The workshops will be extensively documented through audiovisual recordings, field notes, and the collection of artifacts, including sketches, models, and system maps. The iterative nature of the sessions ensures that ideas are tested and refined in real-time, thereby increasing the practical relevance of the solutions generated.

The final phase, which focuses on data analysis, will be conducted over three months. A combination of thematic coding and qualitative profiling techniques will be applied to the workshop outputs. Triangulation across roles, organizations, and data types will strengthen the validity of findings and support the development of grounded theories and operational models. One of the principal deliverables of this phase is the creation of a socio-technical solution map. This map will integrate insights from across the workshops to identify root causes, threat networks, and actionable areas for intervention.

Feasibility is a core consideration in the study design. The required resources are modest, including a facilitation team of two to three members, basic workshop materials such as sticky notes and whiteboards, and logistical support from partner organizations. Organizational cooperation includes providing physical or virtual

space, releasing staff to participate for one full day, and sharing contextual data such as internal policies or anonymized incident reports. While securing employee participation can be challenging, this issue can be addressed by positioning the workshop as both a professional development opportunity and a potential team-building exercise. Importantly, the process is framed as a cost-effective investment. The relatively small upfront resource allocation is justified by the potential for significant long-term savings through the reduction of insider threat incidents.

Expected Contributions

This study contributes to cybersecurity by positioning Design Thinking (DT) as a human-centered, multi-professional, and multi-stakeholder methodology for proactively addressing insider threats—an area traditionally dominated by technical and system-based approaches. The study introduces the DESTIC framework, a structured yet flexible DT model tailored to the socio-technical complexity of insider deviance. By integrating behavioral and motivational theories into the "understand" phase, the framework provides a deeper diagnostic lens to uncover psychological, organizational, and contextual factors that enable insider threats.

Insider threats are not only driven by malice or stress, as they often involve creative problem-solving. Insiders may actively find innovative ways to bypass controls or exploit system weaknesses. This element of "deviant creativity" highlights the need for research approaches that account for creative cognition, rather than relying solely on models focused on compliance or rational choices. Deviant creativity suggests that individuals who engage in deviance often think creatively, using novel ways to combine information for deception and stay ahead (Kapoor, 2025).

A key contribution of this study lies in exploring deviant creativity, a rarely examined dimension in insider threat literature. This concept expands the field's understanding of how insiders innovate harmfully within system constraints, offering new perspectives for anticipating and disrupting such behavior. Additionally, we emphasize the co-creative and iterative nature of DT, demonstrating how cross-disciplinary collaboration can surface new mitigation strategies that are both contextually grounded and adaptable.

The study also highlights a pressing gap in the interplay between emerging technologies, legal frameworks, and authentication systems. As technological capabilities evolve faster than regulatory structures, DT provides a means to explore vulnerabilities, socio-legal, and ethical implications of cybersecurity design. By facilitating stakeholder engagement in design and scenario planning, DT supports the creation of adaptive regulatory responses that align with real-world organizational dynamics.

Our study advances the field by reframing insider threat mitigation as both a technical challenge and a complex, systemic problem that requires human-centered innovation to systematically account for and address creativity as a component of deviant behavior. It contributes theoretically by expanding the conceptual toolkit for studying insider deviance, and practically, by offering a replicable methodology for organizations seeking to strengthen their cybersecurity posture through inclusive and creative problem-solving.

3.5 Synthesis of the Articles

In this section, I synthesize the key findings and insights of Articles 1–4 to answer the research questions:

1. What is the current state of criminological, sociological, and psychological theories used to explain insider deviant behavior in cybersecurity research?

2. How can criminological, psychological, and sociological theories be critically analyzed and synthesized to better mitigate insider deviant behavior in information and cybersecurity?

Insider deviant behaviors in cybersecurity continue to pose a significant threat to organizations, as they originate from within and involve multiple technical, psychological, and social factors. Articles 1 and 2 lay the theoretical groundwork for understanding insider deviant behavior (IDB). In contrast, Article 3 introduces the underexplored impact of AI-induced strain on such behavior, and Article 4 presents Design Thinking as a human-centric approach for addressing insider threats. Together, these articles underscore the need for a new IDB explanation and theoretical approach that integrates psychological insight, contextual awareness, technological responsiveness, and a human-centered perspective, as illustrated in Figure 7.

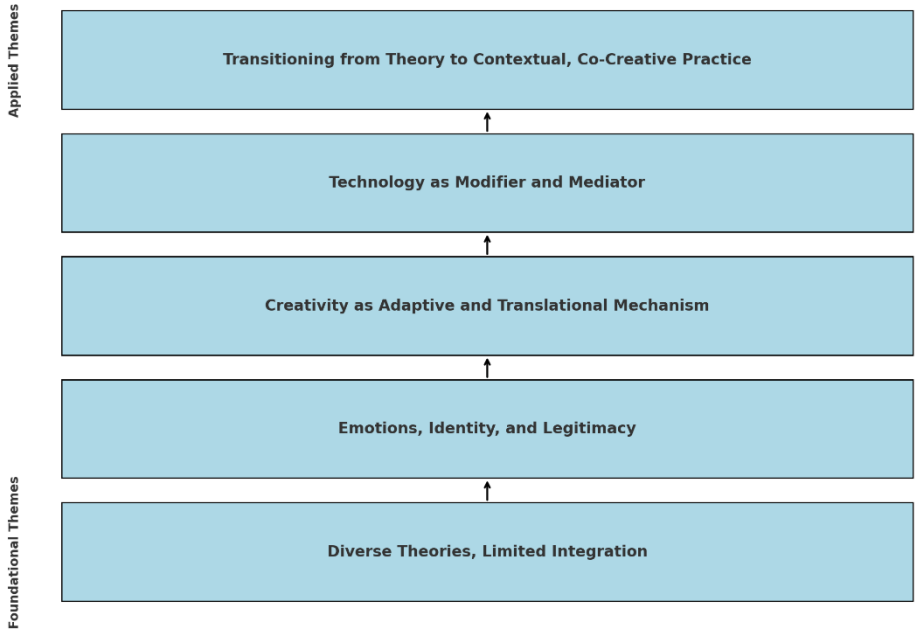

Figure 7. Research Agenda for IDB

A major contribution of this research is the clear distinction between foundational and applied themes in understanding IDB (Figure 7). It demonstrates how research can more effectively explain and predict IDBs through robust theoretical and conceptual groundwork, while also prescribing practical, adaptive solutions grounded in human-centered design and contextual understanding.

Foundational themes establish the theoretical and conceptual base for understanding IDBs**.** These themes explore the application of diverse perspectives, including psychological, socio-cultural, organizational, and socio-economic lenses, and emphasize the critical role of emotion, identity, and trust in shaping insider actions. Such insights challenge excessively rational models of behavior and set the stage for more nuanced, human-centered interpretations of deviance. Understanding the *why* behind IDBs, beyond rules and risks, requires a rich blend of theories and perspectives. These themes reframe insider threats as relational, emotional, and systemic issues, rather than merely technical violations.

Applied themes, on the other hand, translate these foundational insights into practical and adaptive responses. They highlight how creativity influences behavior

under pressure, how technology actively shapes deviance as described in the Fraud Triangle Theory (Albrecht et al., 1984, 2008), and not just as a detection tool. Furthermore, they demonstrate how insider threats can be effectively managed through a contextual understanding and co-designed solutions (Li et al., 2021). These themes connect theoretical insights to real-world practice, offering pathways to innovation in cybersecurity strategies. By centering empathy, adaptability, and collaboration, they enable organizations to respond to insider threats in ways that are not only effective but ethical and sustainable.

Diverse Theories, Limited Integration

Article 1 comprehensively maps 46 theories from psychology, sociology, criminology, and decision-making fields that have been applied to IDB research. These theories are classified into four broad categories—psychological/behavioral, organizational, socio-cultural, and decision-making, and further categorized into eight motivating factors: psychological traits, organizational contexts, situational environments, sociocultural influences, emotional responses, information processing, ethics/values, and socioeconomic conditions. The classification provides a multidimensional lens through which IDB can be viewed, capturing the dynamic interplay between individual cognition and broader systemic influences. Furthermore, Article 1 highlights the impact of fear, motivation, coping mechanisms, and ethical reasoning on employee behavior. For example, fear may promote compliance or trigger deviance, depending on the perceived level of control and the degree of uncertainty surrounding the situation. Misaligned values between individuals and organizations can rationalize unethical conduct, while cultural norms influence whether individuals violate or obey authority and policy. This multifaceted explanation highlights that deviant behavior is rarely the result of a single factor; instead, it emerges through the convergence of interacting psychological, organizational, and socio-cultural forces.

However, the analysis in Article 1 revealed the need for further critical analysis that was undertaken in Article 2. Article 2 highlights the limitations of these theories and their application in research, providing a cohesive and comprehensive understanding of IDBs. Many theories are applied independently, without integration, and are often predicated on assumptions of rational behavior within rigid, unchanging organizational settings. For example, deterrence theory overemphasizes external controls without fully capturing intrinsic motivations or ethical judgment. Coping theories address emotional regulation but neglect organizational legitimacy and cultural variance. Such theories typically presume rational behavior within stable and inflexible environments, which fail to reflect the volatile, uncertain, and emotionally charged contexts in which insider threats are enabled.

The lack of theoretical integration has resulted in a knowledge gap, where introducing factors complicates rather than clarifies our understanding of insider behavior. Article 2 argues for moving beyond isolated theoretical models toward an interdisciplinary synthesis that captures the complexity of insider deviance. It encourages a multidisciplinary and contextual approach, arguing that insider deviant behavior cannot be fully understood through non-adaptive and independent theories and models alone, but should be seen as dynamic, relational, and shaped by multiple connected factors and motivations.

Emotions, Identity, and Trust

Across Articles 1 to 3, a pattern emerges that shows insiders are not just rational decision-makers but individuals navigating complex emotional, social, and ethical realities. While Article 1 recognizes emotions like fear and anxiety, they are usually considered secondary to rational thinking. Article 2 challenges this view, emphasizing that emotions play a central role in shaping compliance and deviance, particularly when uncertainties, stress, or perceived unfairness are present.

Article 3 builds on this by showing how AI can intensify psychological strain. When AI systems are deeply embedded in workplace processes to monitor performance, automate decisions, or replace certain tasks, they can erode employees' sense of control and value, leading to feelings of alienation and distrust. These emotional reactions, particularly when employees feel excluded from decision-making or unfairly treated, are not just side effects. They can be the root causes of insider deviant behavior. In this context, deviance becomes less about bad intentions and more about how individuals cope with technological stress and perceived injustice.

This shift in focus calls for new research areas that move beyond simply asking what causes insiders to violate norms or policies, to exploring how they perceive and emotionally respond to being managed in increasingly digital, monitored environments. It emphasizes that insiders are not just rational actors or inherently deviant individuals, but people influenced by evolving organizational structures, constant surveillance, and their interpretations of fairness and social meaning at work. To understand IDBs, research must prioritize theoretical frameworks that treat emotion, identity, and perceived justice as core drivers, not just background variables.

Creativity as an Adaptive and Translational Mechanism

Insights from Articles 1 to 4 indicate that IDBs do not occur in isolation, but emerge from a complex interplay of motivation, emotional strain, and individual creativity.

Understanding these interactions is crucial for developing human-centered approaches to cybersecurity.

The recurring theme of motivation in Articles 1 and 2 outlines how various psychological and organizational theories (rational choice or moral disengagement) link motivation to deviant actions. Insiders may act out of frustration, ethical concerns, or a perceived injustice in response to a misalignment of organizational goals or a breakdown in trust. Article 2 builds on this insight by arguing that many theoretical frameworks oversimplify motivation, treating it as a predefined concept. Instead, motivation should be understood as dynamic, shaped by context, particularly within organizational settings, cultural influences, and emotional responses.

Article 3 highlights the stressors that are amplified by technology. It highlights how AI systems, despite their ability to enhance organizational efficiencies, can cause psychological and emotional strain among employees. The anxiety, loss of autonomy, and lack of transparency in AI decision-making may drive insiders toward deviant actions through stress. These stressors interact with motivations in an evolving manner to create complex behavioral responses.

Creativity becomes the channel through which motivation and stress are transformed into innovation. While earlier articles imply adaptive behavior, Article 4 directly addresses *deviant creativity*, the idea that insiders often think cleverly to bypass controls, navigate constraints, or achieve goals despite obstacles. Rather than viewing such behavior as purely malicious, Article 4 recognizes it as a sign of cognitive creativity. This recognition reinforces the development of the DESTIC framework, which proposes design thinking as a practical approach to anticipate, engage with, and mitigate the creativity that can make insider threats so unpredictable.

As a whole, the four articles indicate that deviant behavior is frequently a form of creative adaptation to organizational stressors and misalignment, rather than merely a deliberate violation of rules. Motivation, stressors, and creativity form an interdependent system in which insiders navigate complex emotional, organizational, and technological settings. Addressing insider threats, therefore, requires more than control mechanisms; it also requires strategies that understand and respond to how people think, feel, and adapt under pressure.

Technology as Modifier and Mediator, Rather Than a Tool

Articles 1 and 2 treat technology as part of the threat detection toolkit, focusing on identifying insider threats. In contrast, Article 3 offers a more nuanced perspective by framing technology, particularly AI, not as a neutral tool but as a force that actively

shapes employee experiences and behaviors. AI can affect decisions, blur the lines of responsibility, and shift organizational norms. From this perspective, IDBs should not be viewed as isolated violations, but rather as an adaptive and coping response to technology-driven environments that erode trust and moral agency.

Article 4 expands on this viewpoint by introducing DT as a human-centered approach to understanding and addressing insider threats. The DESTIC framework, with its six iterative phases ranging from understanding to narrative building, views technology as an evolving partner in shaping insider dynamics, rather than merely as a passive tool to monitor behavior. Focusing on user experience, empathy, and scenario planning, this approach moves beyond traditional control methods to address the deeper emotional, social, and ethical dimensions of deviance.

Transitioning from Theory to Practice

All four articles address overly simplistic approaches to managing insider threats. Article 2 outlines five key principles for future research: the need for theories that cross disciplinary boundaries, an understanding of context, a focus on ethics, integration of diverse methods, and a commitment to practical outcomes. Article 4 puts these principles into action by employing innovative methods, such as cross-functional workshops, ongoing feedback, and behavioral modeling, to co-design security strategies with stakeholders.

In addition, Article 4 introduces the idea of deviant creativity, a notion that insiders often exploit system flaws not just out of malice, but through creative problem-solving driven by conflicting goals or a lack of ethical alignment. While rarely discussed in traditional threat research, this concept is critical for understanding how deviant behavior can arise within the system. Recognizing this dynamic opens the door to more realistic and proactive strategies for predicting and preventing insider threats.

In conclusion, the synthesis highlights that tackling insider deviance in information and cybersecurity requires more than technical defenses or psychological profiling. It calls for comprehensive theoretical models that integrate cognition, emotion, and situational factors, recognizing that AI actively shapes employees' emotional and behavioral responses. Additionally, it requires innovative methodologies, such as the DESTIC framework, which reflect the relational and evolving nature of deviance. Most importantly, this study urges a shift from simply identifying malicious insiders to understanding how ordinary individuals may deviate in response to complex and often unjust systems. Future research should embrace this complexity, centering empathy, flexibility, and human-centered design to build security approaches that reduce insider risk and reshape the environments that enable such behavior.

4 DISCUSSION

This dissertation defines IDBs as intentional or unintentional actions by individuals who violate security policies through cognitive or physical means to achieve personal or organizational goals, often harming the organization (Anti & Vartiainen, 2024). Research on IDBs seeks to explain, predict, and prescribe solutions and knowledge about the psychological, organizational, and technological factors that lead to such behaviors. Although IDBs have received substantial attention from researchers over the past two decades, the threat remains persistent and complex, especially as social, organizational, cultural, and technological advancements, such as AI, continue to evolve and exert new pressure on employees. Current research approaches often rely on rigid theories that overlook the complex and emotional aspects of insider behavior in digitally driven environments.

This dissertation advances existing research by outlining how multidisciplinary theories from criminology, sociology, and psychology can be integrated and extended to account for the emerging technological, emotional, and cognitive aspects of insider deviance. The study examined how individual traits, rational decision-making, and broader systemic factors, such as organizational trust, emotional strain, and technology-enabled environments, influence insider behavior.

This research contributes to a deeper understanding of IDBs by identifying underexplored but critical areas. Article 1 demonstrated the broad and often fragmented nature of the theoretical landscape of IDB research by mapping theories into eight motivating factors. Article 2, however, critiqued the fragmented and often non-rigorous theoretical landscape by identifying its limitations when applied to research IDBs. Article 2 emphasized the need to integrate these theoretical approaches that reflect the unpredictable and emotionally charged environments in which insiders function. Article 3 introduced emerging technologies such as AI, which can significantly influence employee perception and behavior. Therefore, IDBs are repositioned as possible coping responses to stress induced by external, internal, and technological factors such as perceived inequity, constant surveillance, loss of autonomy, and job instability. As a result, emotion, trust, and perceived fairness must be considered fundamental to understanding IDBs. Article 4 translated these insights into practice by presenting DT and the DESTIC framework as a human-centered approach to addressing insider threats and introduced the concept of "deviant creativity" to capture how deviant insiders innovate within organizational settings where ethical boundaries are unclear.

The contributions from Articles 1-4 suggest that understanding and mitigating insider threats and deviance requires a shift from theory to practice. For example,

theoretically, General Strain Theory (Agnew, 1985, 1992) posits that AI-induced stressors constitute a new class of strain that can be persistent, less transparent, and often unavoidable, leading to deviant behaviors. Practically, the studies highlight how participatory and empathetic approaches like DT can help design better security frameworks that may account for user emotions, perceptions, and motivations.

The research has identified that organizational and technological shortcomings, including weak communication and a lack of transparency in AI, contribute to increased emotional strain and concerns about fairness. Addressing these factors requires rethinking traditional research methodologies that move beyond monitoring and deterrence, including behavioral modeling, and developing context-driven scenarios with input from diverse teams.

In summary, this dissertation identifies three key paradigm shifts to advance insider threat research: integrating emotional, social, and cultural dynamics into theoretical models, recognizing technology as an active influence on behavior and not just a tool, and implementing participatory, adaptable frameworks for developing security measures. These paradigm shifts provide a foundation for research to identify key variables and relationships related to emotional strain, organizational contexts, and technological influences, offering more realistic and human-centered frameworks for understanding and mitigating insider threats and deviant behaviors.

4.1 Reflection of Results with Prior Literature

The findings and insights from this dissertation align with and extend existing literature on IDBs, particularly by highlighting the emotional (Burns et al., 2019; Chen et al., 2024; Chen et al., 2022), contextual (Hsu et al., 2024), and technological (Chatterjee et al., 2015) factors that influence insider actions. Prior research has traditionally emphasized rational choice models and external controls, such as deterrence theory (Burns et al., 2023; Nehme et al., 2022), to explain and predict why insiders violate organizational norms. Articles 1 and 2 reflect on this prior research, highlighting its limitations by pointing out that many theories examining IDBs are applied in isolation and fail to capture the complexities of real-world organizational events.

The findings affirm that Insider deviance cannot be fully explained by individual traits or intentions alone, as research shows these factors interact with contextual influences and motivational states, making both individual and organizational contexts essential to understanding such behavior (Xu et al., 2024). Consistent with prior literature, Article 1 reveals a diverse theoretical landscape; however, Article 2 critiques this work for lacking integration and over-relying on conventional

assumptions about behavior. This resonates with recent critiques calling for more dynamic, interdisciplinary approaches(e.g., Moody et al., 2018).

Article 3 focused on the impact of AI on employee strain, introducing distinct forms of strain, such as AI-induced strain, which is relatively new but supported by growing evidence that technologies like AI can trigger emotional stress, reduce perceived autonomy, and complicate who is ultimately responsible for decisions (Hou & Fan, 2024; Zhang et al., 2025). Although the literature on technostress has explored stressors including overload and complexity (Nisafani et al., 2020), Article 3 positions AI as a psychological catalyst for insider deviance. This recontextualization contributes to the emerging research examining the ethical and emotional aspects of AI in workplaces (e.g., Chuang et al., 2025; Ding et al., 2025; Leong et al., 2025; Zhang et al., 2025).

Article 4's introduction of DT and deviant creativity aligns with recent efforts to humanize cybersecurity (Ashenden et al., 2021; Dorasamy et al., 2019; Snow et al., 2020). Unlike traditional control-based strategies, the DT approach emphasizes empathy, iteration, and shared problem-solving, highlighting a practical shift toward relational and contextual strategies for insider risk management.

4.1.1 Implications for Research

This dissertation makes several contributions to understanding and researching IDBs in modern, digitalized, and high-pressure work environments. The findings from the Articles suggest the need to move beyond narrow, rational explanations to a more comprehensive, real-world understanding of the factors that influence insiders to act deviantly.

The eight factors identified in Article 1 (psychological, organizational, situational, sociocultural, emotional, information processing, ethics and values, and socioeconomic) provide a broader and multidimensional view of insider deviance and indicate that IDBs are not merely influenced by a single factor but through an interaction of several factors in the insider's personal, social, and professional settings. For example, an individual's emotional state, belief systems, or perception of fairness at work can interact in a complex way to shape how they behave or act under pressure. Furthermore, this dissertation emphasizes the significance of fear, motivation, coping strategies, and ethical reasoning in shaping behavior, which are often overlooked yet profoundly influence how individuals perceive and respond to stress and the changing digital environment perceived as hostile. For example, an employee who feels undervalued, undermined, or treated unfairly may disengage or act out, depending on how they emotionally and ethically process their situation. As

current theories are focused heavily on deterrence and monitoring, future research must advocate for the design of emotionally intelligent and ethically grounded systems and policies by integrating emotional insights, such as stress patterns, and burnout indicators into threat detection, examining how perceived fairness value alignment and trust can reduce IDBs, and the use of co-creation methodologies to create ethical guidelines for technology use. Such inclusion will shift the focus from simply enforcing compliance to building cultures rooted in psychological safety, ethical transparency, and shared responsibility.

While theories from criminology, sociology, and psychology have advanced research in IDBs, this thesis has revealed key gaps in their application. For example, most theories assume that people behave logically and predictably, regardless of their emotional or situational state. This assumption does not reflect reality, especially during stressful situations and when making complex ethical decisions. Accordingly, the study calls for the development of more adaptive, interdisciplinary theories that reflect real-world conditions, emotional complexity, organizational culture, and emerging technologies such as AI. These theories must be flexible enough to address grey ethical areas (e.g., whistleblowing vs. loyalty, moral reasoning, and insider actions) and the unpredictability of human behavior in dynamic work environments.

Future research should explore the integration of moral reasoning into how it influences deviant behaviors in cybersecurity contexts. Moral reasoning can be explored through the rationalist perspective (Kohlberg, 1963, 1971) and the intuitionist (emotional) perspective (Haidt, 2001) to understand their influences on deviant behaviors. Studies can examine how employees justify deviance, especially in high-pressure digital environments, the role of emotions (e.g., guilt, empathy, outrage) in shaping behavior under stress, and the differences in ethical or moral reasoning among employees exposed to automation through AI technologies. This research can deepen our understanding of how moral judgments interact with organizational culture and technology use to inform the design of more thoughtful insider threat mitigation strategies.

Building on General Strain Theory (GST) (Agnew, 1985, 1992), the study introduces AI-related stressors as an emerging form of workplace pressure. These pressures include constant surveillance, unclear decision-making processes, and the perceived irrelevance of skills due to the implementation of AI technologies. These stressors can be particularly harmful as they are often subtle, difficult to avoid, and beyond the control of employees. They accumulate over time and can lead to emotional strain, which may potentially increase the likelihood of deviant behaviors.

The concept of deviant creativity introduced in this dissertation adds a fresh perspective to research. Deviant creativity highlights how some employees may

violate rules not with harmful intent but as a means of adapting, problem-solving, or resisting constraints they view as unjust or discouraging, using cognitive innovation as their tool. This perspective challenges the assumption that all deviant behavior is harmful, encouraging research to examine how such actions may reflect creative problem-solving or innovation in response to systemic constraints within organizations. Research can explore when deviance is constructive versus when deviance is deemed harmful, how employees may perceive the morality of violating security rules or policies to achieve goals, and how organizations respond to such behaviors, whether it leads to innovations or punitive actions. This area of research can inform policies that distinguish between harmful deviance and genuine employee dissent, especially in complex systems where rules may be outdated or misaligned with employee values.

This dissertation advocates for a more human-centered approach to theory development. It encourages research to avoid viewing insiders as predictable threats but as individuals who rationally and emotionally respond to complex and high-pressure situations. By integrating insights from multiple disciplines and paying attention to contextual factors and emotions, future research can develop comprehensive theories that will not only explain and predict insider deviance but also help prescribe solutions for organizations to build fairer and more resilient workplaces.

4.1.2 Implications for Practice

The practical insights offered in this dissertation encourage organizations to rethink insider threats not merely as technical security issues, but as human-centered challenges shaped by employees' emotions, perceptions, and everyday work experiences. At the same time, the findings underscore the urgency of deeper collaboration between research and practice in addressing practical concerns so that security strategies are grounded in both scientific insight and organizational reality.

Practically, security policies and practices must take into account employee emotions and perceptions. Individuals are likely to violate policies or disengage when they feel unheard, unfairly treated, or devalued. For example, Edward Snowden may have felt unheard and unseen when his concerns about mass surveillance through internal channels were ignored. Operating under the belief that there was no effective way to challenge or stop the government's actions from within contributed to his decision to leak classified documents. Organizations can mitigate such risks by implementing anonymous surveys and open-door policies to gauge employee emotions and perceptions about their work and daily interactions with work systems (Probst et al.,

2020). Such practices can help identify frustrations early and allow for interventions before resentment or anxiety builds, which may lead to deviant behaviors.

Implementing AI technologies requires acknowledging that fairness and transparency in monitoring and decision-making processes matter. Fair implementation of AI tools requires transparency around how these systems monitor performance, assign tasks, and make decisions so employees understand what is happening and why. Clear communication about implementing AI technologies, their decision-making processes, and who is accountable for their outcomes can help build trust and reduce anxiety, resentment, and disengagement. For example, demonstrating and explaining to employees how these AI technologies calculate their performance scores and what they can do to improve can increase trust and foster a conducive environment that reduces deviant actions.

Organizations must support coping strategies, as employees working in high-pressure environments may need outlets for stress and a safe space to discuss ethical concerns without fear of retaliation. Managers and HR teams can offer systems that support confidentiality and peer support or facilitate workshops on ethical dilemmas related to AI or automation. Instead of organizations framing security policies as compliance measures, they could be presented as a shared commitment to fairness, openness, and well-being.

Further, employee involvement in shaping security policies and systems must be treated as essential, not optional. Including employees in decision-making regarding the rules and systems they interact with will motivate them to adhere to and identify potential problems early. The involvement of employees in scenario building and co-creation, especially in implementing AI tools, can help map out how a proposed system might affect their daily work, thereby identifying unintended consequences that can help mitigate insider deviance.

The concept of deviant creativity highlights that individuals who engage in insider deviance should not be viewed solely as rule-breakers, but as creative thinkers (Cropley, 2023; Kapoor, 2025). These individuals actively combine knowledge, tools, and contextual awareness to find novel ways of bypassing controls or exploiting system weaknesses. Rather than acting out of impulse alone, they often stay ahead of formal safeguards by cognitively innovating within constraints, making their behavior both harder to predict and more damaging if left unaddressed. For example, the factor of technology and information processing in Article 1 suggests that some employees in organizations may use their skills to act in a deviant manner, aiming to prove a point, expose flaws, or complete tasks despite obstacles, but not to harm the organizational system. In such cases, managers should be curious and find ways to use the feedback and skills of such individuals rather than being punitive. Gathering

feedback on why such behavior occurred can reveal inefficiencies that can be improved in the systems across the entire organization.

The kind of organizational culture created matters more than security controls. Organizations must recognize that security is not all about strong technologies like firewalls, but about how employees feel about their working environment. Trust, respect, and psychological safety are important to mitigating insider threats sustainably. Encouraging open conversations, recognizing employee efforts, and responding to employee concerns in a respectful manner can enhance loyalty and reduce emotional strains that lead to deviant behaviors.

In summary, organizations must shift their views of insider threats through the lens of technical or disciplinary actions. Instead, employees must be treated as partners and assets in security whose insights, emotions, and ethical perspectives are crucial in mitigating insider threats and deviant behaviors. When organizations invest in their workforce, not just their systems, they can build secure, humane, and resilient workplaces.

4.1.3 Limitations

This section explains the main limitations of the dissertation. While the study provides useful theoretical insights, it relies heavily on existing literature. Although some empirical findings are drawn from prior work, the analysis is limited by the scope, quality, and focus of those studies. As highlighted in the synthesis, many of these prior works suffered from theoretical fragmentation, short-term focus, and methodological inconsistencies. As a result, some of the findings in this study could not be generalized or have not yet been empirically validated.

The classification of eight categories in Article 1 was based on selected theories drawn from the literature of criminology, psychology, and sociology. The aim was to identify how these theories explain the motivations and contextual factors that influence insider deviance. The review was based on established theories cited in high-ranking IS and security journals and conferences. However, these factors remain conceptual and have yet to undergo empirical testing. Therefore, these factors should be considered explanatory factors intended to guide future research. These factors form a foundation for a deeper analysis and theoretical refinement of insider deviance.

In Article 2, an integrative literature review was conducted to explore the limitations of the theories and their applications in IDB research. Our review again focused on articles published in high-impact journals across IS and security studies, selected

based on relevance and theoretical orientation. Though this approach ensures a comprehensive view from various perspectives, some relevant literature from other disciplines or lower-ranked journals may have been overlooked. Further, because the categorized limitations are interpretive, some subjectivity may have influenced how the theories were categorized.

Article 3, a research-in-progress paper, focused on developing context-specific constructs—AI-induced work strain, perceived inequity, and workload change. These constructs were based on adapted scales from validated instruments in technostress, organizational justice, and workplace strain literature, and were contextualized to reflect AI integration in the workplace. While the validity of the content was supported through feedback and pilot testing, the measures and model had not been tested at the time of submission. Thus, while these constructs show strong theoretical promise, final empirical validation is required to conclude their robustness and predictive power.

Article 4, also a research-in-progress, proposed using Design Thinking—operationalized through the DESTIC framework as a human-centered methodology for mitigating insider deviance. This conceptual approach combines iterative design, user empathy, and stakeholder collaboration to address technical vulnerabilities and the emotional and ethical dimensions of IDB. However, the framework had not been applied in a real-world setting, and its effectiveness remains untested. While the proposed phases are grounded in design and behavioral theories, practical implementation and evaluation will be necessary to establish their utility and adaptability across different organizational contexts.

This dissertation does not claim to have all the answers by acknowledging these limitations. Instead, it offers a step toward a more realistic, flexible, and human-centered understanding of insider deviance. It also highlights the ongoing need for deeper research, better methods, and collaboration across disciplines to keep up with the evolving nature of both threats and workplaces.

5 CONCLUSION

This dissertation examined insider deviant behavior (IDB) in information and cybersecurity by critically examining their theoretical, emotional, organizational, and technological explanations and influences. Through synthesizing four key research contributions, it has become clear that the current landscape of IDB research is defined by diverse theories but fragmented in their application. The use of isolated theories, each explaining only a piece of the problem, has limited our ability to understand and effectively mitigate insider deviant behaviors.

A key insight from this research is the need to center real-world experiences of insiders, rather than viewing deviant behavior as a product of fixed personality traits or simple rational decision-making. This dissertation positions IDBs as a response to dynamic pressures, emotional strain, cultural misalignment, technological disruption, and perceived organizational injustice. Articles 1 and 2 highlight the theoretical gaps and limitations, calling for theories beyond rationalist and rigid, control-focused approaches. Article 3 brings AI into the conversation, reframing technology not as a passive tool but as an active force that reshapes employee experience and moral agency. Article 4 presents a practical, participatory framework grounded in design thinking, providing a way for organizations to engage with insider threats more inclusively and adaptively. The conceptual nature of some frameworks, particularly DESTIC, suggests that further empirical work is needed to test their effectiveness in real-world settings. Additionally, the ethical and cultural implications of AI-driven security practices demand ongoing investigation as threats and technologies evolve.

Despite the studies limitaions, it contributes to a growing body of work that calls for more holistic, responsive, rigorous scientific methods and an ethically grounded understanding of insider threats and deviant behaviors. It lays the foundation for future research and practice that views security not merely as a matter of compliance, but as a shared organizational responsibility shaped by emotions, context, and the complex interplay between human and machine.

The challenge of insider deviance cannot be explained with inflexible models or one-size-fits-all policies. It requires theories that are as adaptive and multifaceted as the environments they aim to protect. This dissertation takes a step in that direction, inviting ongoing dialogue, design, and innovation in pursuit of safer, fairer, and more resilient digital workplaces.

References

Agnew, R. (1985). A revised strain theory of delinquency. *Social Forces*, *64*(1), 151–167.

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

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. *(No Title)*.

Almuthaybiri, M., Elongha, G., & Mgembe, I. (2024). Artificial intelligence in cyber threats intelligence (CTI): Capabilities of current AI models for deepfakes. *Issues in Information Systems*, *25*(2).

Anis, M., & Emil, D. (2022). The impact of job stress on deviant workplace behavior: The mediating role of job satisfaction. *American Journal of Industrial and Business Management*, *12*(1), 123–134.

Anti, E., & Vartiainen, T. (2024a). *Explanations of Insider Deviant Behavior in Information Security: A Systematic Literature Review*.

Anti, E., & Vartiainen, T. (2024b). Explanations of Insider Deviant Behavior in Information Security: A Systematic Literature Review. *Communications of the Association for Information Systems*, *55*(1), 4.

Arnold, R. D., & Wade, J. P. (2015). A definition of systems thinking: A systems approach. *Procedia Computer Science*, *44*, 669–678.

Ashenden, D., Black, R., Reid, I., & Henderson, S. (2021). *Design thinking for cyber deception*.

Balozian, P., Burns, A., & Leidner, D. E. (2023). An Adversarial Dance: Toward an Understanding of Insiders' Responses to Organizational Information Security Measures. *Journal of the Association for Information Systems*, *24*(1), 161–221.

Battistone, M. J., Kemeyou, L., & Varpio, L. (2023). The Theoretical Integrative Review—A Researcher's Guide. *Journal of Graduate Medical Education*, *15*(4), 453–455.

Beccaria, C. (1963). On crimes and punishments (H. Paolucci, Trans.). *Indianapolis, IN: Bobbs-Merrill.(Original Work Published 1764)*.

Bélanger, F., & Crossler, R. E. (2011). Privacy in the digital age: A review of information privacy research in information systems. *MIS Quarterly*, 1017–1041.

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, 1–3.

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

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

Burke, R. H. (2018). *An introduction to criminological theory*. Routledge.

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., 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.

Cacioppo, J. T., Semin, G. R., & Berntson, G. G. (2004). Realism, instrumentalism, and scientific symbiosis: Psychological theory as a search for truth and the discovery of solutions. *American Psychologist*, *59*(4), 214.

Chatterjee, S., Sarker, S., & Valacich, J. S. (2015). The behavioral roots of information systems security: Exploring key factors related to unethical IT use. *Journal of Management Information Systems*, *31*(4), 49–87.

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, H., Hai, Y., Tu, L., & Fan, J. (2024). Not all information security-related stresses are equal: The effects of challenge and hindrance stresses on employees' compliance with information security policies. *Behaviour & Information Technology*, *43*(16), 3939–3954.

Chen, L., Xie, Z., Zhen, J., & Dong, K. (2022). The impact of challenge information security stress on information security policy compliance: The mediating roles of emotions. *Psychology Research and Behavior Management*, 1177–1191.

Chuang, Y.-T., Chiang, H.-L., & Lin, A.-P. (2025). Insights from the Job Demands–Resources Model: AI's dual impact on employees' work and life well-being. *International Journal of Information Management*, *83*, 102887.

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.

Costa, D. L., Collins, M. L., Perl, S. J., Albrethsen, M. J., Silowash, G. J., & Spooner, D. L. (2014). An ontology for insider threat indicators. *Proceedings of the Ninth Conference on Semantic Technologies for Intelligence, Defense, and Security*, 48–53.

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. https://doi.org/10.1057/s41303-017-0059-9

Cropley, D. (2023). Creativity and morality in the world of technology: The intersection of creativity, design, and responsible problem-solving. In *Creativity and Morality* (pp. 283–302). Elsevier.

Cybersecurity Insiders. (2024). *Insider Threat Report Trends, Challenges, and Solution* (p. 26). www.securonix.com

Dam, R. F., & Siang, T. Y. (2021). *What is design thinking and why is it so popular?* Interaction Design Foundation London, UK.

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)*, 1–11.

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.

Denning, D. (1982). *Cryptography and Data Security*. Addison-Wesley.

Ding, X.-Q., Chen, H., Liu, J., Liu, Y.-Z., & Wang, X.-H. (2025). AI-induced behaviors: Bridging proactivity and deviance through motivational insights. *Journal of Managerial Psychology*.

Dorasamy, M., Joanis, G. C., Jiun, L. W., Jambulingam, M., Samsudin, R., & Cheng, N. J. (2019). Cybersecurity issues among working youths in an IOT environment: A design thinking process for solution. *2019 6th International Conference on Research and Innovation in Information Systems (ICRIIS)*, 1–6.

Dorst, K. (2011). The core of 'design thinking' and its application. *Design Studies*, *32*(6), 521–532. https://doi.org/10.1016/j.destud.2011.07.006

Elmrabit, N. (2018). *A multiple-perspective approach for insider-threat risk prediction in cyber-security.* [PhD Thesis]. Loughborough University.

Folger, R., & Cropanzano, R. (2001). Fairness theory: Justice as accountability. *Advances in Organizational Justice*, *1*(1–55), 12.

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

Giddens, A., & Griffiths, S. (2006). *Sociology*. Polity.

Goode, E. (2015). The sociology of deviance: An introduction. *The Handbook of Deviance*, 1–29.

Goode, E. (2022). *Deviant behavior*. Routledge.

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

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

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

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

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.

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.

Homoliak, I., Toffalini, F., Guarnizo, J., Elovici, Y., & Ochoa, M. (2019). Insight into insiders and it: A survey of insider threat taxonomies, analysis, modeling, and countermeasures. *ACM Computing Surveys (CSUR)*, *52*(2), 1–40.

Hou, Y., & Fan, L. (2024). Working with AI: The effect of job stress on hotel employees' work engagement. *Behavioral Sciences*, *14*(11), 1076.

Hsu, J. S.-C., Hung, Y. W., Hsieh, P.-J., & Chiu, C.-M. (2024). Examining formation and alleviation of information security fatigue by using job demands–resources theory. *Information Systems Journal*, *34*(6), 2132–2172.

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

Humphrey, J. A., & Schmalleger, F. (2012). *Deviant Behavior*. Jones & Bartlett Publishers.

Hunker, J., & Probst, C. W. (2011). Insiders and Insider Threats-An Overview of Definitions and Mitigation Techniques. *J. Wirel. Mob. Networks Ubiquitous Comput. Dependable Appl.*, *2*(1), 4–27.

IBM. (2024). *Cost of a Data Breach Report 2024*. https://www.ibm.com/reports/data-breach

IBM & Ponemon Institute. (2024). *Cost of a Data Breach Report 2024*. https://www.ibm.com/reports/data-breach

Ifinedo, P. (2017). Effects of Organization Insiders' Self-Control and Relevant Knowledge on Participation in Information Systems Security Deviant Behavior: [Best Paper Nominee]. *Proceedings of the 2017 ACM SIGMIS Conference on Computers and People Research*, 79–86.

Jang, J., Lee, D. W., & Kwon, G. (2021). An analysis of the influence of organizational justice on organizational commitment. *International Journal of Public Administration*, *44*(2), 146–154.

Kapoor, H. (2025). Shining a light on dark creativity. *Creativity Research Journal*, *37*(2), 236–241.

Keele, S. (2007). *Guidelines for performing systematic literature reviews in software engineering*. Technical report, ver. 2.3 ebse technical report. ebse.

Khan, F., Kim, J. H., Mathiassen, L., & Moore, R. (2021). Data breach management: An integrated risk model. *Information & Management*, *58*(1), 103392.

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

Kwon, H. R., & Silva, E. A. (2020). Mapping the landscape of behavioral theories: Systematic literature review. *Journal of Planning Literature*, *35*(2), 161–179.

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.

Leong, A. M. W., Bai, J. Y., Rasheed, M. I., Hameed, Z., & Okumus, F. (2025). AI disruption threat and employee outcomes: Role of technology insecurity, thriving at work, and trait self-esteem. *International Journal of Hospitality Management*, *126*, 104064.

Leukfeldt, E. R., & Yar, M. (2016). Applying routine activity theory to cybercrime: A theoretical and empirical analysis. *Deviant Behavior*, *37*(3), 263–280.

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.

Loch, K. D., Carr, H. H., & Warkentin, M. E. (1992). Threats to information systems: Today's reality, yesterday's understanding. *Mis Quarterly*, 173–186.

Lowry, P. B., & Moody, G. D. (2015). Proposing the control-reactance compliance model (CRCM) to explain opposing motivations to comply with organisational information security policies. *Information Systems Journal*, *25*(5), 433–463.

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.

Mady, A., Gupta, S., & Warkentin, M. (2023). The effects of knowledge mechanisms on employees' information security threat construal. *Information Systems Journal*, *33*(4), 790–841.

Matsunaga, M. (2022). Uncertainty management, transformational leadership, and job performance in an AI-powered organizational context. *Communication Monographs*, *89*(1), 118–139.

Mattson, T., Aurigemma, S., & Ren, J. (2023). Positively fearful: Activating the individual's HERO within to explain volitional security technology adoption. *Journal of the Association for Information Systems*, *24*(3), 664–699.

Mazzarolo, G., & Jurcut, A. D. (2019). Insider threats in Cyber Security: The enemy within the gates. *arXiv Preprint arXiv:1911.09575*.

Mensah, R. O. (2024). *Reviewing the Theoretical and Conceptual Frameworks in Criminology Research: A Positivity & Normativity Perspective from an African Researcher*.

Micheli, P., Wilner, S. J., Bhatti, S. H., Mura, M., & Beverland, M. B. (2019). Doing design thinking: Conceptual review, synthesis, and research agenda. *Journal of Product Innovation Management*, *36*(2), 124–148.

Mikalef, P., Lemmer, K., Schaefer, C., Ylinen, M., Fjørtoft, S. O., Torvatn, H. Y., Gupta, M., & Niehaves, B. (2023). Examining how AI capabilities can foster organizational performance in public organizations. *Government Information Quarterly*, *40*(2), 101797.

Mills, J. U., Stuban, S. M., & Dever, J. (2017). Predict insider threats using human behaviors. *IEEE Engineering Management Review*, *45*(1), 39–48.

Miryala, N. K., & Gupta, D. (2022). Data Security Challenges and Industry Trends. *IJARCCE International Journal of Advanced Research in Computer and Communication Engineering*, *11*(11), 300–309.

Moody, G. D., Siponen, M., & Pahnila, S. (2018). Toward a Unified Model of Information Security Policy Compliance. *MIS Quarterly*, *42*(1), 285–312, A1–A22.

Moore, M. (2011). Psychological theories of crime and delinquency. *Journal of Human Behavior in the Social Environment*, *21*(3), 226–239.

Nehme, A., Warkentin, M., Jang, K., & Kim, S. (2022). *Beyond Rational Information Security Decisions: An Alternate View*.

Nisafani, A. S., Kiely, G., & Mahony, C. (2020). Workers' technostress: A review of its causes, strains, inhibitors, and impacts. *Journal of Decision Systems*, *29*(sup1), 243–258.

Nurse, J. R., Buckley, O., Legg, P. A., Goldsmith, M., Creese, S., Wright, G. R., & Whitty, M. (2014). Understanding insider threat: A framework for characterising attacks. *2014 IEEE Security and Privacy Workshops*, 214–228.

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.

Pals, H., & Engin, C. (2019). Attachment to society and cognitive deviance: The case of Turkey. *Deviant Behavior*, *40*(7), 799–815.

Paternoster, R., & Simpson, S. (1996). Sanction threats and appeals to morality: Testing a rational choice model of corporate crime. *Law & Society Review*, *30*(3), 549–583.

Pfleeger, S. L., Predd, J. B., Hunker, J., & Bulford, C. (2009). Insiders behaving badly: Addressing bad actors and their actions. *IEEE Transactions on Information Forensics and Security*, *5*(1), 169–179.

Prabhu, S., & Thompson, N. (2022). A primer on insider threats in cybersecurity. *Information Security Journal: A Global Perspective*, *31*(5), 602–611. https://doi.org/10.1080/19393555.2021.1971802

Predd, J., Pfleeger, S. L., Hunker, J., & Bulford, C. (2008). Insiders behaving badly. *IEEE Security & Privacy*, *6*(4), 66–70.

Probst, T. M., Petitta, L., Barbaranelli, C., & Austin, C. (2020). Safety-related moral disengagement in response to job insecurity: Counterintuitive effects of perceived organizational and supervisor support. *Journal of Business Ethics*, *162*(2), 343–358.

Rauf, U., Mohsen, F., & Wei, Z. (2023). A taxonomic classification of insider threats: Existing techniques, future directions & recommendations. *Journal of Cyber Security and Mobility*, *12*(2), 221–252.

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

Razzouk, R., & Shute, V. (2012). What is design thinking and why is it important? *Review of Educational Research*, *82*(3), 330–348.

Robinson, S. L., & Bennett, R. J. (2024). JMI revisionist history of workplace deviance. *Journal of Management Inquiry*, *33*(4), 336–339.

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., & 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.

Roos, P., Gelfand, M., Nau, D., & Lun, J. (2015). Societal threat and cultural variation in the strength of social norms: An evolutionary basis. *Organizational Behavior and Human Decision Processes*, *129*, 14–23.

Rottweiler, B., Gill, P., & Bouhana, N. (2022). Individual and environmental explanations for violent extremist intentions: A German nationally representative survey study. *Justice Quarterly*, *39*(4), 825–846.

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.

Saxena, N., Hayes, E., Bertino, E., Ojo, P., Choo, K.-K. R., & Burnap, P. (2020). Impact and key challenges of insider threats on organizations and critical businesses. *Electronics*, *9*(9), 1460.

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)*, 1–7.

Schultz, E. E. (2002). A framework for understanding and predicting insider attacks. *Computers & Security*, *21*(6), 526–531.

Seymour, M., Riemer, K., Yuan, L., & Dennis, A. (2021). *Beyond deep fakes: Conceptual framework, applications, and research agenda for neural rendering of realistic digital faces*.

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

Snow, S., Happa, J., Horrocks, N., & Glencross, M. (2020). Using design thinking to understand cyber attack surfaces of future smart grids. *Frontiers in Energy Research*, *8*, 591999.

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

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

Tian, Y., Chan, T. J., Suki, N. M., & Kasim, M. A. (2023). Moderating role of perceived trust and perceived service quality on consumers' use behavior of alipay e-wallet system: The perspectives of technology acceptance model and theory of planned behavior. *Human Behavior and Emerging Technologies*, *2023*(1), 5276406.

Tong, J., Marx, J., Turel, O., & Cui, T. (2024). *Combatting Deepfake Misinformation on Social Media: A Scoping Review and Research Agenda*.

Torres, C. I., & Crossler, R. E. (2024). Promoting security behaviors in remote work environments: Personal values shaping information security policy compliance. *Information Systems Research*.

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.

Vasist, P. N., & Krishnan, S. (2022). Deepfakes: An integrative review of the literature and an agenda for future research. *Communications of the Association for Information Systems*, *51*(1), 14.

Von Solms, B. (2001). Corporate governance and information security. *Computers & Security*, *20*(3), 215–218.

Wahab, E., Ajiboye, O., Ogbeyemi, G., & Isaiah, S. (2023). *IntroductIon to SocIologIcal theory*.

Wall, D. S. (2017). Crime, security and information communication technologies: The changing cybersecurity threat landscape and its implications for regulation and policing. *Security and Information Communication Technologies: The Changing Cybersecurity Threat Landscape and Its Implications for Regulation and Policing (July 20, 2017)*.

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.

Webster, J., & Watson, R. T. (2002). Analyzing the past to prepare for the future: Writing a literature review. *MIS Quarterly*, xiii–xxiii.

Wilkes, N., Anderson, V. R., Johnson, C. L., & Bedell, L. M. (2021). Mixed methods research in criminology and criminal justice: A systematic review. *American Journal of Criminal Justice*, 1–21.

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

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

Wolfgang, M. E. (1963). Criminology and the criminologist. *J. Crim. L. Criminology & Police Sci.*, *54*, 155.

World Economic Forum. (2025). *Global Cybersecurity Outlook 2025:Insight Report*. https://reports.weforum.org/docs/WEF_Global_Cybersecurity_Outlook_2025.pdf

Xu, F., Hsu, C., Wang, T., & Lowry, P. B. (2024). The antecedents of employees' proactive information security behaviour: The perspective of proactive motivation. *Information Systems Journal*, *34*(4), 1144–1174.

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

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.

Yuan, S., & Wu, X. (2021). Deep learning for insider threat detection: Review, challenges and opportunities. *Computers & Security*, *104*, 102221.

Zhang, R. Z., Kyung, E. J., Longoni, C., Cian, L., & Mrkva, K. (2025). AI-induced indifference: Unfair AI reduces prosociality. *Cognition*, *254*, 105937.

Zoto, E., Kianpour, M., Kowalski, S. J., & Lopez-Rojas, E. A. (2019). A socio-technical systems approach to design and support systems thinking in cybersecurity and risk management education. *Complex Systems Informatics and Modeling Quarterly*, *18*, 65–75.

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.

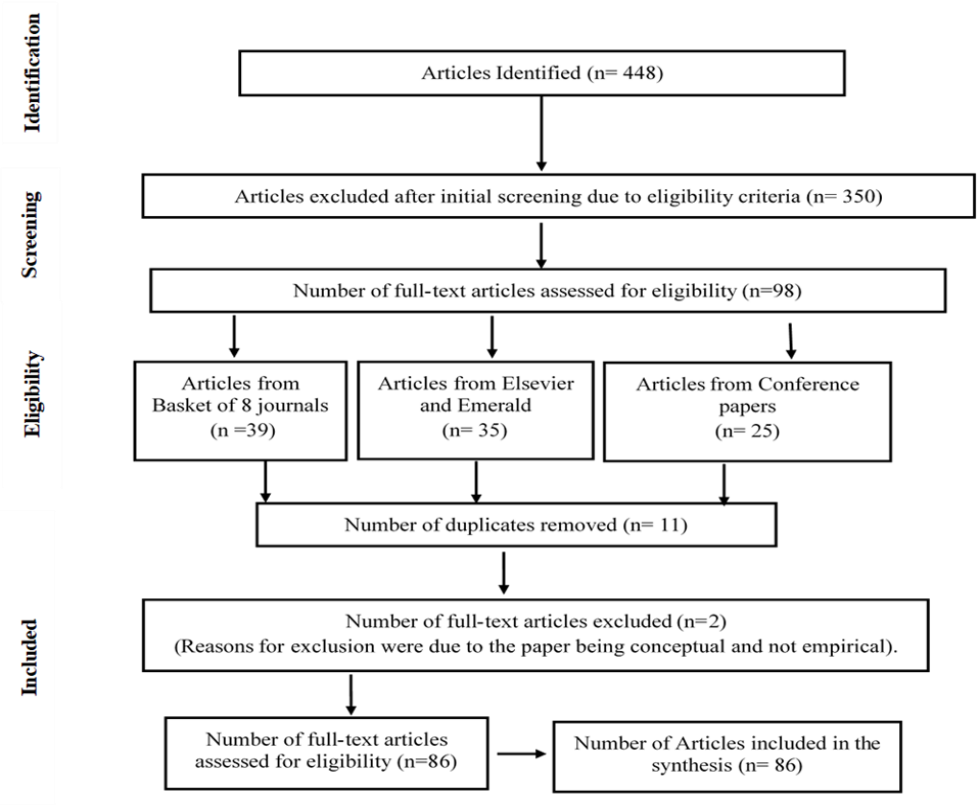

Figure 1. Prisma Flowchart Diagram

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.

Limitations of Theories on Insider Deviant Behavior Research in Information Security: A Theoretical Review and Research Agenda.

Emmanuel Anti, University of Vaasa, emmanuel.anti@uwasa.fi

Tero Vartiainen, University of Vaasa, tero.vartiainen@uwasa.fi

Rebekah Rousi, University of Vaasa, rebekah.rousi@uwasa.fi

Duong Dang, University of Vaasa, duong.dang@uwasa.fi

Abstract:

Information systems (IS) scholars focus increasingly on insider deviant behaviors (IDBs) in information security, examining why employees comply or fail to comply with organizational security policies. Researchers have applied theories from criminology (e.g., General Strain Theory), psychology (e.g., Fear Appeals Theory), and sociology (e.g., Social Control Theory) to study IDBs, offering valuable insights but with notable limitations. This study conducted a Theoretical Integrative Review (TIR) to analyze these limitations across 66 theories. We found that the limitations discussed in the literature can be categorized into Explanation, Prediction, and Prescription. We further applied thematic analysis to group these limitations into five themes: Inconsistencies in Research, Neglect of Influential Factors, Narrow Focus, Challenges in Predicting Behaviors, and Data and Methodological Issues, leading to the development of Action-Guiding Principles to refine and guide future research on IDBs. This study consolidates existing knowledge and highlights key research gaps, providing a comprehensive approach to understanding and mitigating insider threats in information security.

Keywords: Insiders Deviant Behavior, Information Security, Limitations, Theories, Review

Introduction

Information Systems (IS) scholars focus increasingly on the behavioral aspects of information security, applying theories from disciplines like psychology and criminology to study employees' compliance and non-compliance with organizational security policies (Nehme et al., 2022). Research on behavioral aspects of cybersecurity remains largely in the theory development stage (Khan et al., 2022). While human elements are widely recognized as critical factors in security issues (Chatterjee et al., 2015), the focus has been on refining and integrating theories to better capture the complexities of insider or employee behaviors. For example, foundational works such as deterrence theory provided critical early insights into compliance and deviance (Hollinger & Clark, 1983; Straub, 1990). Of significance to behavioral research in information and cybersecurity are insiders and their related deviant behaviors (Balozian et al., 2023). Yin et al. (2024) highlight the critical impact of employee behaviors on organizational information security. They underscore the need to understand the psychological and behavioral motivations and responses of employees to improve compliance and effectiveness.

Insiders can cause substantial damage to organizations, such as loss of revenue, weakened competitive positions, and loss of credibility, particularly when they are trusted individuals with legitimate access to various areas of organizations (Crossler et al., 2013; Green, 2014; Steele & Wargo, 2007). While the behavioral aspect of information and cybersecurity is important, Crossler et al. (2013) explain that much of information and cybersecurity research has concentrated on technological defenses and solutions. As cyber threats evolve, the importance of behavioral studies has grown, highlighting human factors as critical vulnerabilities that create backdoors into information and cybersecurity networks (Maalem Lahcen et al., 2020; Schneier, 2015; Siponen & Vance, 2010).

Unlike external attackers, deviant insiders and their potential to pose internal threats are challenging to detect and prevent (Burns et al., 2023; Hunker & Probst, 2011). Challenges arise due to inadequate measures, inconsistent definitions, fragmented awareness and mitigation efforts, and a lack of systematic collection evidence, all of which obscure the true scale and impact of incidents while overlooking the distinguishing human roles such as attackers and general users (Colwill, 2009; Khan et al., 2022). The motivations behind such IDBs are complex and multifaceted, often involving a combination of personal grievances, financial incentives, perceived organizational injustices, and psychological factors (Willison & Warkentin, 2013).

An IDB in information and cybersecurity has been defined as: "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…" (Anti & Vartiainen, 2024 p.127). The definition suggests that insiders' actions could be intentional/ malicious (Dang, 2014) or unintentional/non-malicious (Mady et al., 2023) and occur through planning (cognitive) and acting (behavior) (Hu et al., 2012). According to Dang (2014), malicious actions involve insiders intentionally misusing legitimate access to cause harm for personal gain, revenge, or ideology, while Nonmalicious Security Violations (NMSVs) are noncriminal rule-breaking actions prioritizing job performance over security compliance, risking security without malicious intent (Guo et al., 2011).

To understand these underlying motivations and intentions concerning IDBs, behavioral research has increasingly adopted theories from various disciplines such as sociology, criminology, and psychology. For instance, from sociology, the Theory of Planned Behavior (TPB) and Social Learning Theory (SLT) have been instrumental in explaining how social influences and perceived control over actions contribute to deviant behaviors (Ajzen, 1991; Bandura, 1977). Criminological theories, such as General Strain Theory (GST) and Routine Activity Theory (RAT), offer insights into how stressors and opportunities can drive individuals to commit insider attacks (Agnew, 1992; Cohen & Felson, 1979). Psychological perspectives, including the Theory of Moral Disengagement(TMD) and Fear Appeals Theory (FAT), shed light on the individual differences that make some employees more prone to engaging in malicious activities (Bandura, 1999; Rogers, 1983; Rogers & Deckner, 1975).

Although these theories offer valuable insights, their actual application in information and cybersecurity is not without limitations. Each theoretical framework presents a distinct perspective for examining IDBs from within a group, but none offers a comprehensive understanding. Our article examines these theories' limitations when exploring IDBs in information and cybersecurity. We further seek to develop action-guiding principles that can enhance the study IDB while emphasizing the specific areas where additional research and theoretical integration are required. Therefore, we propose the following research question:

RQ: What are the limitations of psychological, sociological, and criminological theories applied to IDB research in information security?

This paper is organized as follows: Section 2 discusses the theoretical overview of IDB studies in information and cybersecurity; Section 3 describes the methodology, Theoretical Integrative Review (TIR) for analyzing the theories and their limitations; Section 4 presents the findings; and describes the synthesis and process model development; Section 5 presents the discussions, research application, the research gaps and recommendations, and limitations. In particular, the discussion applies the classic insider leak case of Edward Snowden (Greenwald et al., 2013) as a case study to analyze the limitations identified. Here, we effectuate that Snowden's disclosure of classified information was the result of several factors that demonstrate limitations and incompatibilities in existing theories. The mixture of organizational, personal, contextual, and ethical factors highlights the complexity of real-life IDBs along with the insufficiency of existing theories and frameworks. In section 6, the conclusion, we consider the significance of the study and indicate future directions

Research Background

This section presents an overview of the theories commonly used in IDB research. Here, we also present a discussion on the nature and scope of these theories described, followed by an examination of their specific applications in understanding insider deviance in information security. By critically reviewing the limitations of these theoretical frameworks, we highlight their contributions and identify areas for further development in IDB research.

The Nature and Scope of Theories in Behavioral Information Security

Behavioral research in information and cybersecurity applies sociological, psychological, and criminological theories to analyze, explain, predict, and influence individuals' attitudes and behaviors for desired security outcomes. As cybersecurity threats become increasingly dynamic and complex, behavioral cybersecurity research emphasizes the need for robust theoretical frameworks to address these evolving challenges effectively. Notable theories applied to IDB research include Deterrence Theory (DT) (Beccaria, 1963; Gibbs, 1968), coping-oriented frameworks such as Protection Motivation Theory (PMT) (Rogers, 1975; Rogers & Prentice-Dunn, 1997), Fear Appeals Theory (FAT) (Rogers, 1983; Rogers & Deckner, 1975), and Neutralization Theory (NT) (Gresham & David, 1957; Sykes & Matza, 2017). These theoretical frameworks establish a basis that enhances our knowledge of IDBs by explaining reasons, perceived risks, and justifications that may prompt individuals to engage in deviant actions. For example, Johnston et al. (2023) highlight the prominence of fear appeals in influencing security behaviors while underscoring the growing concerns about their design and effectiveness. The authors call for contextually valid approaches tailored to specific threat environments. Similarly, Siponen et al. (2022) recognize DT as the most widely applied framework for explaining IS security behaviors but critique its misuse. They highlight the failure to distinguish between general and specific deterrence, the interchangeable use of terms, and the lack of scrutiny of its assumptions, which limits understanding of IS security behaviors in specific contexts. While DT focuses on external controls, Posey et al. (2011) emphasize the importance of internal cognitive processes, such as legitimacy perceptions and ethical decision-making, in compliance behaviors. Liang et al. (2019) also critique coping theories like PMT for neglecting emotion-focused coping, yielding inconsistent outcomes, and overlooking cultural contexts. They call for an approach that integrates cognitive and emotional factors to better explain IT security behavior. Siponen et al. (2022), Siponen and Vance (2010), and Posey et al. (2011) argue that these theories often assume static environments, not acknowledging the cognitive, cultural, and situational factors shaping security behaviors

Moody et al. (2018) note that applying psychological, sociological, and criminological theories has produced valuable insights but also a complex array of competing models. These models give rise to a myriad of information security behavioral models that pose difficulties regarding integration and simplification (Moody et al., 2018). Moody et al. (2018) observe that the growing number of models, while enriching, complicates integration and hinders the development of uniform frameworks for diverse organizational and security contexts.

Past research by Straub (1990) and Siponen and Vance (2010) highlights challenges in theories addressing all factors influencing behavior, particularly as cybersecurity threats become more complex. Foundational theories like the Technology Acceptance Model (TAM) (Davis, 1989) and the Theory of Planned Behavior (TPB) (Ajzen, 1991), while historically significant, face criticism for limited relevance in modern contexts. These limitations underscore the need for adaptive, integrative approaches to address evolving insider threats, prompting recent advancements in behavioral cybersecurity to refine and enhance theoretical frameworks.

Application of Theories in IDB Research

Applying theories from other disciplines to IDB research has yielded significant insights, yet limitations in their scope and adaptability continue. Deterrence Theory, for example, has been instrumental in IS security research to explain or predict behaviors or intentions (Siponen et al., 2022). Further, DT has been applied to understand how implementing effective IS security measures, such as dedicated security hours, clear policies, and penalties for violations, can significantly reduce computer abuse incidents (Straub Jr, 1990). Though coping-based theories such as PMT provide a basis for examining how individuals evaluate threats and formulate coping mechanisms in response to security risks, Siponen et al.(2024) argue that untested adaptations in IS security behavior research can hinder progress. They suggest that studies focus on specific components to deepen understanding, even if some elements are omitted. The theories under scrutiny often focus on broad patterns, but may not fully capture specific organizational and contextual dynamics involved in IDBs. Neutralization Theory (NT) has also enhanced research on insider threats (Gresham & David, 1957; Sykes & Matza, 2017), exploring how individuals justify and rationalize deviant actions, such as unauthorized access or manipulation of information.

Phenomena linked to insider threats and deviant behaviors have been thoroughly analyzed and described through diverse models and theories derived from other fields of study. For example, studies by Alawneh and Abbadi (2011), Maasberg et al. (2015), as well as Schoenherr and Thomson (2020) have conducted analyses and developed descriptions of insider threats by investigating different definitions, research methodologies, models, and critical assessments of information, and cybersecurity. Further, these studies have emphasized the diversity in definitions, ranging from broad descriptions of deviant behavior within organizations to more detailed distinctions based on individual characteristics and social contextual factors. The studies above have also explored many research methodologies, including deductive principles, computer models, and empirical observations using synthetic data sets to gain comprehensive insider knowledge. Mackey et al. (2021), Marasi et al. (2018), and Green (2014) provide a comprehensive understanding of workplace deviance, especially in the context of insider threats by explaining workplace deviance as voluntary behavior that violates significant organizational norms. In so doing, this behavior threatens the well-being of an organization, its members, or both. Green (2014) and Di Stefano et al. (2019) however, highlight that workplace deviance typically focuses on employees, but can also include former employees, vendors, and contractors. The study further highlights workplace deviance as incidents involving unauthorized access, manipulation, or tampering with information systems, networks, or data.

Some on-going studies are applying several underemployed theories to explore new dimensions of employee behavior in IS security research (see Table 1). For example, Zhao et al.(2024) are utilizing Cognitive Continuum Theory (CCT) (Hammond, 1981, 1988) to investigate employees' cognitive processes in complying with information security policies (ISPs) across various security environments. Similarly, Jiang and Nehme (2024) utilize the Legitimacy Process Theory (Suchman, 1995) to examine how the perceived severity of data breaches influences employees' perceptions of information security governance legitimacy, which mediates their non-compliance behaviors post-breach. These studies highlight the potential of underemployed theories to provide fresh insights into IDBs by addressing gaps in cognitive decision-making and governance perceptions. Understanding limitations as a residual of these studies can help inspire theory refinement,

innovative methodologies, and contextual understanding. This, ultimately leads to advancing IS security research with broader explanatory power and tailored strategies to address complex IDB challenges effectively

While these theories contribute valuable perspectives, they also face limitations in providing precise explanations, predictions, and prescriptions (see Figure 1). Gregor's (2006) study emphasizes that many theories address the goals of analysis, explanation, prediction, and prescription in varying degrees and manner. This suggests that theories applied in IDB research may effectively analyze and describe behaviors but can fail in their explanation, prediction, and prescription efficacy. For example, theories based on rational decision-making may overlook non-rational factors, such as emotional or context-specific events that tend to influence IDB. In addition, the proposed solutions from these theories may be too generic, lacking the specificity required to address the multifaceted nature of information and cybersecurity contexts effectively.

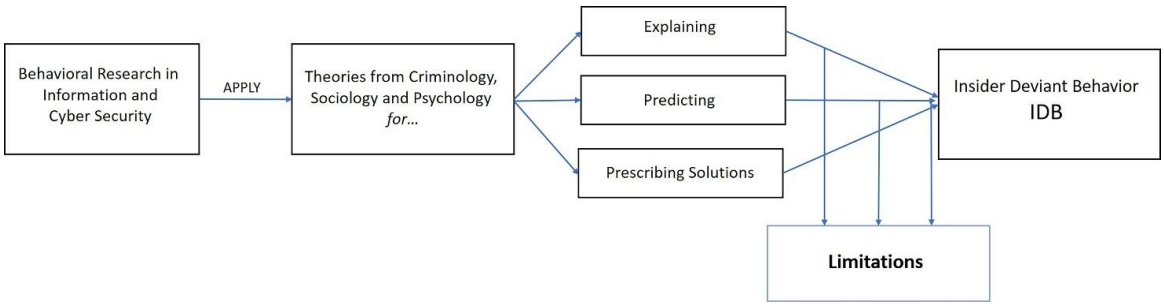

Figure 1 Application of Theories in IDB Research

In this study, we argue that addressing these theoretical limitations is essential to advance IDB research and improve practical applications. To address the research gap, we reviewed the information security literature to analyze theories and identify their limitations. IS research is dedicated to developing theories that systematically explain many areas within the field of study (Mueller & Urbach, 2017). According to Burton-Jones et al. (2015), IS theories take various forms—variance, systems, and process theories- each contributing uniquely through inductive, deductive, and abductive reasoning (Mueller & Urbach, 2017). Therefore, theories in IS research serve as both scientific outputs and instruments for understanding and tackling complex phenomena such as IDBs in information and cybersecurity. Leidner and Gregory (2024) defined theory as a scientifically grounded explanation of relationships among concepts within a specific set of assumptions. Gregor's (2006) four primary goals for theories continue to evolve, reflecting ongoing debate and theoretical refinement within IS, particularly in the domain of insider deviant behavior (IDB) research. This study contends that the behavioral theories applied to study IDBs have limitations in explaining, predicting, and prescribing solutions. Addressing the gaps in insider deviance research can enhance our understanding and mitigation of insider threats across various organizational settings by refining theories and developing context-sensitive frameworks.

Methods

Theoretical Integrative Review (TIR)

This study employed a TIR to critically examine and synthesize the limitations of psychological, sociological, and criminological theories applied to IDB research in information and cybersecurity. According to Battistone et al. (2023), a TIR compares and evaluates theories from the literature to explain a phenomenon. This is achieved by analyzing their premises, explanatory power, inconsistencies, and contributions, such as predictive, explanatory, or emancipatory insights. The purpose of a TIR, according to Battistone et al. (2023), is to reformulate or integrate theories related to a phenomenon, offering interpretations or arguments that may revise existing theories, assess their appropriateness for various research purposes, integrate elements

into new theoretical frameworks, or highlight theoretical limitations. Unlike other forms of literature reviews, which typically synthesize empirical data, a TIR focuses on clarifying the theoretical foundations that shape research on a given phenomenon (Battistone et al., 2023). Furthermore, TIRs analyze, critique, and advance theories with the understanding that they do not aim to produce a single "correct" explanation of a phenomenon. Instead, they acknowledge the fluidity, contextual variability, and interpretive nature of theories. This emphasizes openness to theoretical refinement, reinterpretation, and refutation (Battistone et al., 2023). TIR was chosen as the methodology for this study, as it provided an effective approach to thoroughly examine the limitations of psychological, sociological, and criminological theories in IDB research within information and cybersecurity. This methodology allowed for identifying gaps and proposing a research agenda, contributing to the development of more robust theoretical frameworks to address insider threats in the field.

Review Process

We conducted our TIR following well-established research methods outlined by Keele, (2007) as well as Webster and Watson (2002). The process was organized into three stages: plan, conduct, and report **(see Figure 2).** In the planning stage, we identified the need for the review, developed a review protocol, and evaluated it. During the conduct stage, we searched databases, selected relevant studies, and reviewed them. Finally, in the reporting stage, we presented our findings.

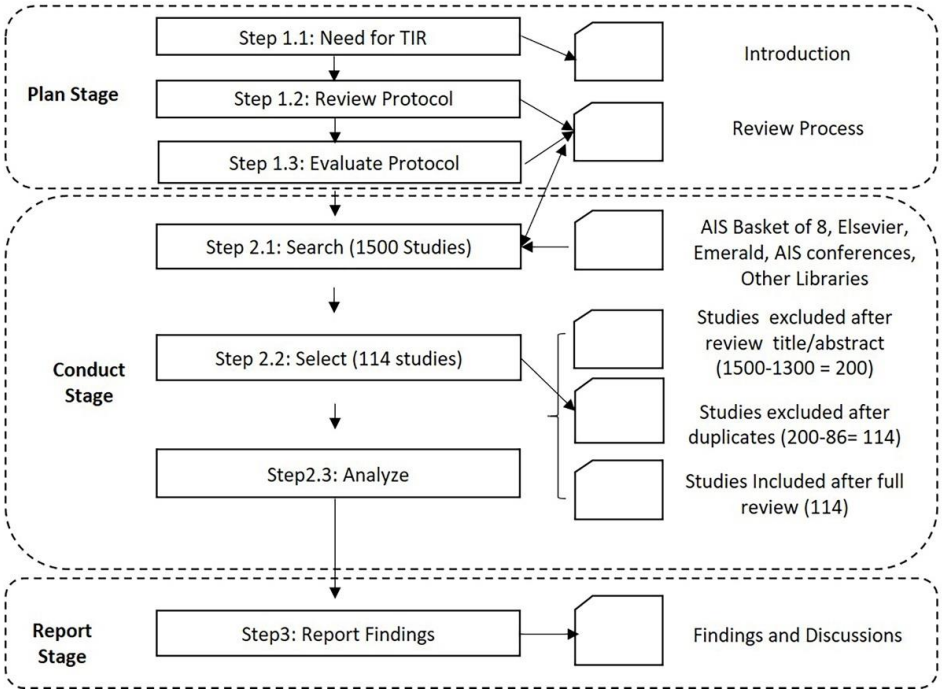

Figure 2 Stages of the Review Process

Our TIR examines the limitations of theories applied to research IDBs within information and cybersecurity. We utilized rigorous inclusion and exclusion criteria to analyze the literature on IDB in information and cybersecurity through criminological, sociological, and psychological perspectives. Our inclusion criteria emphasized: (1) peer-reviewed studies; (2) studies in English; (3) studies published between 1990 and 2024; (4) studies focusing on employees' or insiders' behavior in information and cybersecurity; (5) applied theoretical frameworks relevant to IDB; and (6) enhanced understanding of factors affecting insider behavior

in organizational settings. Studies were excluded if they: (1) predominantly addressed technical or external cybersecurity threats; (2) were short papers; or (3) were opinion articles, commentaries, or brief reports.

We searched key IS academic journals, including the AIS "Basket of 8," Elsevier, Emerald, IS conference proceedings (ECIS, HICSS, AMCIS, ICIS), and databases like Scopus, Web of Science, and Google Scholar, using targeted keywords: ("insider" OR "employee") AND ("information security") AND ("theory" OR "theoretical framework"). This approach critically assessed and refined the literature to fit our scope, explore theoretical limitations in IDB studies, and develop a research framework.

We performed an analysis of 114 articles. First, we carefully evaluated the theories presented in the identified studies to determine whether any of the theories included in the articles were applied to study IDBs. Next, our analysis centered on examining the limitations of these studies, with a specific focus on the limitations of the identified theories and their application in the research of IDBs. To identify categories of limitations, we used grounded theory (Birks & Mills, 2015) as an approach to code initial findings into themes.

The first author evaluated the articles, identified and categorized the limitations. Another author coded the limitations into subthemes and themes, which were then discussed with the first author, these themes were subsequently brought to the entire research team and coauthors for discussion and feedback. As a result, we identified five themes, each with descriptions and solutions, which are presented in the following sections. Throughout our discussions and analysis, we carefully compared and contrasted the concepts presented in the articles, applied theories, findings obtained, limitations, and the themes identified. Our meetings were conducted hybrid, involving in-person and online meetings via Zoom. We concentrated on identifying the theories and evaluating their limitations in their applications to studies on IDBs.

Data Synthesis

We analyzed 114 articles to identify the theories utilized along with how they were applied in IDB research. Next, we analyzed the identified limitations and categorized them into three groups: explanation, prediction, and prescription. Further, we grouped the identified limitations into five (5) themes to enhance the study of IDBs from various theoretical frameworks, providing a more nuanced discussion on how each limitation affects the applicability of findings across diverse contexts. The five themes emerged through identifying a saturation point in the limitations represented within the literature, whereby clear patterns were noticed (Ando et al., 2014). Initial themes were identified in the limitations of the studies, these were then coded according to the type of limitations that the themes represented. We also identified ongoing studies that apply various theories from which we understand that scholars are attempting to address limitations. Thus, their limitations were not analyzed as these studies are still in progress and therefore were excluded from this review. Table 1 summarizes ongoing studies and their applied theories. Subsequently, we synthesized the findings.

Table 1 Identified ongoing studies applying various theories

Theories	Identified Studies
Identity Theory (Burke & Reitzes, 1991)	(Davis, 2024)
Cognitive continuum theory (Hammond, 1981, 1988)	(Zhao et al., 2024)
The theory of the legitimacy process (Suchman, 1995)	(Jiang & Nehme, 2024)
Theory of social influence (Kelman, 1958)	(Agrawal et al., 2023)
Trait activation theory (TAT) (Tett et al., 2013, 2021; Tett & Burnett, 2003)	(Austin, 2023)
Stewardship theory (J. H. Davis et al., 1997)	(Ogbanufe, 2018)

Moral licensing theory (Monin & Miller, 2001)	(Jia & Xu, 2021)
Social exchange theory (Homans, 1958)	(McKnight et al., 2024)

Findings

We examined 66 theories from the review and categorized their limitations into Explanation, Prediction, and Prescription. Tables 4 to 7 (see Appendix A, B, and C) show the categorized limitations. We further grouped the identified limitations into five (5) themes: Inconsistencies in Research, Neglect of Influential Factors, Narrow Focus, Challenges in Predicting Behaviors, and Data and Methodological Issues, summarized in Table 2.

Table 2: Identified Themes

Themes	Description	Solution
Inconsistencies in Research	Identify and document contradictory findings, short-term focus, and restrictive frameworks.	Conduct meta-analyses and longitudinal studies to reconcile inconsistencies and develop comprehensive frameworks.
Neglect of Influential Factors	Include personality, cultural differences, and fear control processes in research designs.	Develop multi-dimensional models that account for these factors and their interactions with security behaviors.
Narrow Focus	Broaden the scope to include diverse security threats, ethical concerns, and real-world applications.	Implement holistic approaches that integrate various security threats and ethical considerations into the models.
Challenges in Predicting Behaviors	Address the complexity of interactions, limited generalizability, and need for integration with other frameworks.	Use advanced statistical methods and machine learning to improve predictive accuracy and integrate findings from multiple theoretical frameworks.
Data and Methodological Issues	Improve data collection methods, address biases, and enhance measurement techniques.	Employ mixed-methods research, including qualitative and quantitative approaches, to capture nuanced behaviors and improve data reliability.

The description of the themes are as follows:

1. **Inconsistencies in Research:** The study of IDB within information and cybersecurity faces limitations such as research inconsistencies, often stemming from contradictory findings, short-term focus, and the use of restrictive theoretical frameworks. Iivari et al. (1998) and Recker et al. (2019) suggest that the results obtained from such inconsistencies are often piecemeal, and conflicting due to the lack of a thorough systematic approach, with the credibility of the results largely dependent on how well the theoretical framework's categories are accepted, and recognized. For instance, the application of deterrence theory in information and cybersecurity behavioral research has yielded mixed results. Some studies suggest that sanctions effectively deter security-related behaviors, while others find no significant impact, particularly in non-malicious IS violations (Siponen et al., 2022). Other studies also report that sanctions can have a limited impact on policy compliance, as certainty may increase compliance intentions, while severity is less influential, with social pressures and perceived effectiveness playing crucial roles (Willison et al., 2018). Further, excessive controls may backfire, causing employee alienation and disrupting organizational activities (Warkentin & Willison, 2009). Additionally, the varying classification of insider threats across studies has created confusion and hindered consensus, making it difficult to effectively compare incidents and identify emerging threats (Predd et al., 2008).

To address these limitations in IDB research, this study proposes researchers conduct meta-analyses that can synthesize existing research, providing a clearer understanding of the phenomenon (Okoli & Schabram, 2015). Moreover, implementing longitudinal studies would allow for the examination of insider behaviors over extended periods, offering insights into the temporal dynamics and long-term effects of security policies (D'Arcy & Lowry, 2019; Warkentin et al., 2016). Developing comprehensive frameworks that integrate diverse theoretical perspectives can also enhance the consistency and applicability of research findings (Wiesche et al., 2017), ultimately contributing to more effective strategies for mitigating insider threats.

2. **Neglect of Influential Factors:** Studying insider deviant behavior in information and cybersecurity requires analyzing critical overarching factors such as the influence of cultural, fear control processes, organizational, environmental, and situational contexts on IDB (malicious and non-malicious). Cultural factors, such as national culture, shared values, and beliefs, can influence individual attitudes and behaviors (Connolly et al., 2014), while internal and external environmental and situational factors can motivate behaviors and actions (Gutierrez et al., 2015; Johnston et al., 2016). Organizational factors like policies and controls can impact information and cybersecurity behaviors (Luo et al., 2020; Warkentin & Willison, 2009). Moreover, cultural contexts influence social behavior and compliance (Tsohou et al., 2015), especially in societies where fear of retribution maintains order, often leading to maladaptive coping mechanisms driven by cultural norms on authority and punishment (Tsohou et al., 2015). Contextual factors such as organizational culture (Box & Pottas, 2014), leadership (Guhr et al., 2019), power dynamics (Soares et al., 2007), ethics and values (Gwebu et al., 2020), as well as organizational challenges (Alotaibi et al., 2016) significantly shape IDBs.
   To ensure a comprehensive understanding of IDBs, it is crucial to consider these critical factors from the outset and develop multidimensional models that integrate their interactions with security behaviors. Incorporating these elements can enhance explanatory power, improve predictive accuracy, and ensure more effective interventions. Overlooking such critical factors can lead to an incomplete understanding of IDBs, oversimplified conclusions, and ineffective solutions.
3. **Narrow Focus:** Research on IDBs often adopts a narrow focus, emphasizing specific threats or isolated incidents while overlooking broader security challenges and ethical considerations. Understanding the dynamic nature of threats is crucial for distinguishing potential risks from actual harms (Wall, 2017). A limited perspective can lead to fragmented strategies that fail to address the complex interplay of risk factors. Expanding the scope to include diverse security threats, ethical concerns, and real-world applications enhances the understanding of insider deviant behaviors, including sabotage, fraud, social engineering, and unauthorized access.
   To address the narrow focus in IDB studies, a holistic approach is needed, integrating interdisciplinary perspectives, diverse methodologies, and broader security concerns (Dhillon et al., 2021). This can be achieved by incorporating socio-organizational and socio-technical orientations (Dhillon et al., 2021), applying supplementary theoretical lenses, and developing frameworks that capture both process and variance perspectives (Cram et al., 2017). Aligning academic research with practitioner concerns such as security attacks and system vulnerabilities ensures a more comprehensive understanding of security challenges, bridging the gap between theory and real-world application.
4. **Challenges in Predicting Behaviors:** Predicting IDBs in information and cybersecurity is challenging due to complex interactions, limited generalizability, and the need for integrated frameworks. While machine learning (ML) enhances prediction accuracy, managing data variability is crucial to prevent overfitting and ensure real-world applicability (Bharadiya, 2023). The dynamic nature of insider threats further complicates predicting. To address this, researchers have leveraged advanced statistical methods and ML techniques to improve predictive accuracy and adaptability to evolving security challenges. For instance, anomaly detection algorithms can be utilized to model user behavior and identify deviations indicative of potential threats (Goldberg et al., 2017). These

algorithms analyze structural, semantic, and temporal data features to identify anomalies by detecting deviations from behavioral baselines, such as unusual URLs accessed or excessive file transfers to removable media (Goldberg et al., 2017). Additionally, integrating diverse theoretical perspectives, such as criminology, sociology, and psychology, into comprehensive models can assist in providing a more holistic understanding of insider deviant behavior. By integrating advanced analytical techniques with theoretical models, researchers can enhance the prediction and mitigation of insider threats.

5. **Data and Methodological Issues:** Research into IDBs within information systems has been hindered by methodological issues, including inadequate data collection methods, biases, and suboptimal measurement techniques. The evolving nature of insider threats and human actions makes accurate predicting difficult, requiring a mixed-methods approach that combines qualitative and quantitative analysis to provide deeper insights and enhance reliability (Huysmans & De Bruyn, 2013). This strategy enables the capture of nuanced behaviors and enhances data reliability. An integrated multidisciplinary approach to cybersecurity can improve prescribing solutions by combining technical and non-technical countermeasures (Pollini et al., 2022). For instance, integrating qualitative insights from interviews or focus groups with quantitative data from surveys or behavioral analytics can provide a comprehensive understanding of the factors influencing deviant behaviors. Such an approach not only mitigates biases inherent in single-method studies but also improves the robustness of findings, thereby contributing to more effective interventions and policies aimed at mitigating insider threats. Additionally, cultural and value theories offer a framework for understanding how societal norms influence individual actions (Schwartz, 2006), while qualitative threat analysis helps prioritize risks, involve non-experts, and utilize expert opinions for risk ranking (Shameli-Sendi et al., 2016). This user-centered, data-driven methodology addresses human factors and socio-cultural variables and adapts to different organizational settings. It simplifies implementation guidelines, enhances applicability, and promotes stakeholder engagement (Pollini et al., 2022)

Discussion

We identified the limitations of theories from different disciplines when applied to information and cybersecurity to study IDBs. We then classified the limitations into three categories: Explanation, Prediction, and Prescription, based on the primary goals of the theory as emphasized by Gregor (2006). In our study, we excluded the goals of analysis and description (Gregor, 2006) from our identified limitations by arguing that insider threats and deviant behaviors have been thoroughly analyzed and described by utilizing diverse models and theories from other fields of study. Further, we coded and grouped the identified limitations into five (5) themes: Inconsistencies in Research, Neglect of Influential Factors, Narrow Focus, Challenges in Predicting Behaviors, and Data and Methodological Issues. Additionally, we developed action-guiding principles (Table 3) to provide a comprehensive, multidisciplinary approach to research, understand, and mitigate IDBs in information and cybersecurity contexts. The essence of the developed principles is to help address key limitations by providing a structured yet adaptable approach that can enable researchers to systematically examine IDB while accounting for the complexities and evolving nature of cybersecurity threats. For example, integrating several theories in IDB research can improve understanding, but it also poses challenges and compatibility concerns. Some theories may be challenging to integrate because of assumptions, scope, and focus variances. For example, the Theory of Planned Behavior (TPB) concentrates on individual intentions and attitudes, while General Deterrence Theory (GDT) highlights sanctions and controls. The combination of these theories may result in conceptual challenges due to their different fundamental assumptions and methodologies for explaining behavior. Compatibility concerns may complicate analysis, undermining theoretical clarity and restricting the effective use of integrated models in IDB research. Our action-guiding principles integrate this knowledge and establish a foundation for future

research to minimize IDBs in information and cybersecurity. Further, the developed principles function as a proposal for developing a theory for further studies of IDBs.

Research Application – Case Study Edward Snowden.

To demonstrate the research application of the themes identified, we may consider Snowden's disclosure of classified information (Greenwald et al., 2013) as a case study. The case of Edward Snowden can reveal crucial factors that must be considered when researching similar IDBs. His actions, motivations, and the organizational response highlight key limitations in current theoretical frameworks and methodological approaches. The themes of inconsistencies in research, neglect of influential factors, narrow focus, challenges in predicting behaviors, and methodological issues can be applied to better understand and study such complex cases.

Inconsistencies in Research

Research on IDBs in information and cybersecurity has produced contradictory findings regarding the motivations and deterrence mechanisms on deviant actions. For example, the organizational culture (Connolly et al., 2017; Hina et al., 2019) at the National Security Agency (NSA) characterized by secrecy, limited internal grievance channels, and low transparency may have contributed to Snowmen's deviant actions. However, the extent to which such factors directly influence IDB remains debated, with some studies emphasizing toxic organizational environments such as stress and lack of support (Cram et al., 2017) may act as primary drivers of IDBs while others focus on individual motivations or situational factors such as beliefs and values (Safa et al., 2015). Contradictory findings also emerge regarding the role of deterrence in preventing insider threats. Snowden's case illustrates this inconsistency, as strict cybersecurity policies and potential legal consequences failed to prevent his actions, contradicting studies that view deterrence theory as a strong predictor of compliance. Further, some studies argue that ideological motivations override security policies (Willison & Warkentin, 2013), while others attribute IDB to weak monitoring systems (Posey et al., 2011). Fear's role is also debated, as it may drive maladaptive coping (Mattson et al., 2023), but its impact remains unclear. Cultural dimensions like power distance show conflicting effects on compliance (Hofstede, 1984; Soares et al., 2007), highlighting the need for integrative research.

The organizational environment in the case of Snowden, may have fostered fear, a toxic, unethical culture with less transparency and accountability, increasing the risk of deviant behavior. Mattson et al. (2023) explain that fear can influence deviant behaviors by driving individuals toward maladaptive coping mechanisms, such as fear control, where they avoid threats rather than addressing them, disrupting rational decision-making and prompting risk-averse or deviant actions to mitigate fear. In addition, cultural dimensions, such as the power distance index (PDI) (Hofstede, 1984; Soares et al., 2007), which reflects the consequences of power inequality and authority relations in society, must be considered when studying IDBs. For example, in high power distance environments, employees may hesitate to report unethical behavior, comply with harmful directives, or engage in deviant acts due to perceived inequalities. Leadership styles shaped by high PDI can hinder the development of a security-conscious culture, increasing the risk of mismanaging insider threats.

Neglect of influential factors

Some studies on IDB overlook critical psychological and cultural factors that influence security behaviors, leading to an incomplete understanding of the phenomenon. For example, Snowden's actions underscore the importance of critical psychological, cultural, and social factors in IDB research. His moral beliefs and rationalizations likely influenced his justification for leaking NSA documents as serving the public interest, highlighting the role of individual motivations and ethical reasoning. Additionally, exposure to whistleblower culture and privacy advocacy groups may have reinforced his decision, demonstrating how social influences shape insider behaviors, factors that can easily be overlooked in traditional security models that focus solely

on technical controls and policy compliance. A multi-dimensional approach is essential to understanding IDBs beyond financial or retaliatory motives. Gathering influential factors early in IDB research provides a comprehensive foundation for explaining the environments in which these behaviors occur. Identifying underlying causes and motivations allows for a nuanced analysis of human behavior in workplace culture. For example, moral beliefs (Baskerville et al., 2014; Luo et al., 2020), rationalizations (Barlow et al., 2013, 2018), and perceived outcomes (Li et al., 2021; Siponen et al., 2014). Societal norms (Hooper & Blunt, 2020; Moody et al., 2018), peer relationships (Ifinedo, 2014, 2019), and collective attitudes (Posey et al., 2015) toward security policies significantly impact insider behaviors. Strong social bonds within an organization (Burns et al., 2023) can either deter or encourage deviance, depending on how security norms are internalized. Without considering these influences, security interventions may fail to address the root causes of IDB. Additionally, insider threats continually evolve over time, including sabotage, fraud, social engineering, unauthorized access, and data leaks. The motivations behind these threats shift due to organizational changes, technological advancements, and emerging security vulnerabilities. Failing to incorporate these critical factors into research limits the ability to develop effective mitigation strategies. Future studies must adopt an integrative approach that accounts for psychological, cultural, and social dimensions to provide a more accurate and comprehensive understanding of insider deviant behavior.

Narrow Focus

Existing research on IDB often focuses narrowly on specific security violations, such as unauthorized data access or financial fraud, without addressing broader ethical concerns and real-world implications. This shift is partly due to the practical difficulties of obtaining valid instances of employees' negative computing behaviors and the increase in security policies (Cram et al., 2017). Additionally, Karlsson et al. (2015) indicate that Information security research often concentrates on a limited set of security violations, with most studies focusing on a few dominant topics, a trend also noted by Willison and Siponen (2007), who observed a narrow focus in the broader field of information security research. The case of Snowden underscores the necessity to broaden this research scope to encompass ethical dilemmas (Gwebu et al., 2020), perceptions of organizational justice (Lowry et al., 2015; Warkentin et al., 2011), and the impact of mass surveillance policies on insider decision-making. Snowden's actions, driven by personal ethics and a belief in government transparency, highlight how ethical considerations can influence insider behavior. A holistic approach should integrate these ethical dimensions into insider threat models, assessing not only the occurrence of security violations but also understanding the moral or legal justifications individuals may use. To address the narrow focus in information security research, Karlsson et al. (2015) advocate for scholars to expand research topics beyond dominant areas; and ensure greater transparency in research methodologies, particularly in information security culture studies

Challenges in Predicting Behaviors

Predicting IDB presents significant challenges due to the complexity of interactions among various factors, limited generalizability of findings, and the necessity for integrating multiple theoretical frameworks (Shropshire et al., 2015). The case of Edward Snowden provides a real-world example of the difficulties in predicting insider threats. Snowden’s actions highlight the dynamic and multifaceted nature of insider threats, demonstrating how personal beliefs, workplace grievances, and access privileges converge to create security vulnerabilities.

To enhance predictive accuracy, researchers must apply advanced statistical methods and machine learning (ML) techniques. These approaches can retrospectively analyze access patterns and communications to establish baselines of normal behavior, identifying deviations that may indicate potential security threats(Bouchama & Kamal, 2021; Duary et al., 2024). In Snowden’s case, an AI-monitored system could have flagged unusual access patterns, such as retrieving large volumes of classified files outside his typical work scope or transferring sensitive data across networks. While such techniques improve detection capabilities,

real-time implementation remains challenging due to the vast amount of data generated and the need to differentiate between benign and malicious activities without excessive false positives or negatives. Therefore, adaptive risk models are essential as they can continuously evaluate insider risks by incorporating both qualitative and quantitative data, considering cultural norms, and adapting to evolving technologies and employee behaviors. Such models can adjust user privileges in response to suspicious behavior, thereby mitigating potential threats. If applied in Snowden's scenario, an adaptive model might have identified risk factors such as his growing disillusionment with government policies by analyzing sentiment changes in communications or behavioral shifts in accessing classified information. Implementing dynamic user privilege adjustments in response to suspicious activity could have restricted unauthorized data access, potentially preventing or mitigating the leak.

Integrating findings from multiple theoretical frameworks is also crucial. A psychosocial model assessing employees' behaviors associated with increased risk of insider abuse could have provided valuable insights into Snowden's motivations. Such models consider various psychological and social factors that influence behavior, allowing for an understanding of the motivations and circumstances that lead to insider abuse (Shropshire et al., 2015). Recognizing and recording such behaviors can enhance the effectiveness of predictive models. By combining advanced analytical approaches with integrative theoretical models, the field can improve the prediction and mitigation of insider threats in information and cybersecurity.

Data and Methodological Issues

Research on insider deviant behavior (IDB) often faces methodological challenges, including biased data collection and an over-reliance on self-reported surveys, which can limit the accuracy and depth of insights (Snyman & Kruger, 2019). These issues can undermine data accuracy and depth, as poorly structured questionnaires may cause respondent confusion, while the sensitive nature of survey topics can lead to social desirability bias, resulting in inaccurate responses (Snyman & Kruger, 2019). Traditional security audits and behavioral monitoring often miss gradual shifts in insider motivations, as they prioritize immediate threats and deviations while overlooking subtle, progressive behavioral changes (Shropshire et al., 2015). As seen in the case of Edward Snowden, standard security measures might not have flagged his evolving intent to leak classified information, as his actions were likely rationalized over time rather than being impulsive violations. This highlights the need for researchers to adopt broader research methods, including mixed-methods and critical approaches; conduct theoretically grounded empirical studies to mitigate theoretical underdevelopment (Karlsson et al., 2015). For example, a mixed-methods approach—integrating quantitative analytics (e.g., behavioral data analysis, anomaly detection, and statistical modeling) with qualitative insights (e.g., interviews, retrospective case studies)—can provide a more nuanced understanding of insider threats. For instance, analyzing Snowden's digital footprint over time, including shifts in communication patterns, access to classified files, and engagement with external entities, might have revealed early indicators of deviant behavior. Complementing this with qualitative analysis, such as interviews with colleagues or assessments of his ideological transformation, could have offered deeper insights into the rationalization process that led to his whistleblowing decision.

Furthermore, retrospective case studies of real-world security violators can help uncover long-term behavioral patterns that traditional short-term studies often overlook. Snowden's case illustrates how insiders may gradually shift their motivations and justifications, making it crucial to adopt a comprehensive theoretical framework. Rather than relying solely on existing models, research should aim to develop prescriptive theories that account for evolving insider behaviors, mitigating IDBs more effectively. By incorporating a multi-faceted analytical approach, organizations can better anticipate and prevent insider threats before they materialize into major security breaches.

Action-Guiding Principles and Research Agenda

Based on our findings, we have developed action-guiding principles designed as flexible guidelines for researchers conducting IDB research in information and cybersecurity. These principles aim to address key limitations in the field, including inconsistencies in research, neglect of influential factors, a narrow focus, challenges in predicting behaviors, as well as data and methodological issues. The framework covers essential aspects such as research perspectives, principles, in addition to research gaps and recommendations**.** By providing a structured yet adaptable approach, these principles enable researchers to systematically examine IDB while accommodating the complexities and evolving nature of cybersecurity threats. We further identified additional areas of research that we recommend for further investigation in the field of IDBs. Table 3 highlights the action-guiding principles and research recommendations.

Table 3 Action Guiding Principles

Perspective	Principles	Research Gaps and Recommendations
Theory	**Interdisciplinary theoretical synthesis**: Researchers should construct its theoretical foundation of insider deviant behavior by systematically integrating perspectives from diverse disciplines—such as psychology, sociology, organizational studies, criminology, and cybersecurity—to ensure a comprehensive understanding of multifaceted phenomena. (Rai, 2018; Seidel & Watson, 2020)	• *Exploring the integration of multiple disciplinary lenses to understand a complex insider deviant behavior*: How do psychological traits (e.g., impulsivity), sociological factors (e.g., peer influence), organizational structures (e.g., hierarchy), criminological opportunity models, and cybersecurity vulnerabilities collectively shape the emergence of insider deviance in organizational settings? • *Testing the predictive power of an interdisciplinary theoretical model for insider deviant behavior:* To what extent can a synthesized framework from sociology (social norms), psychology (motivation), and cybersecurity (system weaknesses) predict employee compliance with data protection policies across different industries? • *Seeking new theoretical contributions to theory of insider deviant behavior through cross-disciplinary synthesis:* What theoretical insights emerge from combining organizational studies (leadership styles), criminology (deviance pathways), and psychology (stress responses) to explain variations in deviant behaviors within organizations?
Context	**Contextual Embeddedness**: Researchers of insider deviant behavior must prioritize the incorporation of specific organizational cultures, workplace practices, and contextual settings to avoid overgeneralization and ensure accurate reflection of the contexts under study. (Avgerou, 2019; Kearns & Lederer, 2004)	• *Examining how organizational culture as a contextual variable shapes insider behavior:* How do the specific cultural norms of a flat organizational structure (e.g., Finland culture) versus a hierarchical one (e.g., Japanese culture) influence the prevalence and nature of insider security breaches in an organization? • *Focusing on the role of workplace practices in modifying risk profiles with insider threats:* In what ways do workplace practices, such as flexible remote work policies, alter the risk factors associated with insider threats compared to traditional office-based settings?

		• *Embedding broader contextual variables into the analysis of insider behavior or threat:* How do contextual pressures, such as regional economic instability or political changes, interact with organizational policies to affect employee decisions to engage in intellectual property theft?
Ethics	**Ethical Reflexivity**: Researchers should continuously evaluate the moral implications of its classification of individuals as "insiders" or "threats.", uphold rigorous standards of privacy and consent in data collection, and critically assess its potential effects on trust and justice within organizational settings. (Mingers & Walsham, 2010)	• *Evaluating the moral consequences of classification of employees and its organizational effects in insider deviant behavior research:* What are the ethical implications of using predictive algorithms to classify employees as potential insider threats, particularly regarding their impact on workplace trust and fairness perceptions? • *Addressing ethical standards in data practices within high-stakes contexts in insider deviant behavior research:* How can data collection methods be designed to ensure informed consent and confidentiality when studying insider behaviors in sensitive industries like healthcare or defense? • *Reflecting on the broader ethical ramifications of research application in insider deviant behavior research:* To what extent do research findings on insider threats, if implemented in surveillance policies, compromise employee autonomy and organizational justice in multinational corporations?
Methods	**Methodological Dynamism and Integration**: Research methodologies should be adaptive, combining qualitative and quantitative approaches with innovative tools (e.g., simulations, machine learning, AI) to iteratively refine frameworks, capture dynamic interactions, and address both individual and systemic dimensions of phenomena. (Siponen & Oinas-Kukkonen, 2007)	• *Combining qualitative and quantitative methods to study evolving phenomena in insider deviant behavior research:* How can a mixed-method approach, integrating ethnographic narratives and machine learning analysis, dynamically track the evolution of insider threat motives in response to emerging cybersecurity risks? • *Employing innovative tools to capture dynamic interactions in insider deviant behavior research:* What insights into systemic vulnerabilities emerge from using AI alongside traditional surveys to analyze feedback loops between organizational policies and employee sabotage behaviors? • *Testing an adaptive methodology for ongoing refinement in insider deviant behavior research:* How effectively can an iterative framework, updated with real-time data and employee interviews, identify triggers for insider fraud in organizations?
Impact	**Applied Collaborative Impact**: Researchers should be co-designed with industry stakeholders to ensure practical relevance, prioritize outputs that enhance training, policy, and system design, and establish iterative feedback loops to refine findings in response to real-world input. (Seidel & Watson, 2020)	• *Focusing on co-creation with industry for practical training outcomes in insider deviant behavior research:* How can collaboration with cybersecurity firms shape research questions that lead to actionable training programs for reducing insider phishing vulnerabilities in organizations? • *Prioritizing policy-relevant outputs through stakeholder collaboration in insider deviant behavior research:* What policy recommendations for mitigating insider threats can be derived from a study co-designed with

		organizational stakeholders, ensuring applicability across diverse corporate governance structures? • *Building iterative stakeholder input into system design improvements in insider deviant behavior research:* How can feedback mechanisms involving employees and managers refine research findings on insider risk over time, enhancing the design of secure protocol in organizations?

Limitations

While identifying the limitations in researching IDB and developing a structured and adaptable framework, the process is not without challenges. The action-guiding principles, aims to enhance research depth, ethical responsibility, and practical relevance, however, they themselves face several limitations that must be acknowledged and addressed to ensure their continued effectiveness in guiding IDB research. One significant challenge lies in integrating diverse knowledge from multiple disciplines. The study of IDB in information and cybersecurity benefits from insights drawn from psychology, criminology, sociology, and cybersecurity. However, these disciplines have distinct theoretical foundations, assumptions, and scopes, making it difficult to synthesize them into a cohesive research approach. While interdisciplinary integration enhances understanding, it also introduces complexity that researchers must navigate carefully to avoid contradictions or misinterpretations.

Another limitation is that of accounting for contextual factors in research. Insider threats vary widely depending on organizational culture, industry-specific risks, and geopolitical influences. Consequently, research findings may not always be transferable across different settings. Additionally, obtaining comprehensive and high-quality data remains a persistent challenge due to privacy regulations and security restrictions that limit researchers' access to sensitive information. Without sufficient data, the ability to apply these principles effectively may be hindered, reducing their overall impact. Further, upholding ethical integrity is also a crucial yet challenging aspect of applying the action-guiding principles in IDB research. The use of monitoring tools, behavioral analysis, and AI-driven data collection methods raises ethical concerns, particularly regarding privacy and consent. Balancing security measures with ethical considerations is complex, as invasive monitoring practices can lead to unintended consequences, such as employee distrust or potential misuse of collected data. To ensure responsible research practices, ethical safeguards must be rigorously implemented, and privacy considerations must remain a priority.

Additionally, applying comprehensive methods in IDB research is complicated by the rapidly evolving nature of security threats. Emerging technologies such as deepfakes, AI-driven social engineering, and blockchain misuse present new challenges that were previously less prevalent or detectable. As cyber threats continue to evolve, research methodologies must be dynamic and capable of adapting to new attack vectors and manipulation techniques. Without continuous methodological refinement, research risks becoming outdated, limiting its effectiveness in addressing real-world security concerns. Finally, prioritizing practical impact presents another key challenge. The ever-changing cybersecurity landscape means that threats and vulnerabilities evolve faster than research can sometimes address them. Ensuring that the action-guiding principles remain relevant requires ongoing adaptation, collaboration with industry stakeholders, and mechanisms for real-world testing. If these principles are not periodically revisited and refined, they may lose their applicability, reducing their effectiveness in guiding actionable cybersecurity research and interventions.

Conclusion

This article reported a study that employed a Theoretical Integrative Review (TIR)(Battistone et al., 2023) to closely scrutinize 66 theories applied in information and cybersecurity to identify their limitations regarding their relevance for examining deviant insider behavior. Three of Gregor's (2006) primary goals of theories were adopted - Explanation, Prediction, and Prescription (with the exclusion of one goal, 'Analysis and Description') – to analyze and identify limitations in the theories for their application relating to insider deviance. The current study advances recent work by explaining the theories in comparison to one another, noting overlaps and differences, and accounting for limitations that can be located in the theories' ability to explain, predict, or prescribe deviant insider behavior.

Through our analysis, we identified key theoretical limitations in IDB research and categorized them into thematic groups, leading to the development of action-guiding principles to enhance future studies in this area. These principles consolidate the theoretical limitations into five key perspectives, providing guidelines to address critical challenges such as inconsistencies in research, neglect of influential factors, a narrow focus, difficulties in predicting behaviors, and data and methodological issues.

The guiding principles proposed in this article provide a comprehensive framework for enhancing IDB research, as they are grounded in a careful consideration of existing theories. Future studies can utilize these guidelines to analyze past cases and current organizational settings, offering deeper insights into the properties and antecedents of IDBs.

Disclosure of interest

There are no competing interests to declare.

Declaration of funding

No funding was received.

References

Abrahams, T. O., Ewuga, S. K., Dawodu, S. O., Adegbite, A. O., & Hassan, A. O. (2024). A review of cybersecurity strategies in modern organizations: Examining the evolution and effectiveness of cybersecurity measures for data protection. Computer Science & IT Research Journal, 5(1), 1–25

Agrawal, D., Davis, J., & Singh, K. (2023). Shaping the attitude towards information security-a social influence approach.

Agnew, R. (1985). A revised strain theory of delinquency. *Social Forces*, *64*(1), 151–167.

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.

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

Ajzen, I., & Fishbein, M. (1977). Attitude-behavior relations: A theoretical analysis and review of empirical research. Psychological Bulletin, 84(5), 888.

Alawneh, M., & Abbadi, I. M. (2011). Defining and analyzing insiders and their threats in organizations. 2011IEEE 10th International Conference on Trust, Security and Privacy in Computing and Communications, 785–794.

Alassaf, M., & Alkhalifah, A. (2021). Exploring the influence of direct and indirect factors on information security policy compliance: A systematic literature review. IEEE Access, 9, 162687–162705.

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.

Ali, R. F., Dominic, P., Ali, S. E. A., Rehman, M., & Sohail, A. (2021). Information security behavior and information security policy compliance: A systematic literature review for identifying the transformation process from noncompliance to compliance. Applied Sciences, 11(8), 3383.

Almansoori, A., Al-Emran, M., & Shaalan, K. (2023). Exploring the frontiers of cybersecurity behavior: A systematic review of studies and theories. Applied Sciences, 13(9), 5700.

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.

Alotaibi, M., Furnell, S., & Clarke, N. (2016). Information security policies: A review of challenges and influencing factors. 2016 11th International Conference for Internet Technology and Secured Transactions (ICITST), 352–358

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.

Alzaabi, F. R., & Mehmood, A. (2024). A review of recent advances, challenges, and opportunities in malicious insider threat detection using machine learning methods. IEEE Access, 12, 30907–30927.

Amir, D., & McAuliffe, K. (2020). Cross-cultural, developmental psychology: Integrating approaches and key insights. Evolution and Human Behavior, 41(5), 430–444. https://doi.org/10.1016/j.evolhumbehav.2020.06.006

Ando, H., Cousins, R., & Young, C. (2014). Achieving saturation in thematic analysis: Development and refinement of a codebook. *Comprehensive Psychology*, *3*, 03-CP.

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), 4.

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.

Austin, R. E. (2023). The Interplay of InfoSec Mindfulness and Sanctions on Extra Role Security Behaviors: A Trait Activation Perspective.

Avgerou, C. (2019). Contextual Explanation: Alternative Approaches and Persistent Challenges. *Management Information Systems Quarterly*, *43*(3), 977–1006.

Bakker, A. B., & Demerouti, E. (2007). The job demands-resources model: State of the art. Journal of Managerial Psychology, 22(3), 309–328.

Balozian, P., Burns, A., & Leidner, D. E. (2023). An Adversarial Dance: Toward an Understanding of Insiders' Responses to Organizational Information Security Measures. Journal of the Association for Information Systems, 24(1), 161–221.

Bandara, W., Furtmueller, E., Gorbacheva, E., Miskon, S., & Beekhuyzen, J. (2015). Achieving rigor in literature reviews: Insights from qualitative data analysis and tool-support. *Communications of the Association for Information Systems*, *37*(1), 8.

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

Bandura, A. (1977). Social learning theory. Englewood Cliffs, NJ: 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. (1994). Self-efficacy (Vol. 4).

Balagopal, N., & Mathew, S. K. (2024). Exploring the factors influencing information security policy compliance and violations: A systematic literature review. Computers & Security, 104062.

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.

Bass, B. M., & Avolio, B. J. (1994). Improving organizational effectiveness through transformational leadership. sage.

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

Battistone, M. J., Kemeyou, L., & Varpio, L. (2023). The Theoretical Integrative Review—A Researcher's Guide. Journal of Graduate Medical Education, 15(4), 453–455.

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

Beccaria, C. (1963). On crimes and punishments (H. Paolucci, Trans.). Indianapolis, IN: Bobbs-Merrill.(Original Work Published 1764).

Bialek, W., Nemenman, I., & Tishby, N. (2001). Predictability, complexity, and learning. Neural Computation, 13(11), 2409–2463.

Bernal, G., & Adames, C. (2017). Cultural adaptations: Conceptual, ethical, contextual, and methodological issues for working with ethnocultural and majority-world populations. Prevention Science, 18(6), 681–688.

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.

Bouchama, F., & Kamal, M. (2021). Enhancing cyber threat detection through machine learning-based behavioral modeling of network traffic patterns. International Journal of Business Intelligence and Big Data Analytics, 4(9), 1–9.

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.

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

Brutus, S., Gill, H., & Duniewicz, K. (2010). State of science in industrial and organizational psychology: A review of self-reported limitations. Personnel Psychology, 63(4), 907–936.

Burke, P. J., & Reitzes, D. C. (1991). An identity theory approach to commitment. Social Psychology Quarterly, 239–251.

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, 3930–3940.

Burns, A., Posey, C., & Roberts, T. L. (2021). Insiders' adaptations to security-based demands in the workplace: An examination of security behavioral complexity. Information Systems Frontiers, 23, 343–360.

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.

Burton-Jones, A., McLean, E. R., & Monod, E. (2015). Theoretical perspectives in IS research: From variance and process to conceptual latitude and conceptual fit. European Journal of Information Systems, 24(6), 664–679.

Caplan, R. D. (1987). Person-environment fit theory and organizations: Commensurate dimensions, time perspectives, and mechanisms. Journal of Vocational Behavior, 31(3), 248–267.

Caplan, R. D., & Van Harrison, R. (1993). Person-environment fit theory: Some history, recent developments, and future directions. Journal of Social Issues, 49(4), 253–275.

Carver, C. S., & Scheier, M. F. (1994). Situational coping and coping dispositions in a stressful transaction. Journal of Personality and Social Psychology, 66(1), 184–195. https://doi.org/10.1037/0022-3514.66.1.184

Carver, C. S., Scheier, M. F., & Weintraub, J. K. (1989). Assessing coping strategies: A theoretically based approach. Journal of Personality and Social Psychology, 56(2), 267–283. https://doi.org/10.1037/0022-3514.56.2.267

Cavanaugh, M. A., Boswell, W. R., Roehling, M. V., & Boudreau, J. W. (2000). An empirical examination of self-reported work stress among US managers. Journal of Applied Psychology, 85(1), 65.

Chatterjee, S., Sarker, S., & Valacich, J. S. (2015). The behavioral roots of information systems security: Exploring key factors related to unethical IT use. Journal of Management Information Systems, 31(4), 49–87.

Chen, H., Hai, Y., Tu, L., & Fan, J. (2024). Not all information security-related stresses are equal: The effects of challenge and hindrance stresses on employees' compliance with information security policies. Behaviour & Information Technology, 43(16), 3939–3954.

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.

Chen, L., Xie, Z., Zhen, J., & Dong, K. (2022). The impact of challenge information security stress on information security policy compliance: The mediating roles of emotions. Psychology Research and Behavior Management, 1177–1191.

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.

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.

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, D. (2014). Managing employee security behaviour in organisations: The role of cultural factors and individual values. ICT Systems Security and Privacy Protection: 29th IFIP TC 11 International Conference, SEC 2014, Marrakech, Morocco, June 2-4, 2014. Proceedings 29, 417–430.

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, 283–296.

Cram, W. A., & D'Arcy, J. (2023). Barking Up the Wrong Tree? Reconsidering Policy Compliance as a Dependent Variable within Behavioral Cybersecurity Research.

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. https://doi.org/10.1057/s41303-017-0059-9

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.

Cuganesan, S., Steele, C., & Hart, A. (2018). How senior management and workplace norms influence information security attitudes and self-efficacy. Behaviour & Information Technology, 37(1), 50–65

D'Arcy, J., & Devaraj, S. (2012). Employee misuse of information technology resources: Testing a contemporary deterrence model. Decision Sciences, 43(6), 1091–1124.

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

D'Arcy, J., & Hovav, A. (2005). Deterring information systems misuse: The impact of three security countermeasures. The Fourth Security Conference, Las Vegas, NV.

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.

Davis, F. D. (1989). Perceived usefulness, perceived ease of use, and user acceptance of information technology. MIS Quarterly, 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.

Davis, R., Campbell, R., Hildon, Z., Hobbs, L., & Michie, S. (2015). Theories of behaviour and behaviour change across the social and behavioural sciences: A scoping review. Health Psychology Review, 9(3), 323–344.

Davis, J. H., Schoorman, F. D., & Donaldson, L. (1997). Toward a stewardship theory of management. Academy of Management Review, 22(1), 20–47.

Davis, J. M. (2024). Hardening the 'Human Firewall'Through Security Role Identity Activation: A Social Information Processing Perspective.

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. 21(1). https://doi.org/10.17705/1JAIS.00595

Dhillon, G., Smith, K., & Dissanayaka, I. (2021). Information systems security research agenda: Exploring the gap between research and practice. *The Journal of Strategic Information Systems*, *30*(4), 101693.

Di Stefano, G., Scrima, F., & Parry, E. (2019). The effect of organizational culture on deviant behaviors in the workplace. The International Journal of Human Resource Management, 30(17), 2482–2503.

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.

Dittes, S., Urbach, N., Ahlemann, F., Smolnik, S., & Müller, T. (2015). Why don't you stick to them? Understanding factors influencing and counter-measures to combat deviant behavior towards organizational IT standards. Wirtschaftsinformatik Proceedings 2015. 42. http://aisel.aisnet.org/wi2015?utm_source=aisel.aisnet.org%2Fwi2015%2F42&utm_medium=PDF&utm_campaign=PDFCoverPages

Doney, P. M., & Cannon, J. P. (1997). An examination of the nature of trust in buyer–seller relationships. Journal of Marketing, 61(2), 35–51.

Duary, S., Choudhury, P., Mishra, S., Sharma, V., Rao, D. D., & Aderemi, A. P. (2024). Cybersecurity Threats Detection in Intelligent Networks using Predictive Analytics Approaches. 2024 4th International Conference on Innovative Practices in Technology and Management (ICIPTM), 1–5.

Eagly, A. H., & Chaiken, S. (1993). The psychology of attitudes.

Eisenhardt, K. M. (1985). Control: Organizational and economic approaches. Management Science, 31(2), 134–149.

EPSU. (2019). GDPR_FINAL_EPSU.pdf. https://www.epsu.org/article/epsu-guide-general-data-protection-regulation-gdpr-now-released

Fan, J., & Zhang, P. (2011). Study on e-government information misuse based on General Deterrence Theory. ICSSSM11, 1–6.

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

Feng, G., Zhu, J., Wang, N., & Liang, H. (2019). How paternalistic leadership influences IT security policy compliance: The mediating role of the social bond. Journal of the Association for Information Systems, 20(11), 2.

Fishbein, M. (1979). A theory of reasoned action: Some applications and implications.

Fleming, J., & Zegwaard, K. E. (2018). Methodologies, methods and ethical considerations for conducting research in work-integrated learning. International Journal of Work-Integrated Learning, 19(3), 205–213.

Folger, R., & Cropanzano, R. (2001). Fairness theory: Justice as accountability. Advances in Organizational Justice, 1(1–55), 12.

Fredrickson, B. L. (2001). The role of positive emotions in positive psychology: The broaden-and-build theory of positive emotions. American Psychologist, 56(3), 218.

Fryer, L. K., & Dinsmore, D. L. (2020). The Promise and Pitfalls of Self-report: Development, research design and analysis issues, and multiple methods. Frontline Learning Research.

Georgiadou, A., Mouzakitis, S., Bounas, K., & Askounis, D. (2022). A cyber-security culture framework for assessing organization readiness. Journal of Computer Information Systems, 62(3), 452–462.

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

Goldberg, H., Young, W., Reardon, M., Phillips, B., & others. (2017). Insider Threat Detection in PRODIGAL.

Gottfredson, M. R., & Hirschi, T. (1990). A general theory of crime. In A general theory of crime. Stanford University Press.

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.

Gregor, S. (2006). The nature of theory in information systems. MIS Quarterly, 611–642.

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

Greulich, M., Lins, S., Pienta, D., Thatcher, J. B., & Sunyaev, A. (2024). Exploring contrasting effects of trust in organizational security practices and protective structures on employees' security-related precaution taking. Information Systems Research.

Guhr, N., Lebek, B., & Breitner, M. H. (2019). The impact of leadership on employees' intended information security behaviour: An examination of the full-range leadership theory. Information Systems Journal, 29(2), 340–362.

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

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

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.

Haag, S., Eckhardt, A., & Schwarz, A. (2019). The acceptance of justifications among shadow IT users and nonusers–an empirical analysis. Information & Management, 56(5), 731–741.

Harrington, S. J. (1996). The effect of codes of ethics and personal denial of responsibility on computer abuse judgments and intentions. MIS Quarterly, 257–278.

'Hammond, K. R. (1981). Principles of Organization in Intuitive and Analytical Cognition. https://api.semanticscholar.org/CorpusID:141471194

Hammond, K. R. (1988). Judgement and Decision Making in Dynamic Tasks. Information and Decision Technologies, 14, 3–14.

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. Berkeley. CA: 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.

Hollinger, R. C., & Clark, J. P. (1983). Deterrence in the workplace: Perceived certainty, perceived severity, and employee theft. Social Forces, 62(2), 398–418.

Homans, G. C. (1958). Social behavior as exchange. American Journal of Sociology, 63(6), 597–606.

Horneman, A., Ditmore, B., Motell, C., & Levy, M. (2022). Predicting the Threat: Investigating Insider Threat Psychological Indicators With Deep Learning

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

Hsu, J. S.-C., Hung, Y. W., Hsieh, P.-J., & Chiu, C.-M. (2024). Examining formation and alleviation of information security fatigue by using job demands–resources theory. Information Systems Journal, 34(6), 2132–2172.

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.

Hunker, J., & Probst, C. W. (2011). Insiders and Insider Threats-An Overview of Definitions and Mitigation Techniques. J. Wirel. Mob. Networks Ubiquitous Comput. Dependable Appl., 2(1), 4–27.

Huysmans, P., & De Bruyn, P. (2013). A mixed methods approach to combining behavioral and design research methods in information systems research. ECIS. https://aisel.aisnet.org/ecis2013_cr/29

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.

Ifinedo, P. (2015). Effects of organizational citizenship behavior and social cognitive factors on employees' non-malicious counterproductive computer security behaviors: An empirical analysis.

Ifinedo, P. (2019). Investigating employee engagement in nonmalicious, end-user computing and information security deviant behavior.

Ifinedo, P. (2022). Exploring Personal and Environmental Factors that Can Reduce Nonmalicious Information Security Violations. Information Systems Management, 1–21.

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.

ISO/IEC 27001:2022. (2022). Information security management systems. https://www.iso.org/standard/27001

Jesson, J. K., & Lacey, F. M. (2006). How to do (or not to do) a critical literature review. Pharmacy Education, 6(2), 139–148.

Jeon, S., Son, I., & Han, J. (2023). Understanding employee's emotional reactions to ISSP compliance: Focus on frustration from security requirements. Behaviour & Information Technology, 42(13), 2093–2110.

Jia, S., & Xu, F. (2021). When Extra-Role Behavior Leads to Employee Security Deviance: A Moral Licensing View. AMCIS.

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 &Amp; Security, 130, 103253. https://doi.org/10.1016/j.cose.2023.103253

Jiang, S., & Nehme, A. (2024). Employees' Post–Breach Information Security Policy Non-Compliance: An Organizational Legitimacy Perspective.

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.

Johnston, A., Di Gangi, P. M., Bélanger, F., Crossler, R. E., Siponen, M., Warkentin, M., & Singh, T. (2023). Seeking rhetorical validity in fear appeal research: An application of rhetorical theory. Computers & Security, 125, 103020.

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, R. (1993). Men and Women of the Corporation, 2nd edn, 1977. BasicBooks, New York, NY.

Kanter, R. M. (1977). Men and Women of the Corporation. New York: Basic Book. Inc.

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

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 Berlin Heidelberg. https://doi.org/10.1007/978-3-642-27739-9_1595-1

Kast, F. E., & Rosenzweig, J. E. (1972). General systems theory: Applications for organization and management. Academy of Management Journal, 15(4), 447–465.

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

Kaur, M., van Eeten, M., Janssen, M., Borgolte, K., & Fiebig, T. (2021). Human factors in security research: Lessons learned from 2008-2018. arXiv Preprint arXiv:2103.13287.

Kearns, G. S., & Lederer, A. L. (2004). The impact of industry contextual factors on IT focus and the use of IT for competitive advantage. *Information & Management*, *41*(7), 899–919.

Keele, S. (2007). Guidelines for performing systematic literature reviews in software engineering. Technical report, ver. 2.3 ebse technical report. ebse.

Kelman, H. C. (1958). Compliance, identification, and internalization three processes of attitude change. Journal of Conflict Resolution, 2(1), 51–60.

Krieg, A. (2020). A contextual behavioral account of culture: Example implementation of a functional behavioral approach to the study of cultural differences in social anxiety. Frontiers in Psychology, 11, 418.

Khan, N. F., Yaqoob, A., Khan, M. S., & Ikram, N. (2022). The cybersecurity behavioral research: A tertiary study. Computers & Security, 120, 102826.

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

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.

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

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.

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

Langer, E. J. (1989). Minding matters: The consequences of mindlessness–mindfulness. In Advances in experimental social psychology (Vol. 22, pp. 137–173). Elsevier.

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.

Leidner, D. E., & Gregory, R. W. (2024). About Theory and Theorizing. Journal of the Association for Information Systems, 25(3), 501–521.

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., & others. (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. "Andy." (2019). What Users Do besides Problem-Focused Coping When Facing IT Security Threats. MIS Quarterly, 43(2), 373-A18.

Lin, C., & Kunnathur, A. S. (2013). Toward developing a theory of end user information security competence.

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.

Lowry, P. B., Moody, G. D., Parameswaran, S., & Brown, N. J. (2023). Examining the differential effectiveness of fear appeals in information security management using two-stage meta-analysis. Journal of Management Information Systems, 40(4), 1099–1138.

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.

Mady, A., Gupta, S., & Warkentin, M. (2023). The effects of knowledge mechanisms on employees' information security threat construal. Information Systems Journal, 33(4), 790–841.

Mackey, J. D., McAllister, C. P., Ellen III, B. P., & Carson, J. E. (2021). A meta-analysis of interpersonal and organizational workplace deviance research. Journal of Management, 47(3), 597–622.

Marasi, S., Bennett, R. J., & Budden, H. (2018). The structure of an organization: Does it influence workplace deviance and Its' dimensions? And to what extent? Journal of Managerial Issues, 8–27.

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, 3518–3526.

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

Mattson, T., Aurigemma, S., & Ren, J. (2023). Positively fearful: Activating the individual's HERO within to explain volitional security technology adoption. Journal of the Association for Information Systems, 24(3), 664–699.

Mayer, R. (1995). An Integrative Model of Organizational Trust. Academy of Management Review.

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

McKnight, Z. C. S., Jang, K., & Jiang, S. (2024). Will Employment Retention Lead to Security Vulnerabilities?

Melville, N. P. (2010). Information Systems Innovation for Environmental Sustainability. MIS Quarterly, 34(1), 1–21.

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. London.

Mingers, J., & Walsham, G. (2010). Toward ethical information systems: The contribution of discourse ethics. *MIS Quarterly*, 833–854

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

Monin, B., & Miller, D. T. (2001). Moral credentials and the expression of prejudice. Journal of Personality and Social Psychology, 81(1), 33.

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.

Mueller, B., & Urbach, N. (2017). Understanding the why, what, and how of theories in IS research. Communications of the Association for Information Systems, 41, 349–388.

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.

Nehme, A., & George, J. (2020). Taking it out on IT: A Mechanistic Model of Abusive Supervision and Computer Abuse.

Nehme, A., Warkentin, M., Jang, K., & Kim, S. (2022). Beyond Rational Information Security Decisions: An Alternate View.

Nicho, M., & Kamoun, F. (2014). Multiple case study approach to identify aggravating variables of insider threats in information systems. Communications of the Association for Information Systems, 35(1), 18.

Nieuwenhuijsen, K., Bruinvels, D., & Frings-Dresen, M. (2010). Psychosocial work environment and stress-related disorders, a systematic review. Occupational Medicine, 60(4), 277–286.

Ogbanufe, O. (2018). The Mediating Role of Psychological Ownership in Increasing Information Security Stewardship Behaviors.

Organ, D. W. (1988). Organizational citizenship behavior: The good soldier syndrome. Lexington books/DC 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.

Ouchi, W. G. (1979). A conceptual framework for the design of organizational control mechanisms. Management Science, 25(9), 833–848.

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

Paré, G., Trudel, M.-C., Jaana, M., & Kitsiou, S. (2015). Synthesizing information systems knowledge: A typology of literature reviews. Information & Management, 52(2), 183–199.

Parker, S. K., Bindl, U. K., & Strauss, K. (2010). Making things happen: A model of proactive motivation. Journal of Management, 36(4), 827–856.

Parker-Follett, M., & Graham, P. (1933). The essentials of leadership. Classics in Management, American Management Association, Washington, DC, 295–308.

Paternoster, R., & Simpson, S. (1996). Sanction threats and appeals to morality: Testing a rational choice model of corporate crime. Law and Society Review, 549–583.

Pollini, A., Callari, T. C., Tedeschi, A., Ruscio, D., Save, L., Chiarugi, F., & Guerri, D. (2022). Leveraging human factors in cybersecurity: An integrated methodological approach. Cognition, Technology & Work, 24(2), 371–390.

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. https://doi.org/10.1080/07421222.2015.1138374.

Posey, C., Bennett, B., Roberts, T., & Lowry, P. B. (2011). When computer monitoring backfires: Invasion of privacy and organizational injustice as precursors to computer abuse. Journal of Information System Security, 7(1), 24-47.

Rai, A. (2018). *Editor's comments: Beyond outdated labels: The blending of IS research traditions*.

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.

Ramakrishnan, T., Hite, D. M., Schuessler, J. H., & Prybutok, V. (2022). Work ethic and information security behavior. Information & Computer Security, 30(3), 364–381.

Rawls, J. (1971). A theory of justice.

Recker, J., Indulska, M., Green, P., Burton-Jones, A., & Weber, R. (2019). Information systems as representations: A review of the theory and evidence. *Journal of the Association for Information Systems*, *20*(6), 5.

Renaud, K., & Zimmermann, V. (2018). Ethical guidelines for nudging in information security & privacy. International Journal of Human-Computer Studies, 120, 22–35.

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, 153–176.

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.

Rousseau, D. M., Sitkin, S. B., Burt, R. S., & Camerer, C. (1998). Not so different after all: A cross-discipline view of trust. Academy of Management Review, 23(3), 393–404.

Rowe, F. (2014). What literature review is not: Diversity, boundaries and recommendations. *European Journal of Information Systems*, *23*(3), 241–255.

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.

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.

Schneier, B. (2015). Secrets and lies: Digital security in a networked world. John Wiley & Sons.

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), 1–7.

Schwartz, S. (2006). A theory of cultural value orientations: Explication and applications. Comparative Sociology, 5(2–3), 137–182.

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.

Seidel, S., & Watson, R. T. (2020). Integrating explanatory/predictive and prescriptive science in information systems research. *Communications of the Association for Information Systems*, *47*(1), 49.

Shameli-Sendi, A., Aghababaei-Barzegar, R., & Cheriet, M. (2016). Taxonomy of information security risk assessment (ISRA). Computers & Security, 57, 14–30.

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

Stewart, K. J. (2003). Trust Transfer on the World Wide Web. Organization Science, 14(1), 5–17.

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.

Siponen, M., Rönkkö, M., Fufan, L., Haag, S., & Laatikainen, G. (2024). Protection Motivation Theory in Information Security Behavior Research: Reconsidering the Fundamentals. Communications of the Association for Information Systems, 53, 1136-1165.

Siponen, M., Soliman, W., & Vance, A. (2022). Common Misunderstandings of Deterrence Theory in Information Systems Research and Future Research Directions. the DATABASE for Advances in Information Systems, 53(1), 25–60.

Siponen, M. T., & Oinas-Kukkonen, H. (2007). A review of information security issues and respective research contributions. *ACM SIGMIS Database: The DATABASE for Advances in Information Systems*, *38*(1), 60–80.

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

Snyder, H. (2019). Literature review as a research methodology: An overview and guidelines. Journal of Business Research, 104, 333–339.

Snyman, D., & Kruger, H. (2019). Behavioural threshold analysis: Methodological and practical considerations for applications in information security. *Behaviour & Information Technology*, *38*(11), 1088–1106

Soares, A. M., Farhangmehr, M., & Shoham, A. (2007). Hofstede's dimensions of culture in international marketing studies. Journal of Business Research, 60(3), 277–284.

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.

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

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

Suchman, M. C. (1995). Managing legitimacy: Strategic and institutional approaches. Academy of Management Review, 20(3), 571–610.

Sutinen, J. G., & Kuperan, K. (1999). A socio-economic theory of regulatory compliance. International Journal of Social Economics, 26(1/2/3), 174–193.

Sykes, G. M., & Matza, D. (2017). Techniques of neutralization: A theory of delinquency. In Delinquency and Drift Revisited, Volume 21 (pp. 33–41). Routledge.

Tett, R. P., & Burnett, D. D. (2003). A personality trait-based interactionist model of job performance. Journal of Applied Psychology, 88(3), 500.

Tett, R. P., Simonet, D. V., Walser, B., & Brown, C. (2013). Trait activation theory: Applications, developments, and implications for person–workplace fit. In Handbook of personality at work (pp. 71–100). Routledge.

Tett, R. P., Toich, M. J., & Ozkum, S. B. (2021). Trait activation theory: A review of the literature and applications to five lines of personality dynamics research. Annual Review of Organizational Psychology and Organizational Behavior, 8(1), 199–233.

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. 24(6). https://doi.org/10.1016/J.COSE.2005.05.002

Torres, C. I., & Crossler, R. E. (2024). Promoting security behaviors in remote work environments: Personal values shaping information security policy compliance. Information Systems Research.

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/4

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), 1–9.

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.

Trope, Y., & Liberman, N. (2010). Construal-level theory of psychological distance. Psychological Review, 117(2), 440.

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. R. (1990). Why people obey the law. Yale University.

Tyler, T. R. (2004). Promoting employee policy adherence and rule following in work settings-The value of self-regulatory approaches. Brook. L. Rev., 70, 1287.

Tyler, T. R. (2009). Self-regulatory approaches to white-collar crime: The importance of legitimacy and procedural justice. In The criminology of white-collar crime (pp. 195–216). Springer.

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

Vroom, V. H. (2005). On the origins of expectancy theory. Great Minds in Management: The Process of Theory Development, 239–258.

Wall, D. S. (2017). Crime, security and information communication technologies: The changing cybersecurity threat landscape and its implications for regulation and policing. Security and Information Communication Technologies: The Changing Cybersecurity Threat Landscape and Its Implications for Regulation and Policing (July 20, 2017).

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.

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

Weber, M. (2016). The types of legitimate domination. In Social theory re-wired (pp. 270–286). Routledge.

Webster, J., & Watson, R. T. (2002). Analyzing the past to prepare for the future: Writing a literature review. MIS Quarterly, xiii–xxiii.

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. Analytical Sociology, 71–94.

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., & Warkentin, M. (2013). Beyond deterrence: An expanded view of employee computer abuse. MIS Quarterly, 1–20.

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 (JAIS), 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., Hsu, C., Wang, T., & Lowry, P. B. (2024). The antecedents of employees' proactive information security behaviour: The perspective of proactive motivation. Information Systems Journal, 34(4), 1144–1174.

Xu, Z., & Guo, K. (2019). It ain't my business: A coping perspective on employee effortful security behavior. Journal of Enterprise Information Management, 32(5), 824–842.

Xue, B., Warkentin, M., Mutchler, L. A., & Balozian, P. (2023). Self-efficacy in information security: A replication study. Journal of Computer Information Systems, 63(1), 1–10.

Yayla, A. (2011). Controlling insider threats with information security policies.

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.

Yazdanmehr, A., Wang, J., & Yang, Z. (2020). Peers matter: The moderating role of social influence on information security policy compliance. Information Systems Journal, 30(5), 791–844.

Yin, Y., Hsu, C., & Zhou, Z. (2024). Understanding employees' responses to information security management practices: A person-environment fit perspective. Behaviour & Information Technology, 43(12), 2987–3009.

Zhao, W., Johnston, A., & Siponen, M. (2024). Intuition or Analysis? Investigation of Employees' Cognitive Mode of Information Security Policy Compliance.

Appendix A: Explanation Limitations

Theory	Description of Limitations
Fear Appeals (Rogers, 1983; Rogers & Deckner, 1975)	1. Contradictory or Inconsistent findings 2. Lack of consideration for how personality and cultural factors influence reactions to fear appeals.
Rational Choice Theory (Hogarth & Reder, 1987)	1. Bounded rationality 2. Recontextualization challenges 3. Inconsistent research findings 4. Complex Causal Relationships
Deterrence (Beccaria, 1963; Gibbs, 1968)	1. Inconsistent research results 2. It does not cover all factors affecting deviant behaviors in IS 3. Does not directly address the use of justification for criminal behavior.
Fraud Triangle (Albrecht et al., 1984, 2008)	1. Single factor focus 2. Root cause analysis
Routine Activity (Cohen & Felson, 1979)	1. Concerns about generalizability, 2. Traditional data collection methods may not capture nuanced behaviors
Situational Action (Wikström, 2014; Wikström et al., 2017)	1. Limited range of situations examined
Expectancy (Vroom, 2005)	1. The challenge of understanding the various and potentially conflicting factors that influence individual behaviors
Moral Disengagement (Bandura, 1999)	1. The limited understanding and explaining severe security incidents are due to unclear insights.
Social Cognitive (Bandura, 1988)	1. Limitations of Self-Reporting Data: It is not accurate and reliable, affecting the explanation of the phenomena. 2. Limitation in explaining Context-Influenced Behaviors
Neutralization (Gresham & David, 1957; Sykes & Matza, 2017)	1. The complexity of neutralization as a construct requires careful measurement and analysis. 2. Complexity of situational factors 3. Neutralization effectiveness varies based on organizational norms,
Coping Theory (Lazarus & Folkman, 1984)	1. Limitations related to the accuracy and reliability of data collected through self-reporting, affecting the explanation of phenomena 2. Limitations in explaining behaviors due to lack of observable behavior 3. The difficulty in understanding and analyzing emotional reactions due to their complex nature

Organizational Justice (Greenberg, 1987)	1. Complexity in accurately measuring perceptions of injustice. 2. Difficulty in disentangling procedural, distributive, and interactional forms of injustice.
Justice (Rawls, 1971)	1. Limitations in explaining behaviors accurately due to potential biases and inaccuracies in self-reported data
Appraisal (Dewe, 1991; Lazarus & Folkman, 1984; Scherer et al., 2001)	1. Difficulty in explaining how individuals assess and interpret situations due to the complex nature of cognitive appraisals. 2. The challenge in explaining behaviors is because of the wide variability in how different individuals respond emotionally. 3. Difficulty in understanding and analyzing emotions due to their intricate and multifaceted nature. 4. The challenge in explaining behaviors due to reactions being heavily influenced by specific contexts.
Transactional Model of Stress (Lazarus & Folkman, 1984)	1. Limitations in explaining behaviors due to the complex and varied demands of Information Security Policies (ISP)
Affective Events (Weiss & Cropanzano, 1996)	1. Limitations in explaining behaviors due to the intricate and varied nature of emotional reactions 2. Difficulty in explaining behaviors because emotions and their effects can vary over time and episodes
Protection Motivation (Rogers, 1975; Rogers & Prentice-Dunn, 1997)	1. Inconsistent empirical findings 2. The challenge in explaining behaviors because of variations across different cultural and contextual settings 3. Limitation of focusing mainly on individual cognition, potentially neglecting other important factors
Reasoned Action (Fishbein, 1979)	1. The limitation that individuals may not always act rationally or systematically process information when making decisions 2. The challenge in explaining behaviors by not considering the impact of external factors like organizational culture and peer influence. 3. Limitations in explaining security behaviors by focusing mainly on intentional actions and neglecting habitual or automatic behaviors
Cognitive Moral Development (Kohlberg, 1963, 1971)	1. The challenge in explaining moral judgments due to their variability across different contexts, requiring multiple scenarios for accurate analysis. 2. Limitations in understanding behavior as individuals may not view security policy non-compliance as a moral issue
Motivational Types of Values (Schwartz, 1992)	1. Understanding and explaining why values may not always lead to corresponding behaviors in complex settings is challenging.
Reactance (Brehm & Brehm, 2013)	1. The challenge in understanding and explaining the nuanced and multifaceted nature of psychological reactance 2. Difficulty in explaining trust as it is a dynamic and evolving construct that changes over time
Social Information Processing (Salancik & Pfeffer, 1978)	1. The challenge in understanding and explaining the nuanced and multifaceted nature of social interactions 2. Difficulty in explaining social influence as it is a dynamic and evolving construct that changes over time.
Dispositional and Situational (Digman, 1997)	1. The challenge in understanding and explaining the intricate and multifaceted nature of interactions between variables or individuals 2. Difficulty in explaining how cognitive processes develop and progress over time.
High Performance and Work Systems (Boxall & Macky, 2009)	1. Challenges in understanding and explaining phenomena due to a lack of detailed or specific information 2. The limitation in explaining behaviors primarily through extrinsic factors, potentially neglecting intrinsic motivations.

Structural Empowerment (R. Kanter, 1993; R. M. Kanter, 1977, 2008)	1. The challenge in understanding and explaining behaviors due to unclear or poorly defined roles.
Fairness (Folger & Cropanzano, 2001)	1. The challenge in understanding and explaining behaviors due to the subjective nature of individual perceptions. 2. The difficulty in explaining how blame is assigned due to its complex and multifaceted nature. 3. The difficulty in understanding trust as it evolves and changes over time.
Planned Behavior (Ajzen, 1991)	1. The challenge in understanding and explaining specific behaviors due to the generic nature of the theory. 2. Difficulty in explaining behaviors by not considering the role of emotions and unconscious biases
Boundary Management (Ashforth et al., 2000)	1. The challenge in understanding and explaining behaviors due to the significant influence of emotions on boundary permeability.
Framework of Emotions (Beaudry & Pinsonneault, 2010)	1. Challenges in understanding and explaining behaviors due to emotions' complicated and multifaceted nature.
Self-Determination (Ryan & Deci, 2000)	1. Challenge in understanding and explaining behaviors by focusing mainly on individual motivations and neglecting broader organizational and contextual factors. 2. Difficulty in explaining behaviors due to a potential misalignment between intrinsic motivation and the extrinsic nature of many security compliance measures.
Agency (Milgram, 1963, 1974)	1. The challenge in understanding and explaining behaviors due to the potential misalignment between the assumptions of principal-agent models and commonly held ethical values
Organizational Citizenship (Katz, 1964; Organ, 1988, 2014)	1. The challenge in understanding and explaining behaviors due to a limited range of constructs considered in the research.
Organizational Control (Eisenhardt, 1985; Ouchi, 1979)	1. The challenge in understanding and explaining behaviors due to potential issues in how constructs are represented and defined.
Hofstede's Cultural Dimensions (Hofstede, 1984; Hofstede & McCrae, 2004)	1. Challenges in understanding and explaining behaviors due to the influence of specific cultural contexts may limit broader applicability.
Social Control (Agnew, 1991)	1. The challenge in understanding and explaining behaviors due to a narrow conceptualization of insiders. 2. Difficulty in explaining security behaviors accurately without considering individual characteristics. 3. Limitation due to an overemphasis on organizational trust, potentially neglecting other relevant factors.
Social Action (Hirschi, 1969, 2017; Weber, 1991)	1. The challenge in understanding and explaining phenomena due to insufficient detail or depth in the explanations provided.
Value Based Compliance (Karlsson & Hedström, 2019)	1. The challenge in understanding and explaining phenomena due to insufficient detail or depth in the explanations provided.

Activity (Kuutti, 1996)	1. Challenges in understanding and explaining behaviors due to the intricate and multifaceted nature of interactions between variables or individuals. 2. Difficulty in explaining behaviors accurately due to the constantly changing and evolving nature of work environments.
Technology Acceptance Model (F. D. Davis, 1989; F. D. Davis et al., 1989)	1. Challenges in understanding and explaining security behaviors due to the multifaceted nature of psychological acceptability and the influence of organizational culture and policies.
Goal Framing' (Lindenberg & Steg, 2007)	1. Challenges in understanding and explaining behaviors due to the complex and multifaceted nature of different scenarios.
General Strain Theory (Agnew, 1985, 1992)	1. Challenges in understanding and explaining behaviors due to a narrow focus on specific strains, potentially overlooking other relevant factors.
Prospect (Kahneman, 1979; Kahneman & Tversky, 2013)	1. Challenges understanding and explaining security behaviors due to an overly broad focus that misses detailed, nuanced factors.
Accountability (Tetlock, 1983)	1. Challenge in understanding and explaining behaviors due to the influence of participants' maturity on their intentions
Cognitive Evaluation (Boal & Cummings, 1981)	1. Challenge in understanding and explaining behaviors due to the limited focus on motivations, neglecting social and organizational factors.
Self-Efficacy (Bandura, 1977; Bandura & Wessels, 1994)	1. Challenges in understanding and explaining behaviors due to focusing too much on individual responsibility, potentially neglecting other influential factors.
Technology Threats Avoidance (Liang et al., 2010)	1. Challenges understanding and explaining behaviors due to the constraints and variability specific to certain contexts.
Opportunity Structure for Crime (Dijk, 1994)	1. Challenge in understanding and explaining behaviors due to the intricate and multifaceted nature of interactions between variables or individuals. 2. Limitation of focusing on specific types of crime, which may not fully capture broader or related issues.
Trust Transfer (Doney & Cannon, 1997; Stewart, 2003)	1. Gaps in fully capturing the complexities of behavior transitions and compliance intentions. That is Trust Transfer Theory does not fully explain how trust impacts cognitive and emotional processes driving transitions from compliance intentions to actual behaviors in dynamic security contexts
Attitude (Ajzen & Fishbein, 1977)	1. Attitude Theory explains behavior as a function of attitudes, but it falls short in addressing the nuanced transitions between intentions and actual compliance behavior, particularly in complex or changing security contexts.
Social Bond (SBT) (Hirschi, 1969)	1. The cultural context may influence the strength and nature of social bonds, limiting the explanatory applicability of the findings to other cultural settings.
Paternalistic Leadership (Parker-Follett & Graham, 1933; Weber, 2016)	1. Paternalistic leadership may manifest differently across cultures, limiting the explanatory scope of the study and its ability to generalize findings to diverse cultural settings. 2. By concentrating on authoritarian, benevolent, and moral leadership styles, the study overlooks other leadership approaches that might also influence ISP compliance, restricting the comprehensive understanding of leadership dynamics.

The Composite Behavior Model (CBM) (Eagly & Chaiken, 1993)	1. The use of four specific security scenarios provides limited explanatory breadth, as it does not account for the full spectrum of security violations, potentially omitting factors that influence participant responses and compliance behaviors.
Beliefs-Actions-Outcomes (BAO) (Melville, 2010)	1. The BAO theory, developed for environmental sustainability, may not fully explain nuanced behaviors and beliefs specific to the IS security domain. 2. By focusing on the belief-action-outcome cycle, the theory oversimplifies security behaviors, potentially missing factors like emotional responses or organizational dynamics that influence decision-making.
The motive–control (MoCo) theory of Insider Computer Abuse (ICA) (Burns et al., 2023)	1. As a middle-range theory, MoCo operates within specific conceptual and contextual boundaries, limiting its ability to provide a comprehensive explanation of all scenarios involving insider computer abuse (ICA). 2. The emphasis on expressive and instrumental motives and intrinsic and extrinsic controls restricts the theory's explanatory breadth, potentially overlooking other influential factors driving ICA.
Self-control theory /General Theory of Crime (Gottfredson & Hirschi, 1990a, 1990b)	1. The theory's emphasis on individual differences in self-regulation limits its ability to explain how situational or contextual factors influence insider computer abuse (ICA) 2. The lack of attention to organizational or environmental contexts hinders a comprehensive understanding of the factors impacting decision-making regarding ICA.
Broaden-and-build (BBT) (Fredrickson, 2001)	1. Self-reported data may not accurately reflect actual security behaviors, limiting the explanatory depth of how emotions influence actions in real-world settings. 2. The findings, based on a specific sample, may not capture the diverse emotional and cultural contexts of different organizations, restricting the explanation of broader patterns in security behaviors.
Trust (Mayer, 1995; Rousseau et al., 1998)	1. The tendency to oversimplify trust as solely producing positive outcomes restricts a nuanced understanding of the dark-side effects of trust, such as overreliance or misplaced trust, and their implications for security behaviors.
Mindfulness (Langer, 1989)	1. By focusing narrowly on the mediating role of mindfulness between trust and precaution-taking behaviors, research may be limited in its explanatory scope, potentially overlooking other relevant dimensions or effects of mindfulness in organizational security. 2. Applying mindfulness theory specifically to information security may restrict its ability to explain behaviors in broader organizational contexts or different domains.
Full-range leadership (Bass & Avolio, 1994)	1. The theory's focus on transformational, transactional, and passive/avoidant leadership styles may not account for other leadership behaviors or nuances that influence security intentions, limiting its explanatory depth.
Job demands–resources (Bakker & Demerouti, 2007)	1. The JD-R model may not fully explain the dynamic and rapidly changing nature of information security contexts, where demands and resources fluctuate significantly. 2. The model's emphasis on psychological outcomes like burnout and engagement limits its ability to explain specific security-related behaviors, such as compliance or non-compliance with security policies. 3. The framework does not fully account for individual differences in perceptions of demands and resources, reducing its explanatory depth across diverse organizational settings and cultures.
Proactive motivation (ProMT) (Parker et al., 2010)	1. The study examines a limited range of variables, potentially overlooking other influential factors that could enhance understanding of proactive ISBs (Information Security Behaviors). 2. The application of the theory was specific to a particular organizational context, which limits the explanatory scope across other settings or industries.
The self-regulatory approach (S-R) (Sutinen & Kuperan, 1999; Tyler, 1990)	1. The S-R approach may fail to explain behavior when employees prioritize maintaining social relationships over adhering to internal values and norms, reducing its effectiveness in such contexts. 2. The approach struggles to account for environments with strong rules-oriented ethical climates, where employees may prioritize personal and social norms over organizational directives, diminishing its explanatory power.

The command-and-control approach (C-C) (Tyler, 1990, 2004, 2009)	1. The C-C approach may fail to explain why overemphasis on external deterrents like monitoring and sanctions can lead to reduced compliance, as employees perceive these measures negatively. 2. The approach struggles to explain behavior in strong rules-oriented ethical climates, where employees prioritize personal and social norms over adherence to organizational directives. 3. The C-C approach is limited in explaining compliance behavior when employees prioritize social relationships over organizational directives due to high susceptibility to interpersonal influence.
Construal-level (CLT) (Trope & Liberman, 2010)	1. Limited explanation of how psychological distance interacts with other factors to shape perception and behavior. 2. Gaps in explaining how these mechanisms influence individuals' construals across different contexts.
Person-Environment (P-E) fit. (Caplan, 1987; Caplan & Van Harrison, 1993)	1. The limited items used for research practicality result in an incomplete explanation of organizational information security (ISec) management, as key aspects may be overlooked.
Challenge-hindrance stressor (Cavanaugh et al., 2000)	1. The focus on challenge stressors overlooks the explanatory role of hindrance stressors, which may also significantly affect emotions and compliance behavior. 2. Limited explanation of how stressors influence compliance behaviors in other cultural or organizational contexts.

Appendix B: Prediction Limitations

Theory	**Description of Limitations**
Fear Appeals (Rogers, 1983; Rogers & Deckner, 1975)	1. Lack of focus on fear control processes. 2. Short-term research focus
Rational Choice Theory (Hogarth & Reder, 1987)	1. Cultural and contextual differences 2. Complexity of modeling criminal behavior
Deterrence (Beccaria, 1963; Gibbs, 1968)	1. Uneven influence of punishment 2. Limited predictive power due to evolving criminal methods 3. Challenges in modeling sanction effects 4. Failure to significantly reduce criminal intention or behavior
Fraud Triangle (Albrecht et al., 1984, 2008)	1. Limited range of factors examined 2. Refinement for IS violations
Routine Activity (Cohen & Felson, 1979)	1. Integration with other theories requires diverse subjects.
Situational Action (Wikström, 2014; Wikström et al., 2017)	1. Does not fully capture complexity and diversity of situational influences
Expectancy (Vroom, 2005)	1. Difficulties in predicting how to effectively motivate secure behaviors due to their complex nature. 2. Challenge in predicting behavior, emphasizing the gap between knowledge and action.

Moral Disengagement (Bandura, 1999)	1. Challenges in predicting and applying findings broadly across various contexts and types of security incidents
Social Cognitive (Bandura, 1988)	1. Challenge in predicting and applying findings broadly across different contexts due to limited generalizability 2. Limitation in predicting long-term or causal relationships due to the reliance on cross-sectional study designs
Neutralization (Gresham & David, 1957; Sykes & Matza, 2017)	1. Limitations in predicting outcomes due to the specific conditions under which a theory or model is applicable 2. Challenge in predicting and generalizing findings due to non-representative sample sizes. 3. the need for better prediction by considering the specific contexts in which behaviors occur
Coping Theory (Lazarus & Folkman, 1984)	1. The challenge in predicting outcomes due to the lack of consideration for the timing and sequence of events or behaviors. 2. Limitations in predicting the effectiveness of different coping strategies (emotion-focused versus problem-focused) in various situations.
Organizational Justice (Greenberg, 1987)	1. Limitation in predicting outcomes due to the potential mediating or moderating effects of other psychological processes. 2. Further research to improve the prediction of outcomes based on context-specific perceptions of injustice
Justice (Rawls, 1971)	1. Difficulty in predicting true compliance and violations due to challenges in measuring actual behavior accurately
Appraisal (Dewe, 1991; Lazarus & Folkman, 1984; Scherer et al., 2001)	1. Challenge in predicting outcomes due to the interaction of various factors influencing behavior. 2. The need to account for conditions that might moderate the relationship between variables when predicting behaviors 3. Difficulty in accurately predicting behaviors due to the complex interplay of cognitive and emotional factors.
Transactional Model of Stress (Lazarus & Folkman, 1984)	1. Challenge in predicting outcomes over different time horizons, distinguishing between immediate and lasting effects 2. Difficulty in accurately predicting specific behavioral outcomes as a result of ISP demands or interventions
Affective Events (Weiss & Cropanzano, 1996)	1. Challenge in predicting outcomes due to the scarcity of empirical studies examining the role of emotions in security compliance 2. Difficulty in predicting the effects of onlookers due to the limited application of Affective Events Theory (AET) in security compliance 3. Need for better predictive models that account for the full complexity of decision-making in security compliance.
Protection Motivation (Rogers, 1975; Rogers & Prentice-Dunn, 1997)	1. Challenge in predicting outcomes due to inconsistent or unreliable predictive strength of models 2. Difficulty in predicting behaviors and outcomes due to the constantly changing nature of security threats 3. The need for better prediction models that consider the impact of habitual behaviors on security compliance 4. Challenge in predicting the role of fear in influencing security behaviors due to incomplete understanding.
Reasoned Action (Fishbein, 1979)	1. Challenge in predicting outcomes due to difficulties in establishing clear causal relationships. 2. Challenge in predicting behaviors across different cultures and contexts due to limited generalizability 3. Difficulty in predicting outcomes accurately due to potentially inadequate or unrealistic scenario representations.

Cognitive Moral Development (Kohlberg, 1963, 1971)	1. The challenge in predicting behavior accurately due to the reliance on a single scenario, which may not capture the complexity of real-life situations.
Motivational Types of Values (Schwartz, 1992)	1. Challenge in predicting behavior consistently due to the variability of scenarios and influencing factors. 2. Difficulty in predicting accurate behaviors due to potential biases in self-reported data.
Reactance (Brehm & Brehm, 2013)	1. The challenge in predicting outcomes accurately due to difficulties in measuring relevant variables and constructs. 2. The difficulty in predicting behaviors due to the influence of varying contextual factors.
Social Information Processing (Salancik & Pfeffer, 1978)	1. Challenge in predicting outcomes accurately due to difficulties in measuring relevant variables and constructs. 2. Difficulty in predicting behaviors due to the influence of varying contextual factors.
Dispositional and Situational (Digman, 1997)	1. Challenge in predicting outcomes due to variations in individual characteristics and behaviors. 2. Difficulty in predicting and applying findings broadly across different contexts and populations due to limited generalizability.
High Performance and Work Systems (Boxall & Macky, 2009)	1. The challenge in predicting outcomes accurately across different cultural contexts due to variability in cultural influences. 2. Difficulty in predicting accurate outcomes due to issues with measuring relevant variables and constructs effectively
Structural Empowerment (R. Kanter, 1993; R. M. Kanter, 1977, 2008)	1. Challenge in predicting long-term or causal relationships due to reliance on cross-sectional study designs.
Fairness (Folger & Cropanzano, 2001)	1. Challenge in predicting outcomes accurately across different cultural contexts due to variability in cultural influences.
Planned Behavior (Ajzen, 1991)	1. Challenge in predicting the effectiveness of ethics training or punishment without understanding the underlying motivational factors. 2. Difficulty in predicting outcomes due to the varying impact of self-control on different types of interventions. 3. Challenge in predicting accurate behaviors due to potential biases in self-reported data. 4. Limitation in predicting behaviors due to the static nature of TPB, which may not account for changing threats and responses.
Boundary Management (Ashforth et al., 2000)	1. Challenge in predicting behaviors accurately due to the ever-changing nature of social media platforms and the overlapping of personal and professional boundaries.
Framework of Emotions (Beaudry & Pinsonneault, 2010)	1. Challenge in predicting behaviors accurately because individuals may experience multiple, simultaneous emotions, resulting in diverse and hard-to-generalize responses.

Self-Determination (Ryan & Deci, 2000)	1. Challenge in predicting compliance behavior due to inconsistent empirical findings on the influence of perceived severity and probability of security breaches. 2. Difficulty in predicting behaviors due to the potential misalignment between Self-Determination Theory (SDT) and the external pressures and obligations driving security behavior.
Agency (Milgram, 1963, 1974)	1. Challenge in predicting and ensuring compliance with IT security behaviors due to the impracticality and high costs of monitoring, as well as differing security perspectives among users.
Organizational Citizenship (Katz, 1964; Organ, 1988, 2014)	1. Challenge in predicting outcomes broadly due to limited applicability of findings across different contexts and populations. 2. Difficulty in predicting long-term or causal relationships due to reliance on cross-sectional data.
Organizational Control (Eisenhardt, 1985; Ouchi, 1979)	1. Challenge in predicting outcomes accurately due to an overemphasis on formal control mechanisms, potentially neglecting other influential factors.
Hofstede's Cultural Dimensions (Hofstede, 1984; Hofstede & McCrae, 2004)	1. Challenge in predicting outcomes broadly due to limited applicability of findings across different contexts and populations. Lack of secondary information. 2. Difficulty in predicting outcomes accurately due to limited sample sizes and lack of diversity, which may not represent the broader population. 3. Challenge in predicting behaviors accurately due to potential biases and inaccuracies in self-reported data.
Social Control (Agnew, 1991)	1. Challenge in predicting outcomes accurately due to limitations in the sample size and diversity, which may not represent the broader population. 2. Difficulty in predicting behaviors accurately without considering all relevant factors. 3. Challenge in predicting security behaviors due to insufficient consideration of human aspects and individual differences.
Social Action (Hirschi, 1969, 2017; Weber, 1991)	1. Challenge in predicting outcomes accurately due to constraints and variability in specific contexts.
Value Based Compliance (Karlsson & Hedström, 2019)	1. Challenge in predicting outcomes accurately due to constraints and variability in specific contexts.
Activity (Kuutti, 1996)	1. Challenge in predicting outcomes broadly due to limited applicability of findings across different contexts and populations.
Technology Acceptance Model (F. D. Davis, 1989; F. D. Davis et al., 1989)	1. Challenge in predicting technology acceptance accurately due to an overemphasis on perceived ease of use (PEOU) and perceived usefulness (PU), neglecting other important factors like social influence, facilitating conditions, and individual differences.
Goal Framing' (Lindenberg & Steg, 2007)	1. Challenge in predicting outcomes accurately due to varying and conflicting research findings. 2. Difficulty in predicting behaviors because outcomes may vary significantly depending on the specific context.
General Strain Theory (Agnew, 1985, 1992)	1. Challenge in predicting outcomes accurately due to potential problems with the validity and reliability of the measures used.

Prospect (Kahneman, 1979; Kahneman & Tversky, 2013)	1. Ensuring that research findings and theories are practically relevant and applicable in real-world settings to develop effective security controls and interventions
Accountability (Tetlock, 1983)	1. Challenge in predicting outcomes accurately due to the potential lack of representation of mature professionals from various industries. 2. Difficulty in predicting behaviors because the context and findings may not apply universally across different settings and industry practices.
Cognitive Evaluation (Boal & Cummings, 1981)	1. Challenge in predicting outcomes accurately due to the assumption that intrinsic and extrinsic motivations operate independently and additively. 2. Difficulty in predicting behaviors because the theory may not consider the changing nature of security threats and practices.
Self-Efficacy (Bandura, 1977; Bandura & Wessels, 1994)	1. Challenge in predicting outcomes accurately due to variability in different contexts. 2. Difficulty in predicting behaviors because of the constantly changing nature of security threats. 3. Difficulty in predicting behaviors due to the significant impact of external factors.
Technology Threats Avoidance (Liang et al., 2010)	1. Challenge in predicting outcomes accurately due to limitations in the sample size, which may not represent the broader population.
Opportunity Structure for Crime (Dijk, 1994)	1. Challenge in predicting outcomes accurately due to the constantly changing nature of risks. 2. Difficulty in predicting behaviors accurately due to the reliance on obtaining precise and reliable information.
Trust Transfer (Doney & Cannon, 1997; Stewart, 2003)	1. The theory's predictive capabilities are limited by its lack of consideration for contextual factors, such as organizational culture, individual trust thresholds, or specific security environments, that might shape how trust influences compliance intentions. 2. Predictive accuracy is reduced due to insufficient attention to moderators (e.g., prior trust levels, leadership style) and mediators (e.g., perceived fairness or competence) that could refine the understanding of how trust translates into ISP compliance intentions.
Attitude (Ajzen & Fishbein, 1977)	1. The theory may not adequately predict ISP compliance across diverse contexts, as it lacks consideration of external factors (e.g., organizational culture or individual differences) that might influence the relationship between attitudes and compliance intentions 2. Predictive power is limited by the lack of attention to variables such as peer influence, emotional responses, or perceived risks, which could alter or mediate the effect of attitudes on compliance behavior.
Social Bond (SBT) (Hirschi, 1969)	1. The lack of a longitudinal perspective restricts the ability to predict how social bonds develop and sustain ISP compliance over time, reducing confidence in the dynamic relationships between bonds and compliance. 2. Reliance on self-reported data from employees and supervisors may introduce bias, weakening predictive accuracy in understanding how social bonds influence compliance behaviors.
Paternalistic Leadership (Parker-Follett & Graham, 1933; Weber, 2016)	1. Self-reported data may introduce biases like social desirability bias, affecting the reliability of predictions regarding the influence of leadership styles on compliance. 2. The use of a cross-sectional design hinders the ability to predict how paternalistic leadership impacts ISP compliance over time, limiting confidence in the causal relationships between PL and compliance behaviors.
The Composite Behavior Model (CBM) (Eagly & Chaiken, 1993)	1. The cross-sectional survey design limits predictive accuracy, as it infers causal relationships from theories without directly establishing them. This makes it challenging to predict behavior changes or outcomes reliably across different contexts or timeframes.

Beliefs-Actions-Outcomes (BAO)	1. The theory may not predict or address maladaptive cycles effectively, where new security measures reinforce negative beliefs, perpetuating noncompliance or maladaptive behaviors. 2. With findings based on a single case study, the predictive power of the BAO theory in diverse organizational contexts remains limited, making it difficult to generalize outcomes.
The motive–control (MoCo) theory of Insider Computer Abuse (ICA) (Burns et al., 2023)	1. The theory's conceptual limitations may hinder its predictive accuracy across diverse contexts of ICA, as it is not designed to generalize beyond its specific assumptions. 2. By concentrating on a limited set of motives and controls, the theory may fail to predict ICA behaviors influenced by less commonly considered factors or combinations of influences.
Self-control theory /General Theory of Crime (Gottfredson & Hirschi, 1990a, 1990b)	1. By overlooking situational influences, the theory's predictive accuracy in diverse or dynamic environments is reduced, as it cannot account for how external factors may alter behavior. 2. The theory does not predict which specific behaviors individuals are likely to exhibit, limiting its ability to anticipate why some engage in ICA.
Broaden-and-build (BBT) (Fredrickson, 2001)	1. The cross-sectional design limits the ability to predict how emotional responses influence precaution-taking behaviors over time, reducing the understanding of dynamic emotional effects. 2. Without controlled experimental settings, researchers cannot reliably predict causal relationships between emotions and security behaviors.
Trust (Mayer, 1995; Rousseau et al., 1998)	1. By focusing on the bright-side effects, researchers may fail to predict negative outcomes of trust, such as reduced vigilance or increased vulnerability due to excessive trust in organizational security measures.
Mindfulness (Langer, 1989)	1. The narrow focus may limit the theory's predictive power, as it overlooks how other aspects of mindfulness might influence diverse security-related behaviors or outcomes. 2. The findings may not reliably predict mindfulness-related behaviors or interventions in settings beyond the specific context of information security, reducing their broader applicability.
Full-range leadership (Bass & Avolio, 1994)	1. Reliance on self-reported data introduces potential biases, such as social desirability bias, reducing the predictive accuracy of how leadership styles influence security behavior. 2. The cross-sectional design limits the ability to predict causal relationships between leadership styles and information security behavior intentions over time.
Job demands–Resources (Bakker & Demerouti, 2007)	1. The theory may struggle to predict behaviors in dynamic security environments where demands and resources change unpredictably. 2. Predictive accuracy is reduced when individual and cultural variations in perceptions of demands and resources are not adequately accounted for.
Proactive motivation (ProMT) (Parker et al., 2010)	1. Reliance on self-reported data introduces potential biases, such as social desirability bias, which may compromise the reliability of predictions about proactive behaviors. 2. The cross-sectional design restricts the ability to predict how variables dynamically influence proactive ISBs over time, reducing confidence in inferred causal relationships.
The self-regulatory approach (S-R) (Sutinen & Kuperan, 1999; Tyler, 1990)	1. The S-R approach may not reliably predict compliance behavior in situations where interpersonal influence significantly affects employee decisions, leading to inconsistent outcomes. 2. Predictive accuracy is limited in organizations with rigid ethical climates, as the reliance on personal and social norms could override the influence of self-regulation on compliance behavior.

The command-and-control approach (C-C) (Tyler, 1990, 2004, 2009)	1. The C-C approach may not reliably predict compliance behavior in scenarios where excessive use of external deterrents causes resistance or non-compliance. 2. The predictive accuracy is reduced in environments with strong ethical climates, as employees may default to personal or social norms instead of organizational policies. 3. The approach may fail to predict non-compliance behaviors in contexts where interpersonal relationships significantly influence employee decisions.
Construal-level (CLT) (Trope & Liberman, 2010)	1. Uncertainties in predicting how to effectively influence individuals' construals, particularly in diverse or dynamic settings, limiting its predictive utility.
Person-Environment (P-E) fit. (Caplan, 1987; Caplan & Van Harrison, 1993)	1. The narrow focus of the theory reduces the predictive power of the study, as it may fail to anticipate outcomes influenced by unexamined aspects of ISec management.
Challenge-hindrance stressor (Cavanaugh et al., 2000)	1. Cross-sectional study design limits the ability to predict how stressors and emotions dynamically influence compliance behaviors over time, reducing confidence in causal relationships. 2. Bias in self-reported data, such as inaccuracies in reporting emotions or compliance behaviors, weakens the predictive accuracy.

Appendix C : Prescription Limitations

Theory	**Description of Limitations**
Fear Appeals (Rogers, 1983; Rogers & Deckner, 1975)	1. Restrictive conceptual frameworks 2. A tendency towards management-centric outcomes. 3. Focuses on a limited set of security threats and responses 4. Raises ethical concerns
Rational Choice Theory (Hogarth & Reder, 1987)	1. Overemphasis on large combined models 2. Inaccurately conceptualized decision-making processes
Deterrence (Beccaria, 1963; Gibbs, 1968)	1. Inadequate application to real environment, 2. Prescriptive power depend on integration with other theoretical frameworks
Fraud Triangle (Albrecht et al., 1984, 2008)	1. Complexity in practical application
Routine Activity (Cohen & Felson, 1979)	1. Practical difficulty in examining abuses in digital world
Situational Action (Wikström, 2014; Wikström et al., 2017)	-
Expectancy (Vroom, 2005)	1. Improving diagnostic methods to better identify and address the underlying issues that lead to insecure behaviors
Moral Disengagement (Bandura, 1999)	-

Social Cognitive (Bandura, 1988)	1. Addressing the intricacies of interactions between multiple variables to better understand and apply findings in practice.
Neutralization (Gresham & David, 1957; Sykes & Matza, 2017)	1. Empirical research needed to understand effective methods to inhibit neutralization techniques. 2. Addressing the practical applications and implications of research findings to make them more useful in real-world settings 3. Integration with other theoretical frameworks to enhance understanding and application
Coping Theory (Lazarus & Folkman, 1984)	1. Improving measurement techniques to more accurately capture and analyze the phenomena being studied
Organizational Justice (Greenberg, 1987)	1. Integrating additional factors to more comprehensively address the complexity of factors
Justice (Rawls, 1971)	1. Addressing the complexities of justice theory to more effectively isolate and measure specific impacts on compliance with information security policies
Appraisal (Dewe, 1991; Lazarus & Folkman, 1984; Scherer et al., 2001)	1. Incorporating new findings with existing theoretical models to enhance understanding and application. 2. Conducting empirical research to validate the theories and models, ensuring their applicability and accuracy
Transactional Model of Stress (Lazarus & Folkman, 1984)	1. Limitation of focusing only on direct effects by considering indirect and broader impacts as well.
Affective Events (Weiss & Cropanzano, 1996)	1. Lack of Explicit Hypotheses. 2. Integrating AET with other theoretical models to enhance understanding and application.
Protection Motivation (Rogers, 1975; Rogers & Prentice-Dunn, 1997)	1. Improving the applicability of theories and models to better fit compliance settings 2. incorporating social and organizational factors to enhance the relevance and effectiveness of security behavior models 3. Much of the existing research relies on only portions of PMT¨ 4. Integrating existing models with other theoretical frameworks to enhance understanding and application.
Reasoned Action (Fishbein, 1979)	1. Incorporating more contextual information to better understand and apply findings in real-world settings.
Cognitive Moral Development (Kohlberg, 1963, 1971)	-
Motivational Types of Values (Schwartz, 1992)	1. Further development and research to better apply theories and models specifically to the context of information security

Reactance (Brehm & Brehm, 2013)	1. Integrating the current model with other theories to enhance understanding and application
Social Information Processing (Salancik & Pfeffer, 1978)	1. Integrating the current model with other theories to enhance understanding and application
Dispositional and Situational (Digman, 1997)	1. Conducting more empirical research to validate the theories and models, ensuring their applicability and accuracy.
High Performance and Work Systems (Boxall & Macky, 2009)	1. Addressing the challenges and complexities involved in applying the theories or models in practical, real-world settings
Structural Empowerment (R. Kanter, 1993; R. M. Kanter, 1977, 2008)	1. Addressing and improving the understanding of all potential benefits to provide a more comprehensive view 2. Exploring the role of psychological empowerment as a mediator to enhance the application and effectiveness of the theory
Fairness (Folger & Cropanzano, 2001)	1. Integrating the current model with other theories to enhance understanding and application
Planned Behavior (Ajzen, 1991)	1. Incorporating organizational culture and external factors to provide a more comprehensive understanding and application.
Boundary Management (Ashforth et al., 2000)	1. The complexity in applying theories or models by considering the different preferences individuals have for separating or integrating their roles.
Framework of Emotions (Beaudry & Pinsonneault, 2010)	1. Addressing the influence of contextual factors, such as organizational culture and individual differences, to improve the universal application of the framework
Self-Determination (Ryan & Deci, 2000)	1. Developing a more comprehensive approach to capture the full complexity of factors influencing security behavior in organizational settings. 2. Empirical studies have shown mixed results regarding the impact of perceived severity and probability of security breaches on compliance
Agency (Milgram, 1963, 1974)	-
Organizational Citizenship (Katz, 1964; Organ, 1988, 2014)	1. Expanding the range and improving the quality of measures used to capture relevant variables and constructs more effectively.
Organizational Control (Eisenhardt, 1985; Ouchi, 1979)	1. Improving or diversifying data collection methods to enhance the accuracy and reliability of the data gathered.

Hofstede's Cultural Dimensions (Hofstede, 1984; Hofstede & McCrae, 2004)	1. Improving the reliability of measurement tools to ensure consistent and accurate data collection. 2. Incorporating secondary information and data sources to provide a more comprehensive understanding and validation of findings.
Social Control (Agnew, 1991)	1. Conducting empirical research to validate the theories and models, ensuring their applicability and accuracy. 2. Broadening the focus beyond organizational trust to include other relevant factors in understanding and predicting security behaviors.
Social Action (Hirschi, 1969, 2017; Weber, 1991)	1. Addressing limitations related to the availability of resources, such as funding, time, and personnel, to enhance research and application. 2. Improving data collection methods to ensure accurate, reliable, and comprehensive data for analysis and decision-making.
Value Based Compliance (Karlsson & Hedström, 2019)	1. Addressing limitations related to the availability of resources, such as funding, time, and personnel, to enhance research and application. 2. Improving data collection methods to ensure accurate, reliable, and comprehensive data for analysis and decision-making.
Activity (Kuutti, 1996)	1. Expanding the focus to include both malicious and non-malicious intentions to provide a more comprehensive understanding of security behaviors. 2. Conducting empirical research to validate theories and models, ensuring their applicability and accuracy.
Technology Acceptance Model (F. D. Davis, 1989; F. D. Davis et al., 1989)	1. Broadening the focus to include a wider range of factors influencing technology acceptance, such as social influence, facilitating conditions, and individual differences, to enhance understanding and applicability.
Goal Framing' (Lindenberg & Steg, 2007)	1. Expanding research and frameworks to be more applicable and relevant to IT security contexts, addressing any gaps in application.
General Strain Theory (Agnew, 1985, 1992)	1. Incorporating qualitative research methods to gain deeper and more comprehensive insights into the phenomena being studied.
Prospect (Kahneman, 1979; Kahneman & Tversky, 2013)	-
Accountability (Tetlock, 1983)	1. Conducting further research to examine the applicability of findings across a wider range of organizational contexts and demographic groups, ensuring broader relevance and utility.
Cognitive Evaluation (Boal & Cummings, 1981)	1. Modifying the theory to be more adaptable and flexible allowing it to account for the dynamic and rapidly changing environment of information security.
Self-Efficacy (Bandura, 1977; Bandura & Wessels, 1994)	1. Improving measurement tools and methods to enhance the accuracy and reliability of data collection and analysis
Technology Threats Avoidance (Liang et al., 2010)	1. Conducting further validation studies to ensure the reliability and accuracy of findings. 2. Expanding the application of research findings to a wider range of settings and populations to enhance generalizability and practical relevance.

Opportunity Structure for Crime (Dijk, 1994)	1. Addressing the practical challenges and feasibility of implementing theories or models in real-world settings.
Trust Transfer (Doney & Cannon, 1997; Stewart, 2003)	1. Trust Transfer Theory provides limited guidance on actionable interventions to foster trust or repair trust breaches within an organization, hindering its utility for designing practical strategies to enhance ISP compliance intentions
Attitude (Ajzen & Fishbein, 1977)	1. Limitation in providing actionable strategies to effectively enhance attitudes or translate positive attitudes into consistent compliance behaviors, limiting its prescriptive utility for organizational interventions
Social Bond (SBT) (Hirschi, 1969)	1. Future studies should explore social bonds in varying cultural contexts to inform strategies for fostering stronger, context-specific bonds that enhance ISP compliance. 2. Conducting longitudinal research could provide actionable insights into the long-term impact of social bonds on compliance, offering robust guidance for policy development and intervention planning.
Paternalistic Leadership (Parker-Follett & Graham, 1933; Weber, 2016)	1. Examine paternalistic leadership in various cultural settings to provide actionable insights for tailoring leadership interventions across diverse organizational contexts. 2. Broadening the scope to include additional leadership styles could help identify more effective approaches for promoting ISP compliance, offering a wider range of strategies for organizational improvement
The Composite Behavior Model (CBM) (Eagly & Chaiken, 1993)	1. Longitudinal research with multiple sources of measurement is recommended to better validate causal relationships, offering stronger evidence for interventions and theoretical refinements. 2. Expanding future studies to include a broader range of non-malicious security violations (NMSVs) can provide more comprehensive data, enhancing the model's applicability and robustness in guiding practical interventions
Beliefs-Actions-Outcomes (BAO) Theory	1. The theory lacks prescriptive strategies for breaking maladaptive belief-action-outcome cycles, which are critical for fostering adaptive security behaviors. 2. The BAO theory does not offer tailored interventions for IS security, requiring adaptation or integration with other frameworks to address domain-specific challenges effectively.
The motive–control (MoCo) theory of Insider Computer Abuse (ICA) (Burns et al., 2023)	1. As a complementary theory, MoCo does not provide standalone solutions, requiring integration with other theories to develop holistic interventions for ICA. 2. The narrow focus on certain motives and controls limits the theory's ability to guide comprehensive or context-sensitive strategies for preventing ICA.
Self-control Theory /General Theory of Crime (Gottfredson & Hirschi, 1990a, 1990b)	1. Without integrating organizational and environmental factors, the theory offers limited guidance on designing interventions or strategies to prevent ICA effectively. 2. The theory does not provide actionable insights into how to motivate individuals away from ICA, reducing its practical utility for developing targeted behavioral interventions.
Broaden-and-build (BBT) (Fredrickson, 2001)	1. Future research should incorporate observational methods or neuroscience techniques to improve the accuracy of data on emotional and behavioral responses. 2. Expanding the sample to include diverse organizational contexts and cultures would improve the applicability of findings and guide more universally relevant interventions. 3. Employing controlled experimental designs in future studies could clarify causal pathways and enhance the development of emotion-based interventions for improving security behaviors.
Trust (Mayer, 1995; Rousseau et al., 1998)	1. Prescriptive insights would benefit from addressing both the positive and negative effects of trust, guiding organizations to balance trust with measures that mitigate potential risks of over trust or misplaced trust.

Mindfulness (Langer, 1989)	1. Exploring additional dimensions of mindfulness, such as its impact on decision-making or emotional regulation, to provide more comprehensive guidance for organizational security practices. 2. Expanding the application of mindfulness theory to diverse organizational contexts and behaviors could enhance its prescriptive utility and generalizability for designing interventions.
Full-range leadership (Bass & Avolio, 1994)	1. Expanding the scope to include additional or hybrid leadership styles could provide more actionable insights for promoting information security intentions. 2. Incorporating alternative data collection methods, such as peer assessments or observational data, can mitigate biases and enhance the reliability of prescriptive recommendations.
Job demands–resources (Bakker & Demerouti, 2007)	1. Adapting the framework to include individual and cultural differences in perceptions of demands and resources would enhance its applicability and effectiveness in diverse organizational settings. 2. Expanding the model to address specific security-related behaviors could provide more actionable insights for improving compliance and reducing non-compliance.
Proactive motivation (ProMT) (Parker et al., 2010)	1. Extending the theory to diverse settings and industries to improve its prescriptive relevance and generalizability. 2. Incorporating alternative data collection methods, such as observational or peer-reported data, could mitigate biases and improve the accuracy of recommendations.
The self-regulatory approach (S-R) (Sutinen & Kuperan, 1999; Tyler, 1990)	1. Limitation on focusing on balancing rules-oriented climates with initiatives that reinforce internalized self-regulatory norms to promote ISP compliance effectively. 2. Limited strategies to mitigate the impact of interpersonal influence on compliance behavior, such as fostering a culture where internal values are aligned with social expectations.
The command-and-control approach (C-C) (Tyler, 1990, 2004, 2009)	1. Interventions should integrate the C-C approach with strategies that support personal and social norms to align with organizational directives effectively. 2. Prescriptions should include building a collaborative culture that aligns interpersonal relationships with organizational security goals, reducing the conflict between social priorities and compliance. 3. Limited in balancing external deterrents with positive reinforcement strategies, such as fostering intrinsic motivation for compliance.
Construal-level theory (CLT) (Trope & Liberman, 2010)	1. There is a need to identify actionable ways to leverage knowledge mechanisms to influence construal effectively in various contexts. 2. Prescriptive strategies should focus on extending the application of CLT to different contexts, improving its practical relevance for shaping perceptions and behaviors.
Person-Environment (P-E) fit. (Caplan, 1987; Caplan & Van Harrison, 1993)	1. Limited integrated ISec framework to provide a comprehensive understanding and guide more effective organizational ISec efforts.
Challenge-hindrance stressor (Cavanaugh et al., 2000)	1. Using alternative data collection methods, such as observational or peer-reported data, could reduce bias and improve the reliability of intervention strategies. 2. Employing longitudinal research could strengthen causal inferences and provide better guidance for designing interventions targeting stressors and compliance behaviors.

Impact of Artificial Intelligence on Employee Strain and Insider Deviance in Cybersecurity

Short Paper

Emmanuel Anti
University of Vaasa
Wolffintie 32, 65200 Vaasa, Finland
emmanuel.anti@uwasa.fi

Duong Dang
University of Vaasa
Wolffintie 32, 65200 Vaasa, Finland
duong.dang@uwasa.fi

Abstract

This paper examines the impact of AI technologies like Performance Monitoring Tools (PMTs) and Automated Decision-Making Systems (ADMSs) on employee strain and the development of insider deviant behavior. Drawing on General Strain Theory (GST), the study explores how workplace stressors exacerbated by AI-driven PMTs and ADMSs may increase the risk of deviant behaviors such as fraud, sabotage, and social engineering. This study employs a quantitative methodology, using surveys to gather data on employee perceptions of AI-driven PMTs and ADMSs on employee strain and insider deviance. We expect that the findings will show AI-induced stress and negative emotions increase the likelihood of insider deviance. This study aims to contribute to research on cybersecurity threats and provide practical insights for organizations implementing AI technologies by offering strategies to mitigate workplace stress and insider threats. Future research will explore the relationship between AI integration, employee strain, and organizational security vulnerabilities.

Keywords: Artificial Intelligence, General Strain Theory, Insider Deviance

Introduction

The integration of AI technologies like Performance Monitoring Tools (PMTs) and Automated Decision-Making Systems (ADMSs) enhances efficiency, decision-making, and innovation, driving digital transformation (Benbya et al., 2020). For instance, Amazon employs AI systems to track employee performance across productivity, quality, safety, and behavior (Spilda et al., 2024). However, AI-driven automation also increases workplace surveillance, stress, and arbitrary disciplinary actions, leading employees to feel unfairly targeted (Spilda et al., 2024). Caminiti (2023) reports that a survey by CNBC and SurveyMonkey revealed that 42% of workers fear AI's effect on their roles, with those earning under $50,000 showing even higher concern. The survey further indicated that the more employees interact with AI, the more concerned they become about its impact on their jobs

Employees may face pressure to meet AI-imposed benchmarks, heightening job dissatisfaction, stress, and turnover (Hou & Fan, 2024; Konuk et al., 2023; Mikalef et al., 2023). Fear of job loss, dehumanization, and diminished human interaction exacerbates psychological distress (Matsunaga, 2022; Nazareno & Schiff, 2021) increasing the likelihood of insider deviance (Dang, 2014; Green, 2014). Financial struggles, personality problems, and social isolation further contribute to retaliatory deviant behaviors, such as sabotage or system exploitation (Liang et al., 2023; Renaud et al., 2024). Although recent studies explore AI's workplace impact (Chesley, 2014; Kola, 2023), there is limited research on the evolution of employee stress, coping strategies, and deviant behaviors under sustained AI interaction. As AI technologies become

more integrated into the workplace, concerns about their psychological and behavioral impacts are growing (Chuang et al., 2025; Leong et al., 2025). Further investigation is needed into organizational interventions mitigating AI-related workplace stress and insider deviance.

This motivates our study to investigate the correlation between AI technologies like PMTs and ADMSs and their impact on workplace strain and insider deviance. Further, we aim to bridge the gap between cybersecurity and deviant behavior research by focusing on AI-induced strain with cybersecurity risks, providing fresh insights into how employees' interactions with AI may lead to harmful actions within organizations. Thus, we focus on the following research question: How do AI-driven PMTs and ADMSs influence employee strain, and how does this strain contribute to insider deviance?

We applied quantitative research approach with general strain theory (Agnew, 1985, 1992) as our theoretical background, using PMTs and ADMSs as applications to answer this question. General strain theory (Agnew, 1985, 1992) explains that negative emotions caused by stressful workplace conditions can lead to deviant behavior. This study aims to contribute to research on cybersecurity threats and provide practical insights for organizations implementing AI technologies by offering strategies to mitigate workplace stress and insider threats. This study offers a novel framework that applies General Strain Theory to AI implementation in cybersecurity by introducing AI-specific workplace stressors, providing new insights into how emerging technologies shape employee deviance. The insights from this study can advance theory and offer practical value to organizations aiming to balance technological efficiency with employee well-being and security.

This paper is organized as follows: First, the literature review and theoretical background are presented. Next, the research methods are introduced. Finally, the paper concludes with discussions and conclusions.

Literature Review and Theoretical Background

Insider Deviance

Insider deviance refers to the violation of organizational norms by trusted individuals (e.g., employees, contractors, or vendors) that threaten organizational well-being, involving compromise, manipulation, unauthorized access, or tampering with ICT and non-ICT systems, whether intentional or unintentional, to achieve personal or organizational outcomes through cognitive and physical processes (Anti & Vartiainen, 2024; Green, 2014). Common insider deviant behaviors include social engineering, fraud, and IT sabotage, influenced by personal predispositions, psychological traits, and workplace stressors (Luo et al., 2020). Factors like financial conflicts, dissatisfaction, and resistance to organizational changes contribute to deviance, while social frustrations, job instability, and resentment toward authority can escalate insider deviance, particularly in response to AI-driven technologies like PMTs and ADMSs (Intelligence & Subcommittee, 2017; Loureiro et al., 2023). For instance, AI-driven surveillance and automation can lead to fears of job replacement and loss of control, fostering anxiety, resentment, and potential hostility toward the organization, increasing insider deviance (Loureiro et al., 2023). These emotional responses align with General Strain Theory (GST), which posits that strain especially when perceived as unjust—can lead to deviant behavior as a coping mechanism (Agnew, 1992). Building on Dang's (2014) integration of GST and organizational injustice, we argue that AI-induced workplace changes—when perceived as unfair or overwhelming—may significantly contribute to insider deviance. These insights are increasingly relevant as AI systems alter traditional work structures and employee control, often without corresponding changes to support systems or accountability structures (Dennehy et al., 2023; Liang et al., 2016)

Implementation of AI Technologies

AI implementation involves integrating artificial intelligence technologies into organizational operations, products, and services, combining AI with expertise, data, and strategies ((Alsheibani et al., 2018; McElheran et al., 2021). Technologies like PMTs and Automated ADMSs enhance productivity and decision-making while requiring substantial system modifications and restructuring (Agrawal et al., 2021). ADMSs shift decision-making to autonomous agents, keeping humans accountable for outcomes (Ivanov, 2023). AI-driven tools influence hiring, promotions, and disciplinary actions, raising concerns over privacy, technostress, and job insecurity (Wamba-Taguimdje et al., 2020). Additionally, misinformation, digital overdependence, and reduced social interaction impact work-life balance and employee morale (Loureiro

et al., 2023; Nishant et al., 2020). For example, while AI can enhance efficiency and decision-making in the workplace, Chuang, Chiang, and Lin (2025); Ding et al. (2025); Leong et al. (2025); and Zhang et al. (2025) emphasize that it can also increase psychological strain when demands such as heightened cognitive load, performance pressure, and constant monitoring exceed the employee's available resources like organizational support, autonomy, or transparency. This imbalance may lead to AI-induced stress, which depletes emotional and psychological resources, resulting in fatigue, anxiety, and reduced work engagement (Hou & Fan, 2024).

Without proper change management, AI integration may lead to job displacement, resistance, and heightened stress, fostering anger toward authority and increasing the risk of insider deviance (Intelligence & Subcommittee, 2017; Leong et al., 2025; Loureiro et al., 2023; Zhang et al., 2025). According to GST, such strains particularly when perceived as unjust or unavoidable can foster negative emotional states like anger or frustration, increasing the likelihood of deviant behavior, when AI is poorly managed.

Hypotheses Development

General Strain Theory

This study adopts General Strain Theory (GST) to examine how AI-driven PMTs and ADMSs contribute to insider deviance by creating workplace stressors. GST, developed by Agnew (1985, 1992), explains how individuals engage in deviant behavior when exposed to stressors such as goal obstruction, loss of valued stimuli, or negative conditions. These stressors trigger negative emotions like anger, frustration, or depression, which can influence individuals' coping mechanisms and responses (Agnew, 1985, 1992).

GST identifies three primary forms of strain: (1) Failure to achieve positively valued goals, often due to the disparity between expectations and actual achievements. (2) Removal of positive stimuli, such as job loss or career stagnation. (3) Presentation of negative stimuli, including workplace stress, excessive monitoring, and unfair treatment.

Prior research has applied GST to workplace deviance, showing how perceived strain contributes to misconduct (Aseltine Jr et al., 2000; Broidy & Agnew, 1997; Moon & Morash, 2017). Studies by Agnew and White, (1992) and Wang et al. (2022) operationalized GST variables such as strain, coping mechanisms, and emotional responses to analyze employee corruption and delinquency. For example, Wang et al. (2022) identified various strains, including resource strain, deviant subcultural strain, economic strain, work-related strain, and political promotion strain.

Building on these studies, we apply GST to AI-driven workplace stressors to examine how employees experience job insecurity, surveillance pressure, and unfair evaluations under PMTs and ADMSs. These AI-related stressors may heighten frustration and resentment toward management, increasing the likelihood of insider deviance. This study advances GST by adapting it to AI-induced workplace stressors characterized by AI-related uncertainty, perceived irreversibility of outcomes, and constant AI presence, thereby maintaining theoretical continuity, refining key variables, and enhancing reliability in explaining both malicious and non-malicious insider deviance. The devised variables, informed by these theoretical foundations, are outlined in Table 1 to illustrate the adaptation of GST in our research framework.

Table 1 Developed Variables

Constructs	Concepts	Selected Sources
AI-induced work strain (AIW)	Strain arising from persistent surveillance, decision-making displacement, job insecurity, and intensified performance pressures from the application of AI technologies in the workplace.	Hou & Fan (2024); Kambur & Yildirim (2023); Winwood et al. (2007)
AI-induced workload change (AIWC)	Changes influenced by job demands, task complexity, and loss of control due to AI technology implementation.	DiStaso & Shoss (2020); Hou & Fan (2024)
AI-induced perceived inequity (AIPI)	Perceptions of unfair treatment in terms of procedures, outcomes, and interpersonal interactions, decision-making from AI technologies.	Lowry et al. (2015); Zhang et al. (2025)

Employee Strain (ES)	Strain caused by Internal and external pressures.	D'Arcy & Teh (2019); Yazdanmehr et al. (2023)
Insider Deviance (ID)	Individuals with legitimate access to an organization's resources who intentionally or unintentionally misuse this access to cause harm, often for personal gain, revenge, or ideological reasons	Dang (2014); Guo et al. (2011)

AI-Induced Work Strains

Winwood et al. (2007) defines work strain as arising from high workloads, tight deadlines, and workplace conflicts, which can negatively impact employees' mental and physical well-being. However, Hou and Fan (2024) explain AI-induced work strain as the psychological stress and emotional burden experienced by employees or managers due to the application of AI technology in the workplace. This may include anxiety over job security, difficulties adapting to AI tools, or cognitive overload from managing complex AI-driven systems. AI-driven PMTs and ADMSs present distinct work strain challenges. AI technologies change decision-making, employment roles, and surveillance, creating psychological and structural pressures. (Kambur & Yildirim, 2023). Employees may suffer stress when artificial intelligence judgments replace human judgment without consultation or feel overwhelmed by the rapid pace of required developing their skills or experience.

Hence, we propose the following hypotheses:

H1: AI-Induced Work Strain Positively Affects Employee Strain.

H2: AI-Induced Work Strain Positively Affects Insider Deviance

AI- Induced Workload Changes

Workload changes are dynamic and influenced by seasons and project demands (DiStaso & Shoss, 2020). High workloads contribute to psychological strain, emotional distress, and fatigue, with anticipated increases intensifying strain and decreases providing relief (DiStaso & Shoss, 2020). AI-induced workload changes affect job demands, task complexity, and control, increasing stress or reducing engagement (Hou & Fan, 2024). For example, AI technologies may reduce manual tasks by automating routine work, but they can also increase cognitive demands by requiring employees to interpret and act on AI outputs. AI-induced workload changes, especially if employees feel overloaded or under-challenged by AI, increase the likelihood of deviant behavior as a form of protest or reaction Such reactions from employees may be due to the perceived removal of positive stimuli such as control over tasks and decisions, social interactions, and career development, to mention a few. We therefore propose these hypotheses:

H3: AI-induced workload Changes Positively Affect Employee Strain.

H4: AI-induced workload Positively Affect Insider Deviance.

AI-Induced Perceived Inequity

According to Lowry et al. (2015), workplace inequity refers to employees' perception of unfair treatment in terms of procedures, outcomes, and interpersonal interactions, leading to negative behaviors like cyberloafing, organizational deviance, counterproductive actions, retaliation, and sabotage, as the fairness of treatment significantly influences these reactions. AI-driven systems can create perceptions of inequity in the workplace such as unequal access to AI resources, biased performance evaluations, lack of transparency in decision-making, or perceived favoritism in task allocation which may lead to dissatisfaction, mistrust, disengagement, and increased resistance to AI integration (Zhang et al., 2025). Perceived inequity represents a failure to achieve positively valued goals espoused by the GST. Hence, we propose the following hypothesis:

H5: AI-induced Perceived Inequity Positively Affects Employee Strain.

Employee Strain

Internal and external pressures, like excessive workloads, deadlines, and conflicts between home and work, can provoke deviant outcomes, while disagreements may incite deviant behavior, jeopardizing autonomy (D'Arcy & Teh, 2019; Yazdanmehr et al., 2023). When employees feel constant surveillance by AI-driven PMTs and are negatively impacted by ADMS decisions, their stress may increase, leading to insider behaviors. We therefore propose this hypothesis:

H6: Employee Strain Positively Affects Insider Deviance.

Taken together, Figure 1 presents the conceptual framework of the study. The control variables incorporated in the model include job role, level of seniority, industry, educational attainment, and employment status.

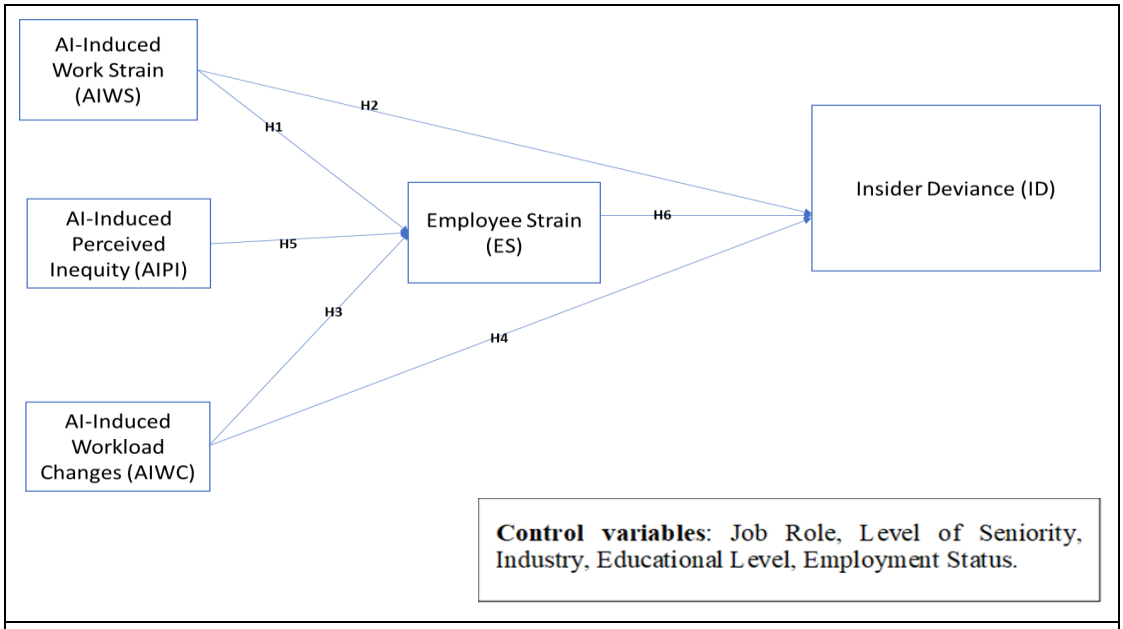

Figure 1. Research Model

Research Methodology

This study employs a quantitative research approach to examine the impact of AI-driven Performance Monitoring Tools (PMTs) and Automated Decision-Making Systems (ADMSs) on insider deviance. Quantitative methods allow for statistical analysis of relationships among measurable variables, ensuring objective and replicable findings (Kumar, 2018; Yilmaz, 2013). To achieve this, the study will use previously validated measures for all constructs, adapting them slightly to fit the research context.

Data was collected through a structured survey designed to gather insights into AI-induced workplace strain, workload changes, perceived inequity, employee strain, and insider deviant behavior. The survey included standardized questions (Roopa & Rani, 2012) to ensure consistency in responses. To ensure diverse representation across job roles, industries, and organizational levels, a stratified random sampling approach were implemented. This method provided precise estimates and enhanced the generalizability of findings (Singh & Masuku, 2014). Participants were recruited from Europe and North America, specifically from the United States and Canada, to account for regional differences in AI adoption and workplace policies. The target respondents were employees who have direct experience with AI-driven PMTs and ADMSs in their workplace or regularly interact with AI tools as part of their job responsibilities in sectors such as technology, finance, healthcare, and manufacturing. A key consideration in the study was the

sample size calculation to ensure statistical reliability. Based on a priori power analysis (Faul et al., 2007), it was determined that a minimum of 102 responses would be required to detect significant effects. However, to account for potential dropouts, response biases, or missing data, the study aimed to collect responses from at least 150 participants. This provided a more robust dataset for statistical analysis and increased the likelihood of capturing meaningful patterns related to AI-induced workplace strain and insider deviance.

The criteria for selecting respondents ensured that participants were well-suited for the study's objectives. Suitable respondents include employees who have had direct exposure to AI-driven PMTs and ADMSs, those who frequently interact with AI tools in their work, and professionals from diverse industries and job roles. For example, the requirement for participants to have direct experience with AI tools was operationalized through screening questions confirming active use of AI-driven systems such as automated decision-making, monitoring, or recommendation tools. By incorporating a broad range of perspectives, the study will be able to account for industry-specific variations in AI adoption and workplace stressors. To control for potential confounding variables, the survey collected data on job role, seniority level, industry sector, company size, and employment type (full-time, part-time, contract, or remote work). This approach ensures that differences in workplace environments and organizational structures do not skew the results.

To measure the constructs of AI-induced workload change, AI-induced perceived inequity, and AI-induced work strain, we utilized items from several validated scales, including technostress (Nisafani et al., 2020), organizational justice (Jang et al., 2021), and workplace strain (Anis & Emil, 2022). These items were adapted to fit the AI context, and content validity was ensured through expert review. The survey design consisted of Likert-scale questions, ranging from 1 = strongly disagree to 7 = strongly agree, to measure perceptions of AI-induced work strain, workload, perceived inequity, and insider deviant behaviors. Additionally, demographic and work-related questions were included to classify respondents based on relevant criteria. The survey also incorporated techniques to minimize response biases, such as randomizing question order to prevent priming effects, including attention-check questions to ensure valid responses, and ensuring participant anonymity and confidentiality to encourage honest feedback. To validate the effectiveness of the survey, a pilot study was conducted before full-scale data collection. The pilot phase included ten participants who tested the questionnaire for clarity and usability, two cybersecurity experts who provided content validation, and a group of doctoral students and faculty members who reviewed the methodological framework. Their feedback led to refinements in question wording and structure, improving the survey's reliability and accuracy. Participants in the pilot study confirmed that the research design, survey content, and procedures were effective and aligned with the study's objectives. Following data collection, statistical techniques are being applied to assess the significance of AI-induced work strain in predicting insider deviance. Regression models are being used to test relationships between key variables, while robustness checks will ensure that findings remain valid across different job roles, industries, and organizational settings. By addressing the unique role of AI in workplace stressors and deviance, this study provides a methodologically rigorous approach to understanding AI's impact on insider threats.

Discussions and Conclusions

We conducted a pilot study to refine our research approach, and the results indicate that both the research design and the questionnaire worked well. Then, the survey was distributed, and we received a total of 141 responses, which met our objectives. Our next step is to analyze data from the study. We expect the results to reveal a significant correlation between AI-induced workplace strains due to the implementation of AI-driven PMTs and ADMSs and the increase of insider deviant behaviors. Grounded in GST (Agnew, 1985, 1992), we anticipate that AI-induced strains may elicit negative emotional responses such as frustration, anxiety, resentment, and distrust, potentially resulting in deviant behaviors, including insider threats.

In theory, the study's result extend GST by applying it to the context of AI adoption in cybersecurity, offering a fresh and underexplored perspective on how AI technologies intensify job stress and influence employee behavior. The results will guide organizations to the potential risks of using AI technologies such as PMTs and ADMSs without sufficient change management or employee support. The study will contribute information systems and organizational behavior literature by introducing and empirically validating AI-specific workplace stressors such as AI-induced work strain, perceived inequity, and workload change as predictors of insider deviance. The study also allows for a more nuanced examination of how AI

technologies affect employees, particularly in terms of emotional well-being and behavioral responses by introducing and operationalizing three new constructs (AI-induced work strain (AIW), AI-induced workload change (AIWC), and AI-induced perceived inequity (AIPI), which are uniquely relevant to ongoing digital transformation and automation processes in organizations.

Practically, the findings of the study can guide organizations in the mitigation of insider threats that may arise from AI-driven environments, thereby enhancing cybersecurity resilience against cyber threats (Järveläinen et al., 2025). This study further encourages fair AI governance and transparent decision-making processes to address employee concerns around autonomy, fairness, and control across both technical and non-technical dimensions. This is crucial, as the existing literature on cybersecurity is predominantly technocentric (Dang & Vartiainen, 2024). Additionally, the study highlights the importance of investing in employee support systems, including targeted training programs and engagement initiatives (Dang et al., 2022), to reduce psychological strain and increase organizational trust. The findings in this study can assist organizations in formulating more effective crisis management strategies and in implementing AI integration processes that are both humane and transparent. In the context of smart cities, for example, stakeholders involved in such initiatives may leverage these insights to develop crisis management frameworks that prioritize citizen engagement and institutional transparency. By proactively addressing sociotechnical stressors such as technological unfamiliarity and management fashion trends, policymakers can enhance public trust and facilitate the smoother adoption of AI-enabled urban innovations (e.g., intelligent traffic management systems, digital services, and AI-assisted platforms) (Dang, 2025). Moreover, by highlighting the psychological costs of unchecked AI adoption such as anxiety, resentment, and perceived injustice, this study offers a framework for balancing technological efficiency with employee well-being and organizational resilience.

The work remaining to complete the paper is as follows: We have developed the theoretical model, validated the survey instrument, and completed data collection, and are now conducting rigorous statistical analyses including regression to examine the relationship between AI-driven workplace strain and insider deviance, with plans to refine theoretical insights and generate actionable recommendations. This paper presents the conceptual framework, construct development, and research design as a foundation for empirical validation and practical implications, with full analysis and manuscript completion expected ending of May 2025.

References

Agnew, R. (1985). A revised strain theory of delinquency. *Social Forces*, *64*(1), 151–167.

Agnew, R. (1992). Foundation for a general strain theory of crime and delinquency. *Criminology*, *30*(1), 47–88. https://doi.org/10.1111/j.1745-9125.1992.tb01093.x

Agnew, R., & White, H. R. (1992). An empirical test of general strain theory. *Criminology*, *30*(4), 475–500. https://doi.org/10.1111/j.1745-9125.1992.tb01113.x

Agrawal, A. K., Gans, J. S., & Goldfarb, A. (2021). *Ai adoption and system-wide change*. National Bureau of Economic Research. 10.3386/w28811

Alsheibani, S., Cheung, Y., & Messom, C. (2018). Artificial Intelligence Adoption: AI-readiness at Firm-Level. *PACIS*, *4*, 231–245. https://aisel.aisnet.org/pacis2018/37

Anis, M., & Emil, D. (2022). The impact of job stress on deviant workplace behavior: The mediating role of job satisfaction. *American Journal of Industrial and Business Management*, *12*(1), 123–134.

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), 4. https://doi.org/10.17705/1CAIS.05501

Aseltine Jr, R. H., Gore, S., & Gordon, J. (2000). Life stress, anger and anxiety, and delinquency: An empirical test of general strain theory. *Journal of Health and Social Behavior*, 256–275. https://doi.org/10.2307/2676320

Benbya, H., Davenport, T. H., & Pachidi, S. (2020). Artificial intelligence in organizations: Current state and future opportunities. *MIS Quarterly Executive*, *19*(4). http://dx.doi.org/10.2139/ssrn.3741983

Broidy, L., & Agnew, R. (1997). Gender and crime: A general strain theory perspective. *Journal of Research in Crime and Delinquency*, *34*(3), 275–306. https://doi.org/10.1177/0022427897034003

Caminiti, S. (2023). *The more workers use AI, the more they worry about their job security, survey finds—Cnbc.com*.https://www.cnbc.com/2023/12/19/the-more-workers-use-ai-the-more-they-worry-about-their-job-security.html

Chesley, N. (2014). Information and communication technology use, work intensification and employee strain and distress. *Work, Employment and Society*, *28*(4), 589–610.

Chuang, Y.-T., Chiang, H.-L., & Lin, A.-P. (2025). Insights from the Job Demands–Resources Model: AI's dual impact on employees' work and life well-being. *International Journal of Information Management*, *83*, 102887. https://doi.org/10.1016/j.ijinfomgt.2025.102887

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)*, 1–11. https://aisel.aisnet.org/confirm2014/10

Dang, D., Mäenpää, T., Mäkipää, J.-P., & Pasanen, T. (2022). The anatomy of citizen science projects in information systems. First Monday, 57(10). https://doi.org/10.5210/fm.v27i10.12698

Dang, D., & Vartiainen, T. (2024). Exploring Socio-technical Gaps in the Cybersecurity of Energy Informatics for Sustainability. In *Adoption of Emerging Information and Communication Technology for Sustainability* (pp. 288–304). CRC Press.

Dang, D. (2025). Digital Innovation as a Management Trend: A Case Study on the Adoption of Smart City Initiatives. In N. H. Thuan, D.-P. Duy, H.-S. Le, & T. Q. Phan (Eds.), Information Systems Research in Vietnam, Volume 3: A Shared Vision and New Frontiers (pp. 149–163). Springer Nature. https://doi.org/10.1007/978-981-97-9835-3_10

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. https://doi.org/10.1016/j.im.2019.02.006

Dennehy, D., Griva, A., Pouloudi, N., Dwivedi, Y. K., Mäntymäki, M., & Pappas, I. O. (2023). Artificial intelligence (AI) and information systems: Perspectives to responsible AI. *Information Systems Frontiers*, *25*(1), 1–7. https://doi.org/10.1007/s10796-022-10365-3

Ding, X.-Q., Chen, H., Liu, J., Liu, Y.-Z., & Wang, X.-H. (2025). AI-induced behaviors: Bridging proactivity and deviance through motivational insights. *Journal of Managerial Psychology*.

DiStaso, M. J., & Shoss, M. K. (2020). Looking forward: How anticipated workload change influences the present workload–emotional strain relationship. *Journal of Occupational Health Psychology*, *25*(6), 401. https://doi.org/10.1037/ocp0000261

Faul, F., Erdfelder, E., Lang, A.-G., & Buchner, A. (2007). G* Power 3: A flexible statistical power analysis program for the social, behavioral, and biomedical sciences. *Behavior Research Methods*, *39*(2), 175–191. https://doi.org/10.3758/BF03193146

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

Guo, K. H., Yuan, Y., Archer, N. P., & Connelly, C. E. (2011). Understanding nonmalicious security violations in the workplace: A composite behavior model. *Journal of Management Information Systems*, *28*(2), 203–236. https://doi.org/10.2753/MIS0742-1222280208

Hou, Y., & Fan, L. (2024). Working with AI: The effect of job stress on hotel employees' work engagement. *Behavioral Sciences*, *14*(11), 1076. https://doi.org/10.3390/bs14111076

Intelligence, & Subcommittee, N. S. A. S. P. R. C. I. T. (2017). *Assessing the Mind of the Malicious Insider: Using a Behavioral Model and Data Analytis to Improve Continuous Evaluation*. Intelligence and National Security Alliance.

Ivanov, S. H. (2023). Automated decision-making. *Foresight*, *25*(1), 4–19. 10.1108/FS-09-2021-0183

Jang, J., Lee, D. W., & Kwon, G. (2021). An analysis of the influence of organizational justice on organizational commitment. *International Journal of Public Administration*, *44*(2), 146–154. https://doi.org/10.1080/01900692.2019.1672185

Järveläinen, J., Dang, D., Mekkanen, M., & Vartiainen, T. (2025). Towards a framework for improving cyber security resilience of critical infrastructure against cyber threats: A dynamic capabilities approach. *Journal of Decision Systems*, *34*(1), 2479546. https://doi.org/10.1080/12460125.2025.2479546

Kambur, E., & Yildirim, T. (2023). From traditional to smart human resources management. *International Journal of Manpower*, *44*(3), 422–452. 10.1108/IJM-10-2021-0622

Kola, V. (2023). The Liberating Effect of AI in Organizations. *1ST Bengkulu International Conference on Economics, Management, Business and Accounting (BICEMBA 2023)*, 275–282.

Konuk, H., Ataman, G., & Kambur, E. (2023). The effect of digitalized workplace on employees' psychological well-being: Digital Taylorism approach. *Technology in Society*, *74*, 102302. https://doi.org/10.1016/j.techsoc.2023.102302

Kumar, R. (2018). *Research methodology: A step-by-step guide for beginners*.

Leong, A. M. W., Bai, J. Y., Rasheed, M. I., Hameed, Z., & Okumus, F. (2025). AI disruption threat and employee outcomes: Role of technology insecurity, thriving at work, and trait self-esteem. *International Journal of Hospitality Management*, *126*, 104064.

Liang, N., Biros, D. P., & Luse, A. (2016). An empirical validation of malicious insider characteristics. *Journal of Management Information Systems*, *33*(2), 361–392.

Liang, N., Biros, D. P., & Luse, A. (2023). An empirical comparison of malicious insiders and benign insiders. *Journal of Computer Information Systems*, 1–13. Loureiro, S. M. C., Bilro, R. G., & Neto, D. (2023). Working with AI: can stress bring happiness? *Service Business*, *17*(1), 233–255.

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. https://doi.org/10.1111/isj.12063

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. 10.17705/1jais.00646

Matsunaga, M. (2022). Uncertainty management, transformational leadership, and job performance in an AI-powered organizational context. *Communication Monographs*, *89*(1), 118–139.

McElheran, K., Li, J. F., Brynjolfsson, E., Kroff, Z., Dinlersoz, E., Foster, L., & Zolas, N. (2021). AI adoption in America: Who, what, and where. *Journal of Economics & Management Strategy*.

Mikalef, P., Lemmer, K., Schaefer, C., Ylinen, M., Fjørtoft, S. O., Torvatn, H. Y., Gupta, M., & Niehaves, B. (2023). Examining how AI capabilities can foster organizational performance in public organizations. *Government Information Quarterly*, *40*(2), 101797. https://doi.org/10.1016/j.giq.2022.101797

Moon, B., & Morash, M. (2017). A test of general strain theory in South Korea: A focus on objective/subjective strains, negative emotions, and composite conditioning factors. *Crime & Delinquency*, *63*(6), 731–756. https://doi.org/10.1177/0011128716686486

Nazareno, L., & Schiff, D. S. (2021). The impact of automation and artificial intelligence on worker well-being. *Technology in Society*, *67*, 101679. https://doi.org/10.1016/j.techsoc.2021.101679

Nisafani, A. S., Kiely, G., & Mahony, C. (2020). Workers' technostress: A review of its causes, strains, inhibitors, and impacts. *Journal of Decision Systems*, *29*(sup1), 243–258.

Nishant, R., Kennedy, M., & Corbett, J. (2020). Artificial intelligence for sustainability: Challenges, opportunities, and a research agenda. *International Journal of Information Management*, *53*, 102104.

Renaud, K., Warkentin, M., Pogrebna, G., & van der Schyff, K. (2024). VISTA: An inclusive insider threat taxonomy, with mitigation strategies. *Information & Management*, *61*(1), 103877.

Roopa, S., & Rani, M. S. (2012). Questionnaire designing for a survey. *Journal of Indian Orthodontic Society*, *46*(4_suppl1), 273–277. https://doi.org/10.5005/jp-journals-10021-1104

Singh, A. S., & Masuku, M. B. (2014). Sampling techniques & determination of sample size in applied statistics research: An overview. *International Journal of Economics, Commerce and Management*, *2*(11), 1–22.

Spilda, F. U., Brittain, L., Cant, C., Cole, M., Mozzachiodi, R., & Graham, M. (2024). Fairwork Amazon Report 2024: Transformation of the Warehouse Sector through AI. *Fairwork Amazon 2024 Report Launch: How Is AI Transforming the Warehouse Sector*.

Wamba-Taguimdje, S.-L., Fosso Wamba, S., Kala Kamdjoug, J. R., & Tchatchouang Wanko, C. E. (2020). Influence of artificial intelligence (AI) on firm performance: The business value of AI-based transformation projects. *Business Process Management Journal*, *26*(7), 1893–1924.

Wang, K., Ma, Z., & Xia, Y. (2022). General strain theory and corruption among Grassroot Chinese public officials: A mixed-method study. *Deviant Behavior*, *43*(4), 472–489.

Winwood, P. C., Bakker, A. B., & Winefield, A. H. (2007). An investigation of the role of non–work-time behavior in buffering the effects of work strain. *Journal of Occupational and Environmental Medicine*, *49*(8), 862–871. 10.1097/JOM.0b013e318124a8dc

Yazdanmehr, A., Li, Y., & Wang, J. (2023). Employee responses to information security related stress: Coping and violation intention. *Information Systems Journal*. https://doi.org/10.1111/isj.12417

Yilmaz, K. (2013). Comparison of quantitative and qualitative research traditions: Epistemological, theoretical, and methodological differences. *European Journal of Education*, *48*(2), 311–325. https://doi.org/10.1111/ejed.12014

Zhang, R. Z., Kyung, E. J., Longoni, C., Cian, L., & Mrkva, K. (2025). AI-induced indifference: Unfair AI reduces prosociality. *Cognition*, *254*, 105937. https://doi.org/10.1016/j.cognition.2024.105937

Mitigating Insider Threats in Cybersecurity: A Design Thinking Approach

Emmanuel Anti[1], Rebekah Rousi [2,]

[1] *University of Vaasa, Wolffintie 34 65200, Vaasa, Finland*
[2] *University of Vaasa, Wolffintie 34 65200, Vaasa, Finland*

Abstract

Insider threats in cybersecurity (ITC) are increasing in frequency and impact, while current technical, psychological, and organizational approaches remain insufficient. These strategies often address narrow aspects like system vulnerabilities or individual behavior without offering a holistic, multidisciplinary solution. This study presents DESTIC, a design thinking (DT) framework to study insider threats. Unlike existing research emphasizing only the "Empathize" phase, DESTIC engages all six DT stages: empathize, define, ideate, prototype, test, and implement to uncover root causes and develop targeted interventions. We apply organizational design workshops, a methodology that combines diverse stakeholders to co-create solutions by examining behavioral, technical, and organizational factors. This study offers a structured, human-centered approach to understanding and proactively preventing insider threats through iterative, collaborative innovation in cybersecurity.

Keywords
Design thinking; insider threats; human-centered design; cybersecurity; framework

1. Introduction

Insider threats in cybersecurity are becoming more frequent and expensive, with malicious insider attacks now accounting for 7% of incidents and averaging USD 4.99 million in damages [1]. Unlike external threats, insiders are trusted personnel with legitimate access, making their actions, whether intentional or accidental, particularly harmful and harder to detect [2], [3]. From 2019 to 2024, insider attacks rose from 66% to 76%, with financial gain as the top motivation increasing from 60% to 74% [4]. These threats can take various forms, including sabotage, data theft, unauthorized sharing, and policy violations, often remaining undetected for an average of 308 days [1].

Insider threats can lead to financial losses, legal consequences, reputational harm, and internal distrust, damaging both an organization's external standing and internal culture [5], [6], [7], [8], [9]. Despite traditional security measures like access controls, monitoring, and awareness training, insider threats persist due to organizational culture, evolving threat dynamics, and complex human motivations [10], [11]. These gaps call for more adaptive, human-focused strategies.

This study proposes applying human-centered design (HCD), specifically design thinking (DT), to insider threat mitigation. In Information Systems, systems thinking – "a system of thinking about systems" [94] – has been a popular paradigm for approaching the study of threats [12], [13], [14]. However, rather than focusing on the systems per se, DT centers on human behavior, needs, and motivations through a transdisciplinary, empathy-driven, and creative

TKTP 2025: Annual Doctoral Symposium of Computer Science, 2.-3.6.2025 Helsinki, Finland

emmanuel.anti@uwasa.fi (E. Anti); rebekah.rousi@uwasa.fi (R. Rousi)
0009-0007-3802-4875 (E. Anti); 0000-0001-5771-3528 (R. Rousi)

approach [15],[16],[17], that not only accounts for systems or actor networks, but also thought processes within these dynamic relations. DT offers a psychologically grounded, multidisciplinary method for understanding the human factors that drive insider actions and designing responses accordingly [18].

The guiding question is: How can design thinking be applied to develop effective proactive strategies for preventing insider threats while offering a deeper understanding of previous cases? This study explores DT's potential to map insider agents' emotional and cognitive dimensions and introduces the DESTIC framework—a human-centered model integrating psychological, social, and environmental insights to create actionable, adaptive strategies for preventing insider threats.

2. Literature Review

Research in insider threats has spanned technological, psychological, and organizational domains, yet these threats remain a persistent concern for organizations. Despite extensive efforts by governments, academics, and research institutions, much of the existing research is anecdotal or based on limited data, resulting in fragmented mitigation strategies [11]. Tools supported by generative AI, such as personas, depend heavily on the quality of user data and research inputs [19], [20]. Consequently, insider threat mitigation remains split between purely technical approaches and broader socio-technical methods [21],22], [23],[24].

2.1. Technical Approaches

Technical approaches focus on policies, system specifications, and controls to detect or prevent insider activity [11]. These include user activity monitoring, intrusion detection systems (IDS), and VPN analysis [25], [26]. For example, Wasko et al. [27] used reality games to simulate insider threats and observed increased deviant behavior in controlled environments. Emerging methods like deep learning enhance detection by analyzing large datasets for subtle behavioral changes [28]. However, these models face limited labeled data, difficulty detecting adaptive behavior, and distinguishing malicious from accidental threats [28], [29].

2.2. Socio-Technical Approaches

Socio-technical strategies integrate human and technical elements, combining rules, training, behavioral monitoring, and organizational culture assessment [10], [30]. Anomaly detection and machine learning help build dynamic user profiles [19]. Despite these strengths, limitations include high implementation costs, difficulty addressing individual motivations, and challenges distinguishing between different types of insider threats [10], [29]. Human-based attacks like social engineering can also bypass technological defenses as technological solutions cannot fully address the social dimension of insider threats [31].

2.3. Social, Psychological, and Organizational Approaches

These approaches examine insider behavior's social and psychological drivers, such as personal stress, entitlement, or workplace dissatisfaction [7], [32]. Theories like deterrence and rational choice have been applied to understand factors contributing to insider threats [33], [34], [35], [36], [37]. However, these methods can be resource-intensive, assume uniform employee responses, and may fail without strong managerial enforcement [37], [38]. Their subjective nature can also lead to bias or misinterpretation, and they may miss threats posed by

unintentional actors or those outside typical profiles [32], [37]. These approaches offer insight into human and organizational factors but are often ineffective without technical support.

2.4. Previous research on Design Thinking in Cybersecurity

While systems thinking is well-established in cybersecurity, design thinking (DT) remains underutilized. Some researchers, however, have begun to apply DT in this space. For example, Dorasamy et al. [39] used DT to address IoT-related cybersecurity issues among youths, generating insights, solutions, a prototype, and feedback. Snow et al. [40] applied DT and behavioral theory to identify key smart grid threats through expert workshops, referencing Nykodym et al. [41] insider threat profiles and Fogg's [42] behavior model. Tseng et al. [43] developed a cybersecurity board game using DT to enhance student awareness in education. Ashenden et al. [44] used DT to design cyber deception tools, producing journey maps that visualized tactics and guided evaluation discussions.

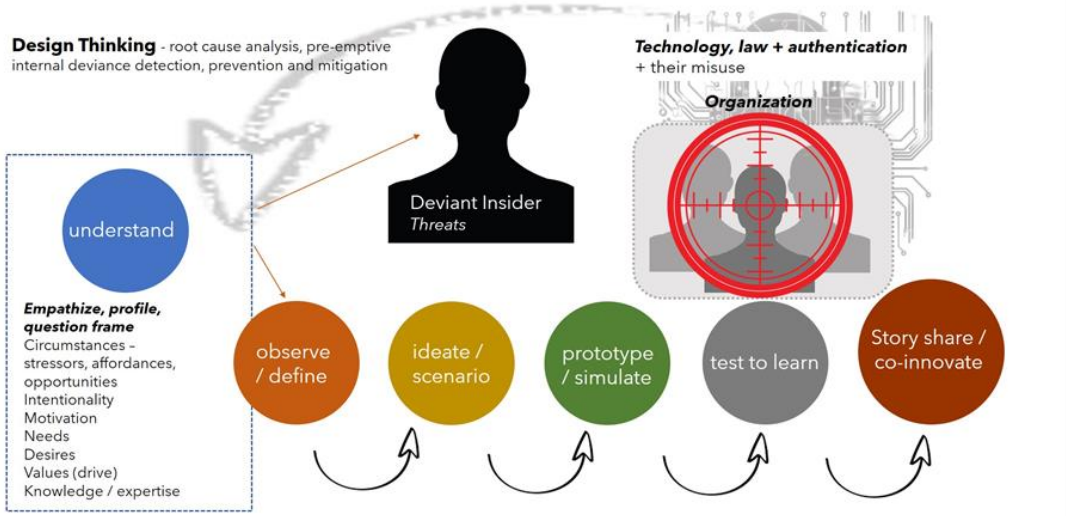

Fig. 1. Design Thinking for ITC framework – DESTIC – the framework offers an order of process from developing an intial understanding of the situation (Understand stage) to observing and defining, ideating and scenario-building, prototyping and simulating, testing and learning, then the official outward communication stage of story sharing and further co-innovation. The process can be implemented in iterative cycles, and the objective is to use each stage with its increasing fidelity as a means of generating more detailed strategic insight on what is happening and can happen, where, and how it can be addressed.

2.5. Design Thinking - From Forensics to Process

In cybersecurity, digital and traditional forensic methods, including psychological profiling, are widely applied [5], [6], [7]. Nevertheless, digital forensics faces challenges such as big data, tool diversity, encryption, legal complexities, and shortages of skilled professionals [48]. As socio-technical systems grow more complex, managing insider threats demands interdisciplinary expertise. No single individual can address all aspects of socio-technical deviance, underscoring the need for multi-professional collaboration. We propose DT as a structured, transdisciplinary approach to address this. Developed by John E. Arnold at Stanford to reduce bias and foster creativity across disciplines [49],[8], [9], [10], DT has evolved through contributions from Dreyfuss, Maslow, Kahn, and Guilford, emphasizing collaboration and tool-based exploration [16], [53], [54]. Grounded in empathy, it isolates creativity blocks that may serve as deviant trajectories, like stress and fear of failure, through iterative, human-focused methods [50], [55]. This study introduces DESTIC (Figure 1), an adapted six-step DT framework for insider threat mitigation in ITCs, enabling root cause analysis and proactive prevention [58].

2.5.1. Understand

To identify the "what" of insider threats, a systematic review by Anti & Vartiainen [59] identifies ten types of insider deviant behaviors, including computer abuse, fraud, IS misuse, policy violations, shadow IT, unauthorized disclosure, and access breaches. However, recognizing these behaviors is only the first step. Understanding insider threats also requires examining individual motivations and external factors such as stressors, technological affordances, and situational opportunities. Organizations must assess human elements like values, beliefs, expertise, and cultural health [59]. Insider risk may also arise from underutilized or disengaged employees who feel undervalued or bored, increasing the likelihood of deviant behavior [60], [61].

2.5.2. Observe/ Define

The observing and defining stage involves analyzing organizational and individual behaviors to uncover factors contributing to insider deviance. Key organizational factors include culture [11], [12], [13], formal and informal controls [65],[66],[67], fairness and justice [68],[69],[70], clear policy enforcement [68], [69], [71], and organizational citizenship [72]. From a psychological perspective, it is essential to assess stress triggers [65], [73], sense of responsibility [74],[75], boundary management [76],[77], and goal framing [78],[79]. Additionally, socio-cultural influences—such as social bonds, cultural norms, and controls [63], [68], [75]—and emotional coping behaviors [59] should be mapped to identify the root causes of deviance.

2.5.3. Ideate / Scenario

In the ideation phase, the investigator(s) – team, strategists – endeavor to list different ideas of matters that can go wrong from an internal information security perspective and map relationships between these ideas and various factors. Ideally, the team will arrive at a stage in which they create storyboards or 'scenarios' in which individuals, their environments, and socio-technical conditions may lead to deviant behavior and potential risk. This process stage involves divergent creative thinking when the team can generate as many ideas as possible that do not necessarily need to be entirely credible, possible, or feasible [14]. The main aim is to gather a spectrum of ideas from the highly likely to the highly unlikely (as yet), which can form the basis of ascertaining current state-of-the-art in internal socio-technical deviance and may also prepare the team for future roadmapping.

2.5.4. Prototype / Simulate

The prototype or simulate stage involves simulation or enactment – i.e., testing the systems and qualified individuals (i.e., recruiting individuals with technical and cyber security expertise) to understand how these high-level ideas and scenarios may unfold in practice. The prototyping phase provides an actionable communicational platform for testing and learning [15]. Prototyping is not simply a mode of actualizing ideas and plans in concrete form but is an extension of cognition itself [16], [17]. We may see that through producing prototypes and simulations, practitioners can further understand the motives, materials, and possibilities of deviant insiders (i.e., via simulation-enabled shared cognition, see [18], [19]). The aim is to cause as much damage as possible in a safe and controlled way. The prototype or simulation should be developed to a standard that allows the development team and bystanders (i.e., stakeholders) to envision realistically how the behavior and its causalities can be realized in practice.

2.5.5. Test to Learn

Testing comes into play with other expert and non-expert communities. Other experts can pinpoint the preciseness and likelihood of particular scenarios. They can also highlight unaccounted-for challenges while critiquing vulnerabilities within the present simulations. On the other hand, the non-experts may highlight blind spots incurred by expertise – i.e., fixation on specific details while people with expertise in other fields and experiences may notice other details. The non-expert community is also valuable from an educational perspective. The learning they undergo while witnessing the unfolding of information security breaches will undoubtedly be enlightening in shaping their behavior. This learning will have additional social benefits in that insight may be shared with colleagues after the simulation experiences (i.e., social learning [20].

2.5.6. Story Share / Co-Innovate

At this stage, learning and innovation intersect. When teams and stakeholders engage in both the DT process and testing, they gain shared insight into insider threats and the environments that enable it, enabling co-innovation [17], [87]. Scenarios and mock-ups become reference points for focused, convergent ideation—bringing together the findings of DT in a meaningful way. The resulting design solution is only part of the outcome. Equally important is communicating its root causes: what problems it addresses and how. Storytelling plays a critical role in this meaning-making process, helping translate complex findings into accessible narratives for non-experts [88]. It raises awareness of how insider threats emerge and how socio-technical systems can address them, fostering broader engagement in cybersecurity practices.

For these solutions to have a lasting impact, they must support co-innovation and contribute to culture generation within organizations [89].

3. Proposed Methodology

This study will adopt a qualitative, exploratory methodology using organizational design workshops to investigate insider threats through a human-centered DT lens. Design workshops are particularly suited for socio-technical IS research and development, offering a collaborative space to engage diverse stakeholders in structured problem-solving while serving as a focus group to identify concerns, vulnerabilities, and structural challenges [90], [91]. These workshops enable the application of DT tools such as empathy mapping, journey mapping, and root cause analysis to surface complex behavioral and organizational dynamics underlying insider threats.

The study will be implemented in three main phases over twelve months. After the initial planning, preparation, and recruitment phase that includes the development of the workshop materials and protocols based on the proposed framework (DESTIC) and established DT practices, piloting the design, securing partnerships with four organizations in high-risk sectors such as finance, healthcare, or public institutions in Finland, the process with launch into the exploratory phase. A multidisciplinary group of participants of five to ten individuals (Cybersecurity experts, IT professionals, managers, HR personnel, general employees, cognitive psychologists, and behavioral experts) from the partner organizations and specialist organizations will be recruited. This multi-professional group will help generate rich, contextual insights aligning with IS research goals of theory-building, system design, and actionable socio-technical innovation [93].

The second phase is expected to take five months, where one intensive design workshop, lasting one full day, will be organized for each organization. Each session will consist of iterative ideation, prototyping, feedback, and refinement sprints. Participants will engage with DT tools such as empathy mapping, journey mapping, root cause analysis, and persona building to explore

and reframe complex behavioral and organizational dynamics underlying insider threats. Focus groups and forensic-style inquiry sessions will further deepen understanding of behaviors, motivations, and systemic vulnerabilities. The iterative format will enable rapid testing and evolution of ideas within each session, creating space for participants to refine interventions in response to group feedback and emergent insights. All sessions will be documented through recordings, field notes, and workshop artifacts such as sketches, models, and system maps.

Thematic and qualitative profiling will be applied to analyze the data, which will take three months. Triangulation across roles, organizations, and data types will support the development of grounded theories and practical models for managing insider threats. The iterative workshop design ensures that emerging findings are shaped collaboratively and refined in real time, strengthening their relevance and applicability. A socio-technical map of possible solutions that adequately address root causes and threat networks will be a key deliverable from this phase.

3.1. Feasibility

The study is designed to be practical, feasible, and directly contribute to scientific advancement and applicable socio-technical solutions (key technologies, guidelines, protocol, etc.). It requires the modest resources of a facilitation team (two to three members), basic materials (sticky notes, markers, whiteboards, or large flip charts), and reasonable logistical support from partner organizations. This support includes providing a physical or virtual space to hold the workshop, allocating employee time to participate (one full day), and granting access to relevant contextual information such as organizational policies, workflows, or anonymized incident data that can inform the design work. The most challenging component could be the allocation of employee time. Nevertheless, several solutions may be found to aid this challenge, such as utilizing the process for *professional development* and even team-building. Most pertinent is calculating the return on investment for potential savings of internal deviance incidents versus the costs of engaging several staff members in intensive research and development. This is essential for meaningful participation and scientifically and professionally grounded results.

4. Expected Contributions and Conclusions

This paper deliberates how Design Thinking (DT) can be applied in cybersecurity to proactively design, mitigate, and prevent insider threats. By leveraging DT's human-centered, multidisciplinary structure, we propose a framework (DESTIC) for addressing insider socio-technical deviance through convergent and divergent creativity, including the underexplored area of deviant creativity. Deviant creativity suggests that individuals who engage in deviance often think creatively, using novel ways to combine information for deception and stay ahead[95]. Our adapted "understand" phase synthesizes behavioral and motivational theories to uncover the conditions that enable insider threats, building on prior DT applications in cybersecurity [39], [43], [44]. We argue that DT's iterative, transdisciplinary collaborative process is uniquely positioned to anticipate future insider threats and co-create preventive solutions with diverse stakeholders. Additionally, we highlight the crucial interplay of technology, law, and authentication, particularly as emerging technologies outpace legal frameworks. DT can assist not only in identifying vulnerabilities but also in shaping adaptive legal and regulatory responses. Ultimately, we position DT as a diagnostic and generative tool for advancing anti-threat innovation in cybersecurity.

Declaration on Generative AI

The author(s) used Grammarly for grammar and spelling checks, followed by manual review and editing. They take full responsibility for the final content.

References

[1] IBM and Ponemon Institute, "Cost of a Data Breach Report 2024," 2024. Accessed: Sep. 17, 2024. [Online]. Available: https://www.ibm.com/reports/data-breach

[2] M. Bishop and C. Gates, "Defining the insider threat," in 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, 2008, pp. 1–3.

[3] C. Colwill, "Human factors in information security: The insider threat–Who can you trust these days?," Information security technical report, vol. 14, no. 4, pp. 186–196, 2009.

[4] Cybersecurity Insiders, "Insider Threat Report Trends, Challenges, and Solution," 2024. Accessed: Feb. 23, 2024. [Online]. Available: www.securonix.com

[5] J. R. Nurse et al., "Understanding insider threat: A framework for characterising attacks," in 2014 IEEE security and privacy workshops, IEEE, 2014, pp. 214–228.

[6] S. Duggineni, "Impact of controls on data integrity and information systems," Science and Technology, vol. 13, no. 2, pp. 29–35, 2023.

[7] F. Khan, J. H. Kim, L. Mathiassen, and R. Moore, "Data breach management: An integrated risk model," Information & Management, vol. 58, no. 1, p. 103392, 2021.

[8] J. D'Arcy, I. Adjerid, C. M. Angst, and A. Glavas, "Too good to be true: Firm social performance and the risk of data breach," Information Systems Research, vol. 31, no. 4, pp. 1200–1223, 2020.

[9] A. H. Juma'h and Y. Alnsour, "The effect of data breaches on company performance," International Journal of Accounting & Information Management, vol. 28, no. 2, pp. 275–301, 2020.

[10] N. Saxena, E. Hayes, E. Bertino, P. Ojo, K.-K. R. Choo, and P. Burnap, "Impact and key challenges of insider threats on organizations and critical businesses," Electronics, vol. 9, no. 9, p. 1460, 2020.

[11] J. Hunker and C. W. Probst, "Insiders and Insider Threats: An Overview of Definitions and Mitigation Techniques," Journal of Wireless Mobile Networks, Ubiquitous Computing and Dependable Applications, vol. 2, no. 1, pp. 4–27, 2011.

[12] H. M. Salim, "Cyber safety: A systems thinking and systems theory approach to managing cyber security risks," PhD Thesis, Massachusetts Institute of Technology, 2014.

[13] E. Zoto, M. Kianpour, S. J. Kowalski, and E. A. Lopez-Rojas, "A socio-technical systems approach to design and support systems thinking in cybersecurity and risk management education," Complex Systems Informatics and Modeling Quarterly, no. 18, pp. 65–75, 2019.

[14] W. Young and N. Leveson, "Systems thinking for safety and security," in Proceedings of the 29th annual computer security applications conference, 2013, pp. 1–8.

[15] D. Norman, The design of everyday things: Revised and expanded edition. Basic books, 2013.

[16] T. Brown, "Change by design: How design thinking creates new alternatives for business and society," Collins Business, 2009.

[17] J. Liedtka, "Why design thinking works," Harvard Business Review, vol. 96, no. 5, pp. 72–79, 2018.

[18] N. Liang, D. P. Biros, and A. Luse, "An empirical validation of malicious insider characteristics," Journal of Management Information Systems, vol. 33, no. 2, pp. 361–392, 2016.

[19] E. Kim, J. Yoon, J. Kwon, T. Liaw, and A. M. Agogino, "From innocent irene to parental patrick: Framing user characteristics and personas to design for cybersecurity," in Proceedings of the Design Society: International Conference on Engineering Design, Cambridge University Press, 2019, pp. 1773–1782.

[20] D. Ki-Aries and S. Faily, "Persona-centred information security awareness," Computers & security, vol. 70, pp. 663–674, 2017.

[21] R. A. Alsowail and T. Al-Shehari, "A multi-tiered framework for insider threat prevention," Electronics, vol. 10, no. 9, p. 1005, 2021.

[22] R. A. Alsowail and T. Al-Shehari, "Empirical detection techniques of insider threat incidents," IEEE Access, vol. 8, pp. 78385–78402, 2020.

[23] D. M. Cappelli, A. P. Moore, and R. F. Trzeciak, The CERT guide to insider threats: how to prevent, detect, and respond to information technology crimes (Theft, Sabotage, Fraud). Addison-Wesley, 2012.

[24] M. Jeong and H. Zo, "Preventing insider threats to enhance organizational security: The role of opportunity-reducing techniques," Telematics and Informatics, vol. 63, p. 101670, 2021.

[25] M. Mohammadi et al., "A comprehensive survey and taxonomy of the SVM-based intrusion detection systems," Journal of Network and Computer Applications, vol. 178, p. 102983, 2021.

[26] N. Elmrabit, S.-H. Yang, and L. Yang, "Insider threats in information security categories and approaches," in 2015 21st International Conference on Automation and Computing (ICAC), IEEE, 2015, pp. 1–6.
[27] S. Wasko et al., "Using alternate reality games to find a needle in a haystack: An approach for testing insider threat detection methods," Computers & Security, vol. 107, p. 102314, 2021.
[28] S. Yuan and X. Wu, "Deep learning for insider threat detection: Review, challenges and opportunities," Computers & Security, vol. 104, p. 102221, 2021.
[29] A. Akhunzada et al., "Man-At-The-End attacks: Analysis, taxonomy, human aspects, motivation and future directions," Journal of Network and Computer Applications, vol. 48, pp. 44–57, 2015.
[30] E. Mumford, "A socio-technical approach to systems design," Requirements engineering, vol. 5, pp. 125–133, 2000.
[31] N. Elmrabit, "A multiple-perspective approach for insider-threat risk prediction in cyber-security.," PhD Thesis, Loughborough University, 2018.
[32] I. Homoliak, F. Toffalini, J. Guarnizo, Y. Elovici, and M. Ochoa, "Insight into insiders and it: A survey of insider threat taxonomies, analysis, modeling, and countermeasures," ACM Computing Surveys (CSUR), vol. 52, no. 2, pp. 1–40, 2019.
[33] J. P. Gibbs, "Crime, punishment, and deterrence," The Southwestern Social Science Quarterly, pp. 515–530, 1968.
[34] J. J. van Dijk, "Understanding crime rates: On the interactions between the rational choices of victims and offenders," The British Journal of Criminology, vol. 34, no. 2, pp. 105–121, 1994.
[35] R. M. Hogarth and M. W. Reder, Rational choice: The contrast between economics and psychology. University of Chicago Press, 1987.
[36] E. D. Shaw, "The role of behavioral research and profiling in malicious cyber insider investigations," Digital investigation, vol. 3, no. 1, pp. 20–31, 2006.
[37] N. S. Safa, C. Maple, T. Watson, and R. Von Solms, "Motivation and opportunity based model to reduce information security insider threats in organisations," Journal of information security and applications, vol. 40, pp. 247–257, 2018.
[38] Y. Chen, K. Ramamurthy, and K.-W. Wen, "Organizations' information security policy compliance: Stick or carrot approach?," Journal of Management Information Systems, vol. 29, no. 3, pp. 157–188, 2012.
[39] M. Dorasamy, G. C. Joanis, L. W. Jiun, M. Jambulingam, R. Samsudin, and N. J. Cheng, "Cybersecurity issues among working youths in an IOT environment: A design thinking process for solution," in 2019 6th International Conference on Research and Innovation in Information Systems (ICRIIS), IEEE, 2019, pp. 1–6.
[40] S. Snow, J. Happa, N. Horrocks, and M. Glencross, "Using design thinking to understand cyber-attack surfaces of future smart grids," Frontiers in Energy Research, vol. 8, p. 591999, 2020.
[41] N. Nykodym, R. Taylor, and J. Vilela, "Criminal profiling and insider cyber-crime," Computer Law & Security Review, vol. 21, no. 5, pp. 408–414, 2005.
[42] B. J. Fogg, "A behavior model for persuasive design," in Proceedings of the 4th international Conference on Persuasive Technology, 2009, pp. 1–7.
[43] S.-S. Tseng, T.-Y. Yang, Y.-J. Wang, and A.-C. Lu, "Designing a cybersecurity board game based on Design Thinking Approach," in Innovative Mobile and Internet Services in Ubiquitous Computing: Proceedings of the 12th International Conference on Innovative Mobile and Internet Services in Ubiquitous Computing (IMIS-2018), Springer, 2019, pp. 642–650.
[44] D. Ashenden, R. Black, I. Reid, and S. Henderson, "Design thinking for cyber deception," Proceedings of the 54th Hawaii International Conference on System Sciences | 2021., 2021, [Online]. Available: http://hdl.handle.net/10125/70853
[45] E. Casey, Handbook of digital forensics and investigation. Academic Press, 2009.
[46] M. Pollitt, "A history of digital forensics," in Advances in Digital Forensics VI: Sixth IFIP WG 11.9 International Conference on Digital Forensics, Hong Kong, China, January 4-6, 2010, Revised Selected Papers 6, Springer, 2010, pp. 3–15.
[47] A. Årnes, Digital forensics. John Wiley & Sons, 2017.
[48] N. M. Karie and H. S. Venter, "Taxonomy of challenges for digital forensics," Journal of forensic sciences, vol. 60, no. 4, pp. 885–893, 2015.

[49] V. P. Seidel and S. K. Fixson, "Adopting design thinking in novice multidisciplinary teams: The application and limits of design methods and reflexive practices," Journal of Product Innovation Management, vol. 30, pp. 19–33, 2013.
[50] J. Auernhammer and B. Roth, "The origin and evolution of Stanford University's design thinking: From product design to design thinking in innovation management," Journal of Product innovation management, vol. 38, no. 6, pp. 623–644, 2021.
[51] R. F. Dam, "The 5 Stages in the Design Thinking Process |." 2024. Accessed: Jan. 01, 2024. [Online]. Available: https://www.interaction-design.org/literature/article/5-stages-in-the-design-thinking-process?srsltid=AfmBOopucCptPkYIIiO9iIrS_8eBUdDXuhDPdopXA24dZL1b4rOpAeLL
[52] U. Johansson-Sköldberg, J. Woodilla, and M. Çetinkaya, "Design thinking: Past, present and possible futures," Creativity and innovation management, vol. 22, no. 2, pp. 121–146, 2013.
[53] K. Dorst, "The core of 'design thinking'and its application," Design studies, vol. 32, no. 6, pp. 521–532, 2011.
[54] T. Kelley, The art of innovation: Lessons in creativity from IDEO, America's leading design firm, vol. 10. Currency, 2001.
[55] A. Dix, "What are Creative Blocks? Interaction Design Foundation." 2016. Accessed: Sep. 23, 2024. [Online]. Available: https://www.interaction-design.org/literature/topics/creative-block
[56] IDEO, "The Design Thinking Process (6 Helpful Steps) –." Accessed: Oct. 01, 2024. [Online]. Available: https://www.ideou.com/blogs/inspiration/design-thinking-process
[57] S. Gibbons, "Design Thinking 101." 2016. Accessed: Sep. 26, 2024. [Online]. Available: https://www.nngroup.com/articles/design-thinking/
[58] N. Hellesen, H. Torres, and G. Wangen, "Empirical case studies of the root-cause analysis method in information security," International Journal on Advances in Security, vol. 11, 2018.
[59] E. Anti and T. Vartiainen, "Explanations of Insider Deviant Behavior in Information Security: A Systematic Literature Review," Association for Information Systems, 2024.
[60] D. Livingstone, "Skill underutilization," in The Oxford handbook of skills and training, Oxford University Press Oxford, 2017, pp. 281–300.
[61] T. A. Sullivan, Marginal workers, marginal jobs: underutilization in the United States labor force. The University of Chicago, 1975.
[62] D. Box and D. Pottas, "A model for information security compliant behaviour in the healthcare context," Procedia Technology, vol. 16, pp. 1462–1470, 2014.
[63] L. Y. Connolly, M. Lang, J. Gathegi, and D. J. Tygar, "Organisational culture, procedural countermeasures, and employee security behaviour: A qualitative study," Information & Computer Security, vol. 25, no. 2, pp. 118–136, 2017.
[64] S. Hina, D. D. D. P. Selvam, and P. B. Lowry, "Institutional governance and protection motivation: Theoretical insights into shaping employees' security compliance behavior in higher education institutions in the developing world," Computers & Security, vol. 87, p. 101594, 2019.
[65] J. D'Arcy and P.-L. Teh, "Predicting employee information security policy compliance on a daily basis: The interplay of security-related stress, emotions, and neutralization," Information & Management, vol. 56, no. 7, p. 103151, 2019.
[66] P. Ifinedo and E. C. Idemudia, "Factors influencing employees' participation in non-malicious, information systems security deviant behavior: Focus on formal control mechanisms and sanctions," 2017.
[67] X. R. Luo, H. Li, Q. Hu, and H. Xu, "Why individual employees commit malicious computer abuse: A routine activity theory perspective," Journal of the Association for Information Systems, vol. 21, no. 6, p. 5, 2020.
[68] P. B. Lowry, C. Posey, R. (Becky) J. Bennett, and T. L. Roberts, "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, vol. 25, no. 3, pp. 193–273, 2015.
[69] R. Willison, M. Warkentin, and A. C. Johnston, "Examining employee computer abuse intentions: Insights from justice, deterrence and neutralization perspectives," Information Systems Journal, vol. 28, no. 2, pp. 266–293, 2018.
[70] A. Nehme and J. George, "Taking it out on IT: A Mechanistic Model of Abusive Supervision and Computer Abuse," 2020.

[71] S. Farshadkhah, C. Van Slyke, and B. Fuller, "Onlooker effect and affective responses in information security violation mitigation," Computers & Security, vol. 100, p. 102082, 2021.
[72] P. Ifinedo, "Effects of organizational citizenship behavior and social cognitive factors on employees' non-malicious counterproductive computer security behaviors: an empirical analysis," 2015.
[73] A. Yazdanmehr, Y. Li, and J. Wang, "Employee responses to information security related stress: Coping and violation intention," Information Systems Journal, 2023.
[74] K. A. Alshare, P. L. Lane, and M. R. Lane, "Information security policy compliance: a higher education case study," Information & Computer Security, vol. 26, no. 1, pp. 91–108, 2018.
[75] A. Yazdanmehr and J. Wang, "Can peers help reduce violations of information security policies? The role of peer monitoring," European Journal of Information Systems, vol. 32, no. 3, pp. 508–528, 2023.
[76] R. Willison and J. Backhouse, "Opportunities for computer crime: considering systems risk from a criminological perspective," European Journal of Information Systems, vol. 15, no. 4, pp. 403–414, 2006.
[77] V.-H. Trieu, V. Cooper, and D. Pallegedara, "Employee's Unauthorized Disclosure of Organizational Information on Social Media: The Role of Emotions and Boundary Permeability," in Proceedings of the 42nd International Conference on Information Systems (ICIS 2021), Association of Information Systems, 2021, pp. 1–9.
[78] P. Ifinedo, "Exploring Personal and Environmental Factors that Can Reduce Nonmalicious Information Security Violations," Information Systems Management, pp. 1–21, 2022.
[79] J. J. Kim, E. H. E. Park, and R. L. Baskerville, "A model of emotion and computer abuse," Information & Management, vol. 53, no. 1, pp. 91–108, 2016.
[80] M. A. Runco and others, "Divergent thinking, creativity, and ideation," The Cambridge handbook of creativity, vol. 413, p. 446, 2010.
[81] P. Newman, M. A. Ferrario, W. Simm, S. Forshaw, A. Friday, and J. Whittle, "The Role of Design Thinking and Physical Prototyping in Social Software Engineering".
[82] J. M. Carroll, "Scenario-based design," in Handbook of human-computer interaction, Elsevier, 1997, pp. 383–406.
[83] C. A. Lauff, D. Kotys-Schwartz, and M. E. Rentschler, "What is a Prototype? What are the Roles of Prototypes in Companies?," Journal of Mechanical Design, vol. 140, no. 6, p. 061102, 2018.
[84] J. J. Zigmont, L. J. Kappus, and S. N. Sudikoff, "Theoretical foundations of learning through simulation," in Seminars in perinatology, Elsevier, 2011, pp. 47–51.
[85] C. S. Witt, "Instructional* simulations and the concepts of shared cognition," [Doctoral Dissertation]University of Nevada, Las Vegas, 2008, [Online]. Available: https://digitalscholarship.unlv.edu/cgi/viewcontent.cgi?article=3859&context=rtds
[86] A. Bandura, "Social learning theory.," Englewood Cliffs, NJ: Prentice Hall, 1977.
[87] A. Cropley, "In praise of convergent thinking," Creativity research journal, vol. 18, no. 3, pp. 391–404, 2006.
[88] K. Stapleton and J. Wilson, "Telling the story: Meaning making in a community narrative," Journal of Pragmatics, vol. 108, pp. 60–80, 2017.
[89] J. Leikas, Life-based design: a holistic approach to designing human-technology interaction. VTT Technical Research Centre of Finland, 2009.
[90] K. Bødker, F. Kensing, and J. Simonsen, "Participatory design in information systems development," Reframing humans in information systems development, pp. 115–134, 2011.
[91] P. Dalsgaard and K. Halskov, "Innovation in participatory design," in Proceedings of the 11th Biennial Participatory Design Conference, 2010, pp. 281–282.
[92] J. Simonsen and T. Robertson, Routledge international handbook of participatory design, vol. 711. Routledge New York, 2013.
[93] M. K. Sein, O. Henfridsson, S. Purao, M. Rossi, and R. Lindgren, "Action design research," MIS quarterly, pp. 37–56, 2011.
[94] R. D. Arnold and J. P. Wade, "A definition of systems thinking: A systems approach," Procedia computer science, vol. 44, pp. 669–678, 2015.
[95] H. Kapoor, "Shining a light on dark creativity," *Creativity Research Journal*, vol. 37, no. 2, pp. 236–241, 2025.