31e Conférence de l'Association Information et Management

20-22 mai 2026 à Neuchâtel (CH)

Comprendre la menace interne : une perspective dyadique de l'(in)adéquation organisation-employé

Aymeric MAILLER, HEC Montréal, Canada

Alina Maria DULIPOVICI, HEC Montréal, Canada

Ryad TITAH, HEC Montréal, Canada

Résumé

La menace interne reste un défi central en sécurité de l'information car l'ubiquité technologique brouille les frontières entre travail légitime, pratiques parallèles et déviance. Dans cette littérature, la lacune théorique tient à l'incapacité des approches linéaires principalement fondées sur la dissuasion à expliquer la diversité des comportements des employés légitimes. Cet article reconceptualise les comportements liés à la sécurité comme une propriété émergente de la dyade organisation-employé, via la théorie des parties prenantes. Sa logique configurationnelle théorique croise deux dimensions orthogonales (congruence des valeurs et complémentarité stratégique) pour générer quatre configurations : protection proactive, non-conformité bienveillante, abus instrumental et abus malveillant. Le cadre distingue contournement, opportunisme et hostilité, puis propose trois réponses managériales : reconception sociotechnique, gouvernance ciblée ou intervention corrective. En proposant une théorie SI de moyenne portée, cette recherche enrichit le champ et invite à remplacer les sanctions indifférenciées par un ajustement des outils, règles et valeurs.

Mots clés

Menace interne ; Comportements des employés liés à la sécurité de l'information ; Adéquation organisation-employé ; Théorie configurationnelle ; Adéquation / inadéquation

Understanding the insider threat: a dyadic organization-employee fit/misfit perspective

Abstract

The insider threat remains a central challenge in information security, as technological ubiquity blurs the boundaries between legitimate work, parallel practices, and deviance. In this literature, the theoretical gap lies in the inability of dominant linear approaches primarily based on deterrence to explain the diversity of behaviors enacted by legitimate employees. This article reconceptualizes these security behaviors as an emergent property of the dyadic organization-employee relationship, drawing on stakeholder theory. Its theoretical configurational logic intersects two orthogonal dimensions, value congruence and strategic complementarity, yielding four configurations: proactive protection, benign non-compliance, instrumental abuse, and malicious abuse. The framework distinguishes circumvention, opportunism, and hostility, then proposes three managerial responses: socio-technical redesign, targeted governance, or corrective intervention. By proposing a mid-range IS theory, this research advances the field and invites replacing undifferentiated sanctions with an adjustment of tools, rules and values.

Keywords

Insider threat; Security-related employee behaviors; Organization–employee fit; Configurational theory; Fit / misfit

1. Introduction

The ubiquitous integration of information technology has positioned employees as a central locus of information security risk, blurring the boundary between legitimate work, parallel practices and deviant behavior (Posey et al., 2013). Although organizations deploy extensive detection and response infrastructures, insider security incidents persist and continue to threaten business continuity, with organizational costs reaching an average of $4.92 million per incident (IBM Corporation, 2025). This persistence highlights a structural challenge that is both theoretically significant and practically consequential: decision-makers face the challenge of securing organizational assets without paralyzing productivity, while the theoretical understanding of how legitimate employees become threats remains fragmented (Posey et al., 2013; Malaurent & Karanasios, 2020). Insiders generally possess privileged access and situated knowledge that may facilitate circumvention or abuse (Magklaras & Furnell, 2005; Zeadally et al., 2012). This intrinsic threat cannot be addressed through technical controls alone; it calls for a fundamental theorization of employees' security-related behaviors within organizations, coupled with practical utility for the protection of vital assets (Posey et al., 2013).

Information Systems research has explored this phenomenon through multiple theoretical traditions, predominantly led by general deterrence theory, which generally posits that governance based on the severity and certainty of sanctions aims to reduce deviance intentions (Silic et al., 2017). Concurrently, other streams mobilize self-determination theory to suggest that the internalization of ethical norms and intrinsic satisfaction foster proactive compliance (Hong & Xu, 2021; X. Chen et al., 2025). In parallel, studies on workarounds and Shadow Information Technology (IT) reveal that many security violations do not stem from deliberate malice, but often constitute pragmatic adaptations by employees attempting to compensate for the functional inadequacy of infrastructures to maintain the firm's performance objectives (Silic et al., 2017). However, despite these significant advances, the literature often remains structured around conceptual frameworks that postulate linear causal relationships and that contrast benevolent deviance with sabotage (Silic & Back, 2014; Silic et al., 2017). This division across research streams constitutes a theoretical limitation, as it often relies on an assumption of behavioral symmetry wherein the absence of deterrent controls would inevitably lead to malice (Siponen & Vance, 2010). Yet, the interaction at a strategic level between the employee and the information system appears to operate through an asymmetrical and combinatorial dynamic where technological structures, business processes and normative values form an interwoven network of fit and misfit (Bartelheimer et al., 2023).

To address these limitations, the objective of this paper is to advance a conceptual framework explaining the emergence of different forms of insider threats as the result of specific causal configurations linking the technological infrastructure and the organizational normative foundation (Zeadally et al., 2012). By explicitly positioning itself as a theory for explaining (Gregor, 2006), this research aims to explain how, why, when and where the alignment or rupture of the dyadic relationship between the organization and the employee might generate asymmetrical behavioral responses (Burns et al., 2023).

The contribution of this paper thus operates along two complementary axes, merging theoretical originality and prescriptive utility (Burns et al., 2023). Conceptually, the study introduces a

configurational perspective that complements variance-based approaches by anchoring itself in the principles of causal complexity and equifinality (Sun et al., 2024). By theorizing that postures ranging from operational circumvention to deliberate sabotage may be structured by distinct amalgams of instrumental inadequacy and value disengagement, our approach seeks to reconcile the existing tensions in the literature under a unified structural lens (Fürstenau et al., 2021). Pragmatically, this conceptualization provides IT decision-makers with an analytical grid to better diagnose the nature of the threat, allowing them to strategically arbitrate between a socio-technical redesign and the application of corrective measures (Duran et al., 2009; Fürstenau et al., 2021). To preserve conceptual coherence, the analysis focuses on legitimate employees operating within a formal corporate context, where employees' security-related behaviors emerge from the dyadic relationship between organizational conditions and employee agency (N. P. Liang et al., 2016; Kim et al., 2022).

By exploring the insider threat through the prism of dyadic fit, this article invites a broadened academic understanding: exposure to risk may not be the mere manifestation of isolated individual rationality, but could result from a structural misalignment heterogeneously associating the technological and ethical dimensions of the firm (Lee et al., 2023).

2. Theoretical foundations: from the isolated to the dyadic relationship in information security

The understanding of insider threat in information security has historically been structured around isolated approaches seeking to predict the compliance or deviance of actors within the firm (Silic et al., 2017; Burns et al., 2023). A first dominant stream is anchored in deterrence theory, positing that the certainty and severity of sanctions constitute the primary levers to reduce abuse intentions and regulate deviant behaviors (Burns et al., 2023). In contrast, a motivational perspective mobilizes self-determination theory to emphasize the critical role of rule internalization and psychological need satisfaction in the adoption of proactive behaviors (Hong & Xu, 2021; X. Chen et al., 2025). Concurrently, studies focusing on workaround practices and non-malicious security violations rely on coping theory or the theory of interpersonal behavior to suggest that non-compliance often emerges as a pragmatic or even routine, response to constraining information systems (Nadhrah & Michell, 2014). Although these research traditions have considerably enriched the taxonomy of security-related employee behaviors, they share a major structural limitation: they tend to model the employee as an asocial actor whose decisions depend on independent and linear variables, thereby omitting the profoundly interactive and asymmetrical nature of their relationship with the classic corporate environment (Johnston et al., 2025).

Building on this limitation, the analysis of security-related employee behavior can be anchored in a dyadic logic. Stakeholder theory provides this foundation by viewing the employee not as an isolated source of threat, but as a stakeholder whose cooperation depends on the quality of the exchange with the organization (Bundy et al., 2018). In a formal corporate environment, strictly characterized by prescribed business processes, this relationship relies on the concept of organization-stakeholder fit (Bundy et al., 2018). This fit unfolds into two central constructs. First, value congruence materializes the normative alignment between the employee's ethical

principles and the firm's security imperatives, acting as a central foundation of trust and moral engagement (Edwards & Cable, 2009). Second, strategic complementarity captures the instrumental dimension of the relationship, namely the capacity of the technological infrastructure and security processes to provide the resources necessary for the employee to accomplish tasks effectively. These two dimensions operate in concert at the organizational level; compliance with security policies is therefore not the result of a one-dimensional rational calculation, but the outcome of an ongoing negotiation between preserving values and accessing operational resources (Edwards & Cable, 2009; Bundy et al., 2018).

Within this analytical perimeter, the literature attempts to capture a complex behavioral spectrum that ideally begins with proactive protection (Xu et al., 2024). In this state, employees voluntarily exceed formal requirements to actively defend organizational information assets and anticipate security threats. Research often mobilizes self-determination theory or organizational citizenship models to explain how intrinsic motivation fosters these extra-role security behaviors (Hong & Xu, 2021). However, these variance-based perspectives predominantly focus on isolated psychological drivers, frequently overlooking how the instrumental adequacy of the technological environment remains an important condition for sustaining such voluntary engagement over time (Xu et al., 2024).

Moving along this spectrum, a significant portion of the literature focuses on benign non-compliance, operationalized as non-malicious security violations aimed at resolving operational frictions and supporting work completion (Bartelheimer et al., 2023). These acts typically emerge when prescribed systems hinder task execution, forcing the adoption of workarounds (Van Offenbeek et al., 2024). To bypass this inadequate infrastructure, employees mobilize neutralization techniques, allowing them to temporarily suspend their moral obligations and rationalize their infraction without degrading their self-concept (Siponen & Vance, 2010; Haag et al., 2019). While neutralization explains the cognitive rationalization, it remains a partial explanation that isolates the employee from the broader dyadic context, failing to fully integrate the ongoing tension between operational constraints and the preservation of organizational allegiance (Siponen & Vance, 2010).

Distinct from these well-intentioned adaptations, the literature also documents instrumental abuse, a behavior where actors deliberately exploit their legitimate technological access for personal gain or opportunistic purposes (Willison & Warkentin, 2013; Lowry et al., 2015). While deterrence theory and rational choice models frequently attempt to explain these acts through strict cost-benefit calculations of potential sanctions, they struggle to contextualize them within the organizational fabric (Willison & Warkentin, 2013). These atomistic models often obscure the structural prerequisites of such deviance, notably the paradox where a highly functional technological infrastructure provides the very means for opportunism once the employee's ethical identification with the firm has dissolved (H. Chen et al., 2019).

Finally, the spectrum culminates in malicious abuse, involving deliberate retaliatory sabotage or data destruction (Idensohn et al., 2026). Research based on coping theory or the fraud triangle models these extreme abuses as conscious strategies triggered by perceived injustice, while other perspectives view deviation as a matter of habit (Johnston et al., 2025; Idensohn et al., 2026). By treating non-compliance either as a purely psychological failure or a mere lack of

deterrence, the existing literature fails to offer a unified framework capable of capturing the full equifinality of these diverse trajectories within a classic corporate environment (Johnston et al., 2025).

This theoretical fragmentation thus reveals a major insufficiency in understanding insider threats. The juxtaposition of disparate streams structurally fails to capture the substitution and conjunction effects inherent to dyadic fit (Bundy et al., 2018). More critically, existing models fail to explain why similar instrumental constraints may lead to fundamentally different behavioral outcomes depending on their combination with normative conditions (Fiss, 2011; Furnari et al., 2021). This limitation reveals the absence of a theoretical mechanism capable of capturing causal asymmetry and equifinality within the insider threat phenomenon (Furnari et al., 2021). Consequently, to overcome this incommensurability, a neo-configurational posture becomes particularly appropriate (Fiss, 2011). The following section (Section 3) will transform this theoretical foundation into explicit configurational propositions, theorizing how the systemic architecture of the employee-organization relationship orchestrates the equifinal emergence of these contrasting behavioral profiles.

3. Theoretical development and configurational propositions

3.1. Methodology and declaration concerning GenAI

The methodology mobilizes experimental vignettes as a conceptual device to connect controlled theoretical manipulations with plausible organizational situations. The vignettes are not treated as data, but as theoretically grounded illustrations intended to improve the interpretability and future testability of the four configurational pathways (Aguinis & Bradley, 2014; Harrits & Møller, 2021). Their design follows four condensed steps: first, the manipulated dimensions are derived directly from the conceptual framework, contrasting value congruence with value incongruence and strategic complementarity with strategic incompatibility (Bundy et al., 2018); second, these abstract combinations are translated into realistic scenarios while keeping the broader organizational context sufficiently stable (Atzmüller & Steiner, 2010; Payton & Gould, 2022); third, each vignette clarifies the expected intentions, judgments, rationalizations and causal mechanisms associated with a specific configurational state; and fourth, future empirical use would require pre-testing with experts or representative employees to assess plausibility, comprehension, and manipulation checks, while reducing social desirability bias (Aguinis & Bradley, 2014; Haag et al., 2025).

Declaration of use of Generative Artificial Intelligence technologies: the authors used generative artificial intelligence tools solely to improve the readability and linguistic quality of the manuscript. The tools were not used to generate scientific content, analyses or interpretations. The authors take full responsibility for the content of the article.

3.2. Configurational logic of security fit/misfit

The study of security-related employee behaviors has long been dominated by variance models, which seek to isolate the net, independent effects of variables such as sanction severity or hierarchical pressure on the intention to comply (Bulgurcu et al., 2010; Burns et al., 2023). However, this linear analytical logic appears epistemologically insufficient to capture the

inherent complexity of the insider threat phenomenon (Fiss, 2011). To grasp this limitation, it is imperative to distinguish a merely complicated system from a genuinely complex environment (Schneier & Vance, 2025). In a complicated system, interactions between components remain linear, well-structured, and predictable, allowing for rigorous testing of isolated causes and effects related to security risks (Schneier & Vance, 2025). Conversely, the classic corporate environment is characterized by true complexity, involving non-linear, ad hoc, and tightly coupled interactions between employees, technological constraints and security policies (Schneier & Vance, 2025). This complexity generates emergent employee behaviors that make it impossible to understand the insider threat through the simple addition of isolated factors (El Sawy et al., 2010). Capturing this dynamic requires shifting to a configurational theorization to model equifinality; that is, the possibility that radically opposed employee responses can stem from asymmetrical combinations of organizational factors (Fiss, 2007). It should be noted at the outset that the framework developed here represents a purely theoretical configurational approach aimed at formulating conceptual propositions, rather than an empirical demonstration.

To structure this theoretical model, the analysis is built around two major constitutive dimensions (Bundy et al., 2018). The first dimension is value congruence (VC), which characterizes the normative fit between employees' ethical principles and the organization's security objectives (Edwards & Cable, 2009). The second dimension is strategic complementarity (SC), which evaluates the instrumental fit, meaning the extent to which the prescribed technological infrastructure supports the employee's operational requirements without hindering their efficiency. The dynamic interaction within a complex environment between the presence or absence (misfit) of these two dimensions acts as the theoretical engine of our model (Schneier & Vance, 2025). To enhance the interpretability of the configurational logic, each theoretical pathway is complemented by illustrative vignettes (Table 2-5), acting as a device for the cognitive simulation of causal mechanisms to concretize abstract combinations of conditions into plausible organizational situations.

		instrumental dimension	
		Fit – strategic complementarity (SC)	**Misfit – strategic incompatibility (SI)**
normative dimension	**Fit – value congruence (VC)**	Satisfactory fit (VC x SC): guardian and proactive protection	Resource compromise (VC x SI): circumventer and benign non-compliance
	Misfit – value incongruence (VI)	Value compromise (VI x SC): opportunist and instrumental abuse	Severe misfit (VI x SI): fighter and malicious abuse

Table 1: Configurational framework for organization-employee fit/misfit based on (Bundy et al., 2018)

3.3. Satisfactory fit (VC x SC): guardian and proactive protection

The first causal pathway of our model theorizes the emergence of proactive information protection, a behavior that transcends simple passive compliance with rules (Xu et al., 2024). This trajectory emerges when a satisfactory fit is achieved within the dyadic relationship (Bundy et al., 2018). In this "guardian" archetype, the employee strongly identifies with the

company's imperatives (value congruence) and simultaneously benefits from a technological environment that facilitates task completion (strategic complementarity) (Posey et al., 2013). The combinatorial logic here rests on a mutual reinforcement effect: the presence of adequate technological resources prevents operational exhaustion, thereby allowing moral engagement to be fully expressed through autonomous motivation (X. Chen et al., 2025). Unhindered by technology, the employee mobilizes their energy to actively defend the organization's information system (Burns et al., 2021).

This proactive protection configuration is illustrated in more detail by the following situational vignette, thereby illustrating how the congruence of values and strategic complementarity jointly support security-oriented behaviors.

You work as a financial analyst in a classic corporate environment and must urgently transfer a report containing highly sensitive client data to a business partner (Safa & Von Solms, 2016). Your company's technological infrastructure provides an encrypted transfer platform that integrates smoothly into your email interface, guaranteeing seamless operation without slowing down your regular workflow (Strong & Volkoff, 2010). At the same time, your organization cultivates a strict ethical culture focused on the absolute respect of client privacy, a fundamental value that resonates deeply with your own moral convictions (Edwards & Cable, 2009). Experiencing this satisfactory fit between the prescribed tool and your internalized principles, you not only consistently use the official platform, but you also deliberately take the initiative to guide a new colleague who was mistakenly about to use an unsecured personal email account (Posey et al., 2015).

Table 2: situational vignette about proactive and secure sharing of client data

3.4. Resource compromise (VC x SI): circumventer and benign non-compliance

The causal asymmetry of the model is reflected through the exploration of compromise situations (Fiss, 2011). The second causal pathway reflects the emergence of non-malicious security violations and the adoption of workarounds (Bartelheimer et al., 2023). This trajectory, specific to the "circumventer" archetype, emerges when the employee faces a specifically technological misfit (SI) while maintaining a strong attachment to the company's values (VC) (Bundy et al., 2018). The underlying theoretical mechanics reside in a substitution conflict. Because the official technological infrastructure is flawed, overly complex, or inadequate, it severely hinders work efficiency (Van Offenbeek et al., 2024). Faced with this instrumental constraint, the employee chooses to sacrifice the formal security procedure in favor of parallel tools (for example: shadow IT) to preserve their operational capacity and achieve the organizational goals they continue to value (Silic & Back, 2014; Haag et al., 2019).

This resource compromise configuration is further illustrated by the following situational vignette, thus making it possible to understand how congruence of values and strategic incompatibility jointly lead to workarounds motivated by efficiency.

You hold the position of a data analyst and are responsible for delivering a decisive performance report for the imminent launch of a new marketing campaign (Malaurent & Karanasios, 2020). You are deeply committed to the success of your department and completely adhere to the corporate culture that values high performance, demonstrating an intact normative attachment (Suar & Khuntia, 2010). However, the analysis software provided and mandated by the information systems department proves to be obsolete, lacks essential functionalities, and systematically crashes when processing large volumes of data, representing a major instrumental deficit (Bartelheimer et al., 2023). To overcome this technological constraint while meeting the critical deadline set by your hierarchy, you choose to sacrifice the formal security procedure by downloading an unauthorized open-source analysis tool from the Internet (Bartelheimer et al., 2023; Haag et al., 2025). You adopt this parallel work practice exclusively to resolve the substitution conflict and guarantee the successful completion of your mission (Bartelheimer et al., 2023)

Table 3: situational vignette about adopting a parallel analysis tool to cope with an obsolete infrastructure

3.5. Value compromise (VI x SC): opportunist and instrumental abuse

The third pathway models instrumental computer abuse, characteristic of the "opportunist" archetype (Willison & Warkentin, 2013; Idensohn et al., 2026). This trajectory emerges during a normative rupture: the organization provides excellent resources and broad access that greatly facilitate work (SC), but the moral tie and ethical identification between the employee and the organization are broken (VI) (H. Chen et al., 2019). The explanatory logic of this configuration relies on the presence of an opportunity for action coupled with the absence of internal moral constraint (Willison et al., 2018; Idensohn et al., 2026). Possessing high-performing legitimate access but lacking any loyalty to security imperatives, the employee exploits the technological infrastructure for personal advantage or financial gain (Lowry et al., 2015).

This normative compromise configuration is illustrated in more detail by the following situational vignette, thus making it possible to concretize how the value incongruence and the strong strategic complementarity jointly facilitate the instrumental computer abuse.

You hold the position of a market analyst in a classic corporate environment and have privileged access to the organization's customer database (Duran et al., 2009; Johnston et al., 2025). Your company's technological infrastructure is highly efficient, providing you with seamless and fast data extraction tools that greatly facilitate the accomplishment of your daily tasks, thus materializing strong strategic complementarity. However, you no longer identify at all with the company's ethical principles, and you consider the information security policy to be a hypocritical moral constraint that does not concern you, which illustrates profound value incongruence (H. Chen et al., 2019; Burns et al., 2023). Possessing high-performing legitimate access but completely lacking loyalty to the organization's security imperatives, you decide to exploit this technological opportunity to discreetly download a list of high-potential clients to sell to a third party for personal financial gain (Burns et al., 2023)

Table 4: situational vignette about exfiltration of client data for a lucrative side business

3.6. Severe misfit (VI x SI): fighter and malicious abuse

Finally, the fourth pathway theorizes the escalation toward expressive malicious acts (Willison & Warkentin, 2013; Johnston et al., 2025). This trajectory of total rupture, embodied by the "fighter", reflects the combination of deep moral disaffection (VI) and a technological environment perceived as constraining, unfair or paralyzing (SI). This double deprivation acts as a powerful catalyst for resentment (Xu et al., 2020). The conjunction of an instrumental misfit that generates operational frustration and a normative incongruence that deactivates all ethical restraint suggests a dynamic that triggers acts of sabotage, revenge or deliberate destruction of informational assets (Johnston et al., 2025).

This severe misfit configuration is illustrated in more detail by the following situational vignette, thus making it possible to understand how the value incongruence and strategic incompatibility jointly precipitate deliberate retaliatory abuse.

You hold the position of a network administrator in a classic corporate environment and are responsible for server maintenance (Jenkins et al., 2010; McInroy & Beer, 2022). The organization forces you to use an obsolete and extremely rigid management system that crashes daily, severely hindering your ability to accomplish your tasks and materializing strong strategic incompatibility (Bartelheimer et al., 2023; Van Offenbeek et al., 2024). At the same time, you recently received an unjustified performance evaluation and perceive the management culture as deeply toxic, which has completely destroyed your loyalty and generated profound value incongruence (Willison et al., 2018). Driven by strong resentment in the face of this constant operational frustration and absolute moral rupture, you deliberately decide to erase the company's backup databases, thereby committing an expressive act of sabotage aimed exclusively at punishing the organization (Jenkins et al., 2010; Willison & Warkentin, 2013).

Table 5: situational vignette about deliberate sabotage of critical infrastructure

3.7. Configurational propositions

The articulation of these four causal pathways suggests that the absence of proactive protection does not mechanically lead to malice (Fiss, 2011). Understanding this equifinality allows us to formulate the following configurational propositions (Fiss, 2007):

Proposition 1: When the major constitutive conditions of value congruence and strategic complementarity are jointly met, they form a configuration of satisfactory fit likely to produce proactive information protection by employees (Posey et al., 2013; Bundy et al., 2018).

Proposition 2: When the constitutive condition of value congruence is maintained, but interacts with strong strategic incompatibility (technological misfit), this combination forms a resource compromise configuration likely to produce parallel work practices and non-malicious security violations (Bundy et al., 2018; Bartelheimer et al., 2023).

Proposition 3: When the condition of value incongruence is coupled with high strategic complementarity providing significant access opportunities, this combination forms a normative compromise configuration likely to produce instrumental computer abuse (Bundy et al., 2018; Idensohn et al., 2026).

Proposition 4: When the conditions of strong value incongruence and severe strategic incompatibility are jointly met, they form a configuration of dyadic rupture likely to produce deliberate and malicious computer abuse (Bundy et al., 2018; Johnston et al., 2025).

4. Discussion

4.1. What the theoretical configuration reveals about the phenomenon

The configurational approach developed in this research transcends reductionist views of the insider threat by restoring the true complexity inherent to behavioral dynamics within the classic corporate environment (Idensohn et al., 2026). Instead of conceptualizing the employee as an isolated actor reacting mechanically to the probability of sanctions, our modeling suggests a precise distinction of organizational situations that, until now, were conflated under the generic prism of non-compliance (Y. Chen et al., 2021). By anchoring the analysis on dyadic fit, the model theorizes that employee behavior emerges from an asymmetrical interaction between the instrumental resources provided and internalized normative imperatives (Bundy et al., 2018). Thus, the configuration indicates specific states of rupture that invite distinct strategic responses: circumvention (circumventer) signals a problem of technological dissonance calling for a socio-technical redesign rather than a sanction (Van Offenbeek et al., 2024); opportunism (opportunist) denotes a normative rupture suggesting targeted control and strict governance (Idensohn et al., 2026); while hostility (fighter) materializes a double rupture placing the organization in a critical, high-risk organizational state (Bundy et al., 2018). This diagnostic granularity structures action and provides a fine-grained understanding of the phenomenon beyond mere descriptive diversity (Furnari et al., 2021). The associated illustrative vignettes support the interpretability of these configurations by illustrating how similar structural conditions might formally translate into distinct behavioral manifestations in the field (Martin et al., 2024).

4.2. Contributions to the mobilized theories

This conceptualization offers major contributions to the theories traditionally mobilized in management information systems by reorganizing their insights around the mechanics of fit and misfit (Gresov & Drazin, 1997). First, it substantially extends the scope of stakeholder theory, initially designed for macroscopic cooperation analysis, by applying it to the resolution of micro-conflicts related to the insider threat (Bundy et al., 2018). By articulating this theory around our interaction mechanism, we posit that employee cooperation (fit) or deviance (misfit) can be interpreted through dyadic fit configurations (Bundy et al., 2018). Second, by tightly linking employee behaviors to rupture configurations, our model challenges the universal primacy of deterrence theory (Burns et al., 2023; X. Chen et al., 2025). It theorizes that the strict cost-benefit calculus of sanctions operates predominantly in situations of normative disengagement, thereby limiting the absolute effectiveness of formal controls against employees primarily seeking to alleviate a technological inadequacy through workaround practices (Siponen & Vance, 2010; Haag et al., 2025). Finally, this research reconciles the apparent tensions between coping theory and the theory of interpersonal behavior regarding non-malicious security violations (H. Liang et al., 2019; Y. Chen et al., 2021). Relying on configurational interaction, our model indicates that conscious rationalization and habitual

automatism are not mutually exclusive but act as substitution mechanisms when the employee must compensate for an ill-fitting infrastructure while preserving their allegiance to the firm's performance objectives (H. Liang et al., 2019; Van Offenbeek et al., 2024).

4.3. Specific theoretical contribution

Beyond these cross-enrichments, the specific theoretical contribution of this article lies in the introduction of a novel explanatory logic entirely anchored in the configurational paradigm (Fiss, 2007, 2011). By formally conceptualizing the equifinality of security-related employee behaviors, this research theorizes that insider threats of different intensities stem from fundamentally distinct causal combinations rather than a simple linear variation or the addition of independent variables (Fiss et al., 2013). This combinatorial logic highlights powerful structural substitution effects, suggesting that a strong normative attachment can prevent deliberate malice despite a failing technological infrastructure, generating instead a compensatory and benevolent non-compliance (Fiss, 2011). Furthermore, our theorization proposes an explicit operationalization of the principle of causal asymmetry in the field of information security (Furnari et al., 2021). It advances the concept that the absence of conditions leading to proactive protection does not mechanically trigger acts of sabotage, as the latter is likely to require a specific dynamic of dyadic rupture characterized by a simultaneous, combined, and joint breakdown of strategic complementarity and value congruence (Bundy et al., 2018).

4.4. Non-academic implications: society, business, management

The implications of these configurational recipes extend beyond the purely academic sphere to structure strategic actions at societal, business, and managerial levels (Johnston et al., 2025; X. Chen et al., 2025). On a societal level, facing major global challenges related to information protection, this approach indicates that an exclusively punitive work environment may exacerbate deviant behaviors among internal actors instead of mitigating the underlying technical weaknesses they are forced to exploit (Lowry et al., 2015; Silic et al., 2017). On a business level, the recognition and dynamic management of a satisfactory fit invite a transformation of the information systems security function: from a simple restrictive cost center, it could emerge as a genuine lever for value creation where strategic complementarity preserves the organization's agility and operational efficiency against competition (Sun et al., 2024). Practically, for daily management, this framework invites decision-makers to step away from blind sanction-based approaches and adopt a proactive engineering of fit structured by our diagnostic reading (Strong & Volkoff, 2010; Van Offenbeek et al., 2024). IT managers are invited to treat operational circumvention through a meticulous socio-technical redesign of work processes (Bartelheimer et al., 2023), to manage opportunism through targeted reinforcement of governance and access controls (Haag et al., 2025), and to circumscribe deliberate hostility as a critical risk requiring emergency intervention and precautionary measures (Duran et al., 2009). Decision-makers would thus benefit from accurately arbitrating between compliance rigor and workflow flexibility, designing facilitating interfaces and actively cultivating identification with corporate ethical principles to transform their collaborators into proactive protectors of the information system (X. Chen et al., 2025; Haag et al., 2025).

4.5. Boundary conditions, limitations and empirical agenda

The explanatory scope of this theory is intentionally bounded. First, its contextual boundary lies in the classic formal corporate environment, where employees operate within structured business processes, formal security policies, and identifiable managerial authority. The model is therefore not designed to explain attacks conducted by external intruders, nor security incidents occurring in loosely organized communities, criminal networks, or fully inter-organizational ecosystems. Second, its behavioral boundary concerns intentional security-related actions performed by legitimate employees who possess continuous access to organizational information systems. The framework does not address purely accidental errors, momentary inattention, or technical failures independent of employee agency. Third, its normative boundary assumes a boundedly rational actor whose behavior remains connected to organizational tensions, perceived constraints, value alignment, or value rupture. It therefore does not seek to theorize clinically pathological conduct detached from organizational management dynamics.

These boundaries also clarify the limitations and empirical agenda of the paper. Because the framework is theoretical, the four configurations should be treated as causal recipes to be tested rather than as empirically validated classes. Future research could first mobilize fuzzy-set qualitative comparative analysis (fsQCA) to examine whether combinations of value congruence, value incongruence, strategic complementarity, and strategic incompatibility are sufficient or necessary for distinct security-related employee behaviors (Fiss, 2011; Furnari et al., 2021). Qualitative vignette experiments or mixed protocols could then assess how employees interpret situations of instrumental inadequacy, normative rupture, or dual misfit before engaging in circumvention, opportunism, or hostile abuse (Martin et al., 2024). Finally, longitudinal designs would be particularly valuable for examining how dyadic fit evolves over time, especially during the implementation of new information systems, when temporary misfits may either be repaired, normalized through workarounds, or escalate into more severe forms of insider threat (Malaurent & Karanasios, 2020).

5. Conclusion

The ubiquitous integration of information systems within the classic corporate environment has profoundly blurred the boundary between legitimate task performance and the emergence of the insider threat (Johnston et al., 2025). Driven by the persistent challenge of security incidents involving employees, the central objective of this theoretical research was to elucidate how and why legitimate employees engage in radically divergent behaviors regarding prescribed policies, spanning a spectrum from proactive asset protection to deliberate abuse (Burns et al., 2023). By mobilizing stakeholder theory to construct an explanatory framework, this article theorizes that the insider threat does not merely reflect a simple linear continuum from strict compliance to calculated malice, driven solely by the fear of formal sanctions (Siponen & Vance, 2010; Bundy et al., 2018). Instead, employees' security-related behaviors represent an emergent and asymmetrical property of the dyadic relationship between the organization and the employee (Fiss, 2011; Bundy et al., 2018). We propose that these employee behavioral trajectories are generated by distinct configurations of fit and misfit, anchored around two orthogonal dimensions: strategic complementarity, which captures the instrumental adequacy

of technological resources to support the workflow, and value congruence, which reflects the normative alignment of shared ethical principles (Edwards & Cable, 2009; Strong & Volkoff, 2010). This configurational approach offers a theoretical resolution to existing tensions in the literature by suggesting that efficiency-driven circumventions and expressive malicious acts arise from fundamentally different organizational conditions rather than from a simple uniform failure of managerial control (Wong et al., 2022; Idensohn et al., 2026). Ultimately, this conceptualization shifts the analytical focus from the isolated individual to the complex organizational system they inhabit daily (Fiss, 2007). By introducing equifinality to the core of information security, this framework provides a conceptual foundation that now calls for empirical testing across diverse corporate contexts (Gresov & Drazin, 1997). This perspective thereby invites the scientific community to further explore how the ongoing evolution of the dyadic relationship between the organization and its employees continuously shapes and reconfigures the insider threat landscape (Johnston et al., 2025).

6. Bibliography

Aguinis, H., & Bradley, K. J. (2014). Best practice recommendations for designing and implementing experimental vignette methodology studies. *Organizational Research Methods*, *17*(4), 351–371. https://doi.org/10.1177/1094428114547952

Atzmüller, C., & Steiner, P. M. (2010). Experimental vignette studies in survey research. *Methodology*, *6*(3), 128–138. https://doi.org/10.1027/1614-2241/a000014

Bartelheimer, C., Wolf, V., & Beverungen, D. (2023). Workarounds as generative mechanisms for bottom-up process innovation—Insights from a multiple case study. *Information Systems Journal*, *33*(5), 1085–1150. https://doi.org/10.1111/isj.12435

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. https://doi.org/10.2307/25750690

Bundy, J., Vogel, R. M., & Zachary, M. A. (2018). Organization–stakeholder fit: A dynamic theory of cooperation, compromise, and conflict between an organization and its stakeholders. *Strategic Management Journal*, *39*(2), 476–501. https://doi.org/10.1002/smj.2736

Burns, A. J., 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*(2), 343–360. https://doi.org/10.1007/s10796-019-09951-9

Burns, A. J., 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. https://doi.org/10.1287/isre.2022.1133

Chen, H., Chau, P. Y. K., & 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. https://doi.org/10.1108/ITP-12-2017-0421

Chen, X., Schöni, L., Distler, V., & Zimmermann, V. (2025). Beyond Deterrence: A Systematic Review of the Role of Autonomous Motivation in Organizational Security Behavior Studies. *Proceedings of the 2025 CHI Conference on Human Factors in Computing Systems*, 1–28. https://doi.org/10.1145/3706598.3713122

Chen, Y., Galletta, D. F., Lowry, P. B., Luo, X. R., 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. https://doi.org/10.1287/isre.2021.1014

Duran, F. A., Conrad, S. H., Conrad, G. N., Duggan, D. P., & Held, E. B. (2009). Building a system for insider security. *IEEE Security & Privacy Magazine*, *7*(6), 30–38. https://doi.org/10.1109/MSP.2009.111

Edwards, J. R., & Cable, D. M. (2009). The value of value congruence. *Journal of Applied Psychology*, *94*(3), 654–677. https://doi.org/10.1037/a0014891

El Sawy, O. A., Malhotra, A., Park, Y., & Pavlou, P. A. (2010). **Research Commentary** — Seeking the Configurations of Digital Ecodynamics: It Takes Three to Tango. *Information Systems Research*, *21*(4), 835–848. https://doi.org/10.1287/isre.1100.0326

Fiss, P. C. (2007). A set-theoretic approach to organizational configurations. *Academy of Management Review*, *32*(4), 1180–1198. https://doi.org/10.5465/amr.2007.26586092

Fiss, P. C. (2011). Building better causal theories: A fuzzy set approach to typologies in organization research. *Academy of Management Journal*, *54*(2), 393–420. https://doi.org/10.5465/amj.2011.60263120

Fiss, P. C., Marx, A., & Cambré, B. (2013). Chapter 1 Configurational Theory and Methods in Organizational Research: Introduction. In P. C. Fiss, B. Cambré, & A. Marx (Eds.), *Research in the Sociology of Organizations* (Vol. 38, pp. 1–22). Emerald Group Publishing Limited. https://doi.org/10.1108/S0733-558X(2013)0000038005

Furnari, S., Crilly, D., Misangyi, V. F., Greckhamer, T., Fiss, P. C., & Aguilera, R. V. (2021). Capturing Causal Complexity: Heuristics for Configurational Theorizing. *Academy of Management Review*, *46*(4), 778–799. https://doi.org/10.5465/amr.2019.0298

Fürstenau, D., Rothe, H., & Sandner, M. (2021). Leaving the Shadow: A Configurational Approach to Explain Post-identification Outcomes of Shadow IT Systems. *Business & Information Systems Engineering*, *63*(2), 97–111. https://doi.org/10.1007/s12599-020-00635-2

Gregor, S. (2006). The nature of theory in information systems. *MIS Quarterly*, *30*(3), 611. https://doi.org/10.2307/25148742

Gresov, C., & Drazin, R. (1997). Equifinality: Functional Equivalence in Organization Design. *The Academy of Management Review*, *22*(2), 403–428. https://doi.org/10.5465/amr.1997.9707154064

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. https://doi.org/10.1016/j.im.2018.11.006

Haag, S., Siegfried, N., & Winkler, N. (2025). Informal control responses to information security policy violations: A factorial survey on insurance employees' moral licensing of insider threats. *Computers & Security*, *157*, 104575. https://doi.org/10.1016/j.cose.2025.104575

Harrits, G. S., & Møller, M. Ø. (2021). Qualitative vignette experiments: A mixed methods design. *Journal of Mixed Methods Research*, *15*(4), 526–545. https://doi.org/10.1177/1558689820977607

Hong, Y., & Xu, M. (2021). Autonomous Motivation and Information Security Policy Compliance: Role of Job Satisfaction, Responsibility, and Deterrence. *Journal of Organizational and End User Computing*, *33*(6), 1–17. https://doi.org/10.4018/JOEUC.20211101.oa9

IBM Corporation. (2025). *Cost of a Data Breach Report 2025: The AI Oversight Gap* [Rapport technique]. IBM Corporation. https://www.ibm.com/reports/data-breach

Idensohn, C., Flowerday, S., Van Der Schyff, K., & Chua, Y. T. (2026). Malicious insider threats in cybersecurity: A fraud triangle and Machiavellian perspective. *Computers in Human Behavior*, *174*, 108809. https://doi.org/10.1016/j.chb.2025.108809

Jenkins, N., Bloor, M., Fischer, J., Berney, L., & Neale, J. (2010). Putting it in context: The use of vignettes in qualitative interviewing. *Qualitative Research*, *10*(2), 175–198. https://doi.org/10.1177/1468794109356737

Johnston, A. C., Goel, S., & Williams, K. (2025). From cyber benign to cyber malicious: Unveiling the evolution of insider cyber maliciousness from a stage theory perspective. *European Journal of Information Systems*, *34*(4), 739–757. https://doi.org/10.1080/0960085X.2024.2413072

Kim, J., Park, E. H., Park, Y. S., Chun, K. H., & Wiles, L. L. (2022). Prosocial rule breaking on health information security at healthcare organisations in south korea. *Information Systems Journal*, *32*(1), 164–191. https://doi.org/10.1111/isj.12338

Lee, D., Lallie, H. S., & Michaelides, N. (2023). The impact of an employee's psychological contract breach on compliance with information security policies: Intrinsic and extrinsic motivation. *Cognition, Technology & Work*, *25*(2–3), 273–289. https://doi.org/10.1007/s10111-023-00727-5

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. https://doi.org/10.25300/MISQ/2019/14360

Liang, N. P., Biros, D. P., & Luse, A. (2016). An empirical validation of malicious insider characteristics. *Journal of Management Information Systems*, *33*(2), 361–392. https://doi.org/10.1080/07421222.2016.1205925

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

Magklaras, G. B., & Furnell, S. M. (2005). A preliminary model of end user sophistication for insider threat prediction in IT systems. *Computers & Security*, *24*(5), 371–380. https://doi.org/10.1016/j.cose.2004.10.003

Malaurent, J., & Karanasios, S. (2020). Learning from Workaround Practices: The Challenge of Enterprise System Implementations in Multinational Corporations. *Information Systems Journal*, *30*(4), 639–663. https://doi.org/10.1111/isj.12272

Martin, É., Bergeron, D., & Gaboury, I. (2024). The Use of Vignettes to Improve the Validity of Qualitative Interviews for Realist Evaluation. *Qualitative Health Research*, *35*(3), 267–274. https://doi.org/10.1177/10497323241237411

McInroy, L. B., & Beer, O. W. J. (2022). Adapting vignettes for internet-based research: Eliciting realistic responses to the digital milieu. *International Journal of Social Research Methodology*, *25*(3), 335–347. https://doi.org/10.1080/13645579.2021.1901440

Nadhrah, N., & Michell, V. (2014). Workaround Motivation Model (WAMM): An Adaptation of Theory of Interpersonal Behaviour. In K. Liu, S. R. Gulliver, W. Li, & C. Yu (Eds.), *Service Science and Knowledge Innovation* (Vol. 426, pp. 52–62). Springer Berlin Heidelberg. https://doi.org/10.1007/978-3-642-55355-4_6

Payton, K. S. E., & Gould, J. B. (2022). Vignette Research Methodology: An Essential Tool for Quality Improvement Collaboratives. *Healthcare*, *11*(1), 1–12. https://doi.org/10.3390/healthcare11010007

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., Roberts, T. L., Lowry, P. B., Bennett, R. J., & Courtney, J. F. (2013). Insiders' protection of organizational information assets: Development of a systematics-based taxonomy and theory of diversity for protection-motivated Behaviors1. *MIS Quarterly*, *37*(4), 1189–1210. https://doi.org/10.25300/MISQ/2013/37.4.09

Safa, N. S., & Von Solms, R. (2016). An information security knowledge sharing model in organizations. *Computers in Human Behavior*, *57*, 442–451. https://doi.org/10.1016/j.chb.2015.12.037

Schneier, B., & Vance, A. (2025). Guest Editorial: "Complexity is the Worst Enemy of Security": Studying Cybersecurity Through the Lens of Organizational Complexity. *MIS Quarterly*, *49*(1), 205–210. https://doi.org/10.25300/MISQ/2025/49.1.075

Silic, M., & Back, A. (2014). Shadow IT – A view from behind the curtain. *Computers & Security*, *45*, 274–283. https://doi.org/10.1016/j.cose.2014.06.007

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. https://doi.org/10.1016/j.im.2017.02.007

Siponen, M., & Vance, A. (2010). Neutralization: New insights into the problem of employee information systems security policy violations. *MIS Quarterly*, *34*(3), 487–502. https://doi.org/10.2307/25750688

Strong, D. M., & Volkoff, O. (2010). Understanding Organization—Enterprise System Fit: A Path to Theorizing the Information Technology Artifact1. *MIS Quarterly*, *34*(4), 731–756. https://doi.org/10.2307/25750703

Suar, D., & Khuntia, R. (2010). Influence of Personal Values and Value Congruence on Unethical Practices and Work Behavior. *Journal of Business Ethics*, *97*(3), 443–460. https://doi.org/10.1007/s10551-010-0517-y

Sun, Y., Tan, C., Lim, K. H., Liang, T., & Yeh, Y. (2024). Strategic contexts, strategic orientations and organisational technology adoption: A configurational approach. *Information Systems Journal*, *34*(4), 1355–1401. https://doi.org/10.1111/isj.12497

Van Offenbeek, M. A. G., Vos, J. F. J., Van Den Hooff, B., & Boonstra, A. (2024). When workarounds aggravate misfits in the use of electronic health record systems. *Information Systems Journal*, *34*(2), 293–326. https://doi.org/10.1111/isj.12478

Willison, R., & Warkentin, M. (2013). Beyond Deterrence: An Expanded View of Employee Computer Abuse1. *MIS Quarterly*, *37*(1), 1–20. https://doi.org/10.25300/MISQ/2013/37.1.01

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. https://doi.org/10.1111/isj.12129

Wong, L. H. M., Hurbean, L., Davison, R. M., Ou, C. X., & Muntean, M. (2022). Working around inadequate information systems in the workplace: An empirical study in Romania. *International Journal of Information Management*, *64*, 102471. https://doi.org/10.1016/j.ijinfomgt.2022.102471

Xu, F., Hsu, C., Wang, T. (David), & Lowry, P. B. (2024). The antecedents of employees' proactive information security behaviour: The perspective of proactive motivation. *Information Systems Journal*, *34*(4), 1144–1174. https://doi.org/10.1111/isj.12488

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. https://doi.org/10.1016/j.im.2019.103180

Zeadally, S., Yu, B., Jeong, D. H., & Liang, L. (2012). Detecting insider threats: Solutions and trends. *Information Security Journal: A Global Perspective*, *21*(4), 183–192. https://doi.org/10.1080/19393555.2011.654318