Going the 'Extra' Mile: The Role of Sensemaking in Extra-Role Security Behaviors

Ayse Nur Asyali
University of Luxembourg
aysenur.asyali@uni.lu

Ayah Tharwat
University of Luxembourg
ayah.tharwat@uni.lu

Muriel Frank
University of Luxembourg
muriel.frank@uni.lu

Lennart Jaeger
lennartjaegerggs@gmail.com

Abstract

As organizations are increasingly challenged by evolving information security threats that demand more than employee compliance to address, interest has grown in understanding extra-role security behaviors (ERSBs)—voluntary actions employees take beyond formal security policies that benefit organizations' security. Despite this interest, theoretical understanding of the individual and organizational factors that shape the cognitive process motivating such behaviors remains limited. Drawing on the lens of sensemaking, this study develops a theoretical framework presenting the process by which employees navigate organizational ambiguity and engage in ERSBs. Based on 40 in-depth interviews, our findings highlight the critical roles of security culture as organizational antecedent as well as cognitive frames and emotions as individual antecedents on the sensemaking process, ultimately influencing ERSBs. Using these insights, organizations and practitioners can better design and communicate policies, promote security dialogue, and build a security-forward environment that encourages ERSBs across all organizational roles.

Keywords: Extra-role security behavior, Sensemaking, Interviews, Qualitative research, Information security policy compliance.

1. Introduction

Formal compliance with information security policies (ISPs) is widely regarded as the foundation of organizational information security (Bulgurcu et al., 2010). Organizations invest heavily in the development of security procedures, the provision of training, and the implementation of monitoring systems to ensure that employees follow the prescribed rules and protocols (Flores et al., 2014). These efforts are based on the assumption that clearly articulated expectations, when supported by awareness and enforcement mechanisms, will lead to compliant behavior and mitigate security risks (Bulgurcu et al., 2010).

While compliance models perform well in structured environments where threats are well-defined and procedures are specific, increasing evidence suggests that these approaches offer a limited view of security behavior in practice (Hsu et al., 2015; Jaeger & Eckhardt, 2018; Vedadi et al., 2025). Security incidents frequently unfold in dynamic and ambiguous conditions, where cues may be subtle, policies unclear, and the appropriate course of action not readily apparent (Li et al., 2021). In such cases, rule-following alone is insufficient, as employees must interpret their environment, assess potential risks, and determine appropriate responses (Lin & Luo, 2021; Vedadi et al., 2025; Xu et al., 2024).

Therefore, while understanding why employees fail to comply remains important, it is equally critical to examine how they act beyond compliance when rules fall short. These behaviors, called extra-role security behaviors (ERSBs), include helping colleagues, raising concerns, modeling best practices, or proactively seeking information (Frank & Kohn, 2023). Notably, ERSBs do not only compensate for policy gaps, but can also reinforce and legitimize formal compliance efforts (Jaeger & Eckhardt, 2018). As such, ERSBs play a critical role in supporting organizational security, especially in contexts where threats evolve faster than policies can adapt (Xu et al., 2024). Understanding how and why these behaviors emerge requires a shift in perspective, from asking whether employees are compliant, to exploring how they make sense of

URI: https://hdl.handle.net/10125/111945
978-0-9981331-9-5

and respond to the security challenges they encounter particularly when those challenges cannot be addressed through rule-following alone. Drawing on sensemaking theory (Weick, 1995), we therefore examine how employees construct meaning from their organization's culture through the interplay between their cognitive frames and emotions to inform their security-related actions. We address the research question: *How does the sensemaking process contribute to the emergence of extra-role security behaviors in practice?* To answer this, the study pursues a twofold objective: first, to explore how employees' interpretations of organizational culture, cognitive frames, and emotions shape their security sensemaking; and second, to examine how this process ultimately leads to ERSB. We investigate these objectives through an in-depth qualitative study based on semi-structured interviews across two organizations with 40 employees. In doing so, we extend previous ERSB work by integrating insights from the sensemaking literature (Maitlis & Christianson, 2014; Weick et al., 2005) and showing how sensemaking processes shape employee decisions to participate in voluntary security actions. While prior conceptual models have emphasized the importance of sensemaking in information security behavior (Lin & Luo, 2021), this study offers an empirical account of how such behaviors unfold in practice.

2. Theoretical Background

2.1. Extra-Role Security Behavior

Organizations have long relied on ISPs, sets of guidelines, roles, and responsibilities that employees are expected to abide by, to monitor security behaviors (i.e., employee compliance) and protect against system risks (Bulgurcu et al., 2010; Hsu et al., 2015). When employees go beyond these formal obligations and perform intrinsically motivated actions that are not dependent on rewards or punishments, they exhibit ERSBs (Hsu et al., 2015). According to the taxonomy proposed by Frank and Kohn (2023), ERSB can be expressed through nine distinct approaches: (1) helping, (2) stewardship, (3) civic virtue, (4) whistleblowing, (5) sportsmanship, (6) organizational compliance, (7) organizational loyalty, (8) individual initiative, and (9) self-development. *Helping* is an affiliative promotive behavior that emphasizes small, informal acts of security assistance to support others, such as providing tips on how to securely use a system or educating colleagues on ISPs (Van Dyne et al., 1995). *Stewardship* is a more proactive form of ERSB in which a more experienced employee intervenes by offering cautious advice to help colleagues avoid security risks or ISP non-compliance (Frank & Kohn, 2023; Van Dyne et al., 1995). *Civic virtue* involves actively participating in security processes by challenging security behaviors and offering suggestions to improve security practices. *Whistleblowing* or reporting involves formally notifying superiors of non-compliance behaviors of colleagues. *Sportsmanship* involves tolerating security-related hindrances (i.e. in order to comply with ISPs) (Frank & Kohn, 2023). *Organizational compliance* is the act of adhering to security rules, regulations, and procedures. [1] *Organizational loyalty* is the commitment to protecting ones organization from security threats. *Individual initiative* is when employees go beyond the minimal expectations by voluntarily changing passwords, using protective screens, and discussing security. *Self-development* refers to self-initiated security education during ones free time to keep up with the evolving threat landscape (Frank & Kohn, 2023). Although ERSBs are critical to improving organizational outcomes (Hsu et al., 2015), surprisingly, few studies have examined the intricate factors that motivate such behaviors. This suggests that further research is needed to better understand how and why employees engage in any of the nine distinct ERSBs.

2.2. Sensemaking

Sensemaking, first presented by Weick (1995), refers to the retrospective process in which an individual gathers facts or opinions to construct their understanding of an incident or interaction (Lin & Luo, 2021; Weick et al., 2005). Much of the literature on sensemaking has focused on three main developmental stages: (1) scanning, (2) interpreting, and (3) responding (Daft & Weick, 1984). *Scanning* is the initial stage of sensemaking, where individuals actively retrieve cues to make sense of their environment (Daft & Weick, 1984). In a security context, this involves understanding an organization's culture, how ISPs are communicated the level of employee ISP awareness, and the formal consequences of non-compliance (Dupont et al., 2023; Lin & Luo, 2021). *Interpreting* involves categorization of certain stimuli as relevant or irrelevant to the activity at hand (Barr & Huff, 1997). For information security, this may include how employees perceive ISPs – whether they view them as important or constraining - and how they understand their own role in maintaining

[1] While compliance is often described as an in-role obligation, we treat it here as potentially extra-role under certain conditions. Specifically, when employees comply with security requirements in the absence of monitoring or obvious enforcement, their choice to adhere becomes discretionary rather than compelled. In such cases, compliance aligns with the broader spirit of extra-role security behavior (for a detailed discussion see Frank and Kohn, 2023).

security, whether as active and primary or passive and secondary (Dupont et al., 2023). Lastly, *Responding* is when employees act upon their interpretations by seeking solutions to an information security problem (Hahn et al., 2014). This would be their willingness to improve their own security practices, change their behavior, or comply with ISPs. For information security sensemaking, employees draw on these three stages when faced with an uncertain security interaction (Lin & Luo, 2021).

Sensemaking is shaped by various antecedents, including unexpected events (Weick, 1995), emotional experiences (Maitlis et al., 2013), and individual cognitive frames, all of which are influenced by organizational identity and shared culture (Hahn et al., 2014; Harris, 1994). In information security, employees draw upon these shared security beliefs and practices, which either enable or constrain their sensemaking process (Lin & Luo, 2021). At the individual level, sensemaking is driven by both cognitive frames and emotional states (Weick et al., 2005). Over time, as individuals gain security experience and knowledge, their cognitive frames evolve and influence the rigor and depth of their scanning process (Hahn et al., 2014). Likewise, emotional experiences play a prominent role in sensemaking (Maitlis et al., 2013), as people tend to remember and interpret past events that correspond to their current emotional states (Weick, 1995).

Information security studies have employed the sensemaking lens to understand how employees make sense of their surroundings, respond to threats, and engage in security behaviors. For instance, Lin and Luo (2021) conceptualized how organizational culture enables and constrains the sensemaking process through which information security behaviors - diagnosing, solving, and performing security behaviors- emerge. Dupont et al. (2023) applied sensemaking to analyze cyberresilience, specifically how information security professionals understand and interpret cyber tensions that influence decision making and practices. Lakshmi et al. (2021) examined how the dynamics between technology, individuals, and organizations shape sensemaking of incident response. While these studies offer valuable insights into the application of sensemaking in information security, little is known about how sensemaking unfolds for ERSBs. To address this gap, our study applies and extends the sensemaking framework to understand the process in which employees choose to perform ERSBs within their organization. We position sensemaking as a central process that connects ISP interpretations and actions to explain why employees engage in extra-role security behaviors (ERSBs).

3. Methodology

We conducted a qualitative study, interviewing a total of 40 employees in various positions at two different companies. This approach, which is suitable for in-depth studies of sensitive topics (Silverio et al., 2022), including information security (Balozian et al., 2023), allowed us to explore employees' experiences with and perceptions of information security measures and policies.

3.1. Interview Design

Our semi-structured interview protocol was divided into three parts with 15 pre-prepared questions, with room for follow-up questions if needed (Myers & Newman, 2007). In addition to gathering general information about the interviewees, such as their position and work experience, we asked them about their roles and perceptions of security measures, as well as their knowledge of and attitudes toward ISPs. By focusing on their perceptions, we were able to gain insight into their sensemaking processes along the dimensions of scanning, interpreting, and responding. The interview questions are available upon request. In total, we interviewed 40 employees who held different positions, as our goal was to understand how employees generally make sense of whether or not to engage in ERSBs. The interviews, all conducted using online video tools, lasted an average of 49 minutes and were transcribed and anonymized prior to analysis to protect participants' identities.

3.2. Data Collection

Participants were recruited on a voluntary basis (Podsakoff et al., 2003) in two different companies: an international pharmaceutical company (n=18) and an international mechanical engineering company (n=22). We included IT and non-IT employees, but ensured that none of them worked in the security department where policy decisions are made. At the time of data collection, they were full-time employees who had spent an average time of more than 8.5 years at their current employer. The majority of participants (n=29) were male and based in Europe (n=18), Asia (n=12), the United States (n=6) or Australia (n=4).

3.3. Data Analysis

In the first iteration, the first two authors open-coded the interviews and then discussed their first-order concepts that emerged during the analyses with the entire research team. Throughout this first-order analysis (Gioia et al., 2013) the authors identified 127 concepts regarding participants' feelings about security, and their understanding of security measures, the security culture and security behaviors initiated by themselves or their colleagues. In the second round, the authors used axial coding to organize these concepts into higher-level categories (Saldaña, 2013). In the final step, the researchers compiled these higher-level categories into a more theory-centric data structure (Gioia et al., 2013). It encompassed four key constructs: (1) organizational security culture, (2) individual antecedents consisting of (a) cognitive frames and (b) emotions, (3) the sensemaking process consisting of (a) scanning, (b) interpretation, and (c) responding, and (4) ERSBs. They then alternated between analyzing the surface patterns and delving into the granular insights they could extract from the participants' sensemaking processes. This involved sketching a series of diagrams to document the evolution of sensemaking of ERSBs. Thus, the four key constructs were incorporated into the final model presented in Figure 1, which will be further discussed in the following results section.

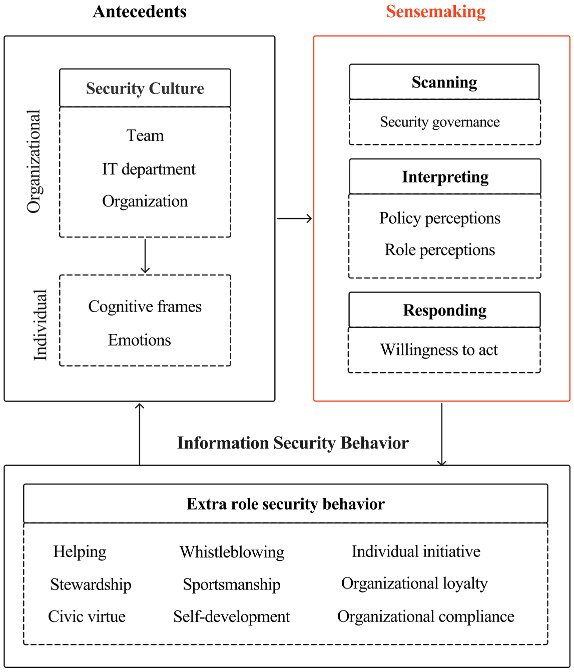

Figure 1: Sensemaking model of extra-role security behaviors.

4. Results

Our analysis of 40 interviews indicates that the sensemaking of ERSBs emerges from a process shaped by organizational and individual antecedents (Figure 1). Organizational antecedents reflect the cultural environment. In particular, the values, norms, and informal practices communicated within teams, through the IT department, and across the wider organization, influencing how employees understand and prioritize security (D'Arcy & Greene, 2014; Wiley et al., 2020). Individual antecedents involve employees' cognitive frames (e.g., prior knowledge, professional identity) and emotional orientations (e.g., anxiety, confidence) (Harris, 1994; Maitlis et al., 2013) that affect how they perceive and react to security-related risks. These antecedents shape the way employees engage in sensemaking (Weick, 1995), a recursive process of scanning for cues, interpreting their meaning, and forming a response (Lin & Luo, 2021).

4.1. Organizational antecedents

Organizational culture, broadly defined as the shared values, norms, and practices that guide behavior within a collective, has long been recognized as a foundational condition for how employees make sense of uncertainty (Harris, 1994). In the context of information security, organizational culture shapes not only what is communicated, but also how employees perceive what is important, what is expected of them, and how seriously security should be taken (Maitlis & Christianson, 2014; Weick, 1995). [2]

Our participants' sensemaking was closely tied to organizational culture. Employees described how their understanding of security was shaped by informal routines, conversations, and implicit norms in their immediate teams, interactions with the IT department, and broader organizational messaging. Often, it was what was emphasized, ignored, or left unspoken that revealed how security was culturally positioned in their workplace. These patterns reflect earlier work by Li et al. (2021), who argue that organizational security practices are commonly refracted through informal, team-level dynamics, what they term "tribal security." In such environments, formal policies may be present, but the norms that shape behavior are frequently tacit, localized, and inconsistent.

The team was often the most immediate and influential layer. P13 described how her manager relayed key updates: "*She's really good at forwarding things and making sure we don't miss anything.*" In such teams, security was actively communicated

[2] Although culture is our main focus, it is closely related to organizational climate, defined as employees' immediate perceptions of policies and practices (Vedadi et al., 2025), which can trigger sensemaking around specific events or incidents. Thus, some findings may reflect climate effects, understood here as part of the broader cultural context that influences security sensemaking.

and reinforced informally. Even mistakes were constructively addressed, as P25 explained: "*I can imagine that [if someone forgets to lock their screen] it might be brought up, but then in a funny way, not in a nasty way, but rather as a joke [...] because I would actually say that the people in my team trust each other, but that's already a safety aspect.*"

Views on the IT department were more mixed. Some participants found IT helpful in crises, but others experienced it as opaque or dismissive. P18 described reporting a flaw and being told, "*That's working as intended*," which left them doubting the department's openness. In these cases, the cultural disconnect appeared to weaken both commitment and clarity, making it harder for employees to judge when or how to step in proactively.

At the organizational level, participants questioned whether they were truly seen as partners in security. P38 asked, "*What is the company doing for me? Because I do things for the company. What are they doing for me in terms of security?*" Others echoed this imbalance. P5 noted, "*We only listen, receive the rules*," emphasizing the lack of background or involvement in decisions.

These varied perceptions illustrate how culture shaped the sensemaking around ERSBs. For some, cultural signals, such as strong team trust or visible managerial involvement, generated a sense of commitment that motivated them to act beyond formal rules, while their absence often led employees to interpret security as a low priority, adhere narrowly to formal responsibilities, and ultimately avoid taking initiative. For others, cultural cues shape ERSBs not through commitment but by clarifying expectations and boundaries, making it easier to judge when discretionary action is appropriate.

Importantly, these cultural cues do not just shape behavior directly, they also influence how employees mentally frame security issues and emotionally respond to them (Harris, 1994; Lin & Luo, 2021; Maitlis et al., 2013). This interaction provides the foundation for how they interpret and respond to security demands, an individual-level process we explore in the next section.

4.2. Individual antecedents

Individual antecedents in our model consist of two interrelated components: cognitive frames and emotional responses. Cognitive frames refer to how employees understand and mentally organize information security—including their level of security knowledge, prior exposure to threats, and familiarity with secure practices. Emotions, in turn, reflect the affective dimension of this engagement, including anxiety, fear, uncertainty or confidence about security.

Cognitive frames varied widely across participants. Some expressed confidence in their understanding and habits. As P11 noted, "*You have to be so darn careful now [...] but you can tell [spoof emails] a mile off basically [...] if you don't know, click on the address and you'll see that it's complete rubbish anyway.*" Others, however, revealed gaps in security awareness. As P8 pointed out, "*I don't think our employees know what IT is doing, what their role is. It's not to reset your password. It's bigger than that.*"

While some participants attributed their awareness to personal habits or past experiences, others traced it to structured initiatives such as awareness training. For example, P1 shared the personal impact of such programs: "*I think it's raised awareness [...] I've become a lot more aware. I've put most things in my junk e-mail now that I don't know.*"

Emotional responses to cybersecurity ranged from general concern to fear, often originating from what participants could not control or fully understand. As P21 explained, "*It's a fear [...] we are so unaware and we rely on our IT folks quite a lot.*" Also, P19 described this sense of ambiguity vividly: "*One gray uncertainty, a big, gray cloud of uncertainty.*"

These emotional reactions were often entangled with low security knowledge, reinforcing passivity or reliance on others. The interplay between uncertainty and fear created hesitation about how to act, especially in ambiguous situations. As P21 observed, "*You hear all these scams [...] and you kind of go, is this a scam? Is this trying to [...] get into our systems? [...] And I think that's where a lot of anxiety comes out of.*"

Taken together, the combined influence of organizational culture and individual orientations shaped how employees engaged in sensemaking. We explore this process in the next section.

4.3. Sensemaking

4.3.1. Scanning Participants began sensemaking by trying to understand what the organization expected of them regarding security. This stage, focused on security governance—policies and procedures in place to monitor compliance—typically involved scanning for available policies, communications, or cues about acceptable behavior and risks. However, many described limited clarity or accessibility. As P3 noted, "*I don't know where the information security policy is [...] I think I signed it when I joined, but that was years ago.*" Similarly, P26 noted, "*I know there are rules, but it's not something we see unless something goes wrong.*"

For most, policy awareness was limited to compliance prompts such as mandatory training or system warnings, rather than being embedded in daily practices.

Participants also reflected on the disconnect between the formal existence of policies and their practical relevance. Some viewed governance as overly centralized or disconnected from their actual roles. P12, for example, noted that they would go directly to someone in IT for help with a security issue, even though they suspected "*that's probably not the right answer [...] I've probably been told what the right answer is.*" These comments illustrate how scanning was often informal and reliant on memory or interpersonal networks, rather than on clear, accessible governance frameworks.

4.3.2. Interpreting

As participants encountered or recalled policies and guidance or noted their absence, they actively interpreted what these materials meant for their behavior. This stage of sensemaking was centered on two interrelated subcomponents: policy perceptions and role perceptions.

Several participants viewed ISPs as necessary but insufficient without clear explanations. P38 emphasized this disconnect: "*If you don't explain why this and that policy [...] what are the changes [...] then you ask yourself questions: why are we doing this and this and that?*" For many, inconsistency across departments or systems made policy interpretation difficult. P3 explained: "*We definitely have consistency issues across the business. I've been working with legal on copyright recently [...] people download papers and then what are they allowed to do with it? Do they even understand that?*"

In parallel, participants interpreted their own roles in security through a mix of formal and informal cues. Some participants saw themselves as active security actors, while others placed that responsibility elsewhere. P25 expressed ownership: "*I think everyone actually has a responsibility themselves and that's why I would say I also have a responsibility.*" In contrast, P17 said, referring to the Chief Information Security Officer (CISO), "*It's not really a common topic [...] if we get breached, it's [the CISO's] issue,*" reflecting a sense of distance from security concerns. Such contrasting role perceptions shaped the extent to which participants saw security as part of their everyday responsibilities or something delegated to others.

4.3.3. Responding

In this final stage of sensemaking, participants translated their interpretations into intentions. This stage centered on their willingness to act, not necessarily by taking action, but by articulating suggestions, preferences, or mental models of how security could be improved.

For some, this willingness emerged as constructive input to improve security processes. P7, for example, advocated for positive reinforcement: "*I think I was told a good example of this would be like promoting people who actually do lock their computer [...] giving them something of a reward*" Others emphasized the importance of explaining why policies exist. As P8 put it, "*If an end user doesn't understand why, then either you need to explain it to them so they understand the gravity or you need to make things very easy for them.*"

Still others envisioned ways to improve training and awareness in light of evolving threats. P39 warned that phishing and hacking were becoming more sophisticated: "*We will need more than just this simple training [...] we will need better advice in my opinion.*" P20 similarly proposed pacing security content more effectively: "*There's too much up front [...] it needs to be more bite-size pieces [...] people stop listening and they're not really understanding the message.*"

Participants' willingness to act laid the groundwork for broader engagement. For many, this final stage of sensemaking did not stop at reflections or suggestions but became a springboard for enacting understandings through behavior. In Weick et al. (2005) terms, enactment refers to how individuals test and affirm their interpretations by acting in ways that help create the very environment they are trying to comprehend. In this sense, employees actively shape their organizational context by initiating discretionary actions. These actions, explored in the following section, illustrate how sensemaking translated into sustained voluntary contributions to organizational security.

4.4. ERSBs

Participants exhibited a wide range of ERSBs, encompassing all nine types previously outlined in the literature: helping, stewardship, whistleblowing, civic virtue, self-development, individual initiative, sportsmanship, organizational loyalty, and organizational compliance (Frank & Kohn, 2023).

Helping behaviors were mostly interpersonal, with employees offering informal support to colleagues who were unsure how to handle specific security tasks. P2, for example, described routinely assisting colleagues: "*I'll show them how to log incidents.*" Others filled in gaps when formal IT responses were too slow or confusing. As P23 explained, "*It's usually easier if I google something for a colleague [...] instead of involving IT, which can take multiple emails.*" These moments of informal support helped maintain security practices and fostered a collaborative sense of responsibility.

Stewardship was expressed in small but meaningful ways, where employees internalized security norms and reinforced them in their teams. P40 noted simply, "*From time to time [...] I just tell them [...] turn off your monitor or lock your screen*," treating it as a regular habit to maintain awareness. P6 described a protective stance toward email hygiene: "*OK, you received some strange e-mail, so it's better that you delete it.*" These actions, while not part of anyone's formal job description, reflected an embedded sense of care for the collective security of the workplace.

Whistleblowing involved reporting violations when participants believed action was needed. P14 stated, "*If things happen [...] that could be a more significant impact [...] I will definitely bring [it] up to my superior or even maybe talk to anyone from the global team*". P15 described escalation for repeat violations: "*I talk to my manager [...] then the company will give him warning [...] then I think we pursue the user.*"

Civic virtue was reflected in participants' suggestions and advocacy to improve security processes and address organizational blind spots. P10, for instance, described how their team initiated a discussion that led to the joining their forum to ensure consistent messaging: "*That was something that we discussed as a team and thought that was important to kind of get her on board [...] just to make sure that everybody's [...] aware of what's going on.*"

Beyond these commonly recognized forms, other ERSB types also surfaced. For example, self-development was reflected in P14's habit of monitoring security-related news: "*Every morning before I start work [...] I will spend about 10–15 minutes [...] I will go to the local website [...] that concerns information security or any new regulations.*" Individual initiative was demonstrated through proactive reminders and peer guidance. As P38 explained, "*I ask them [colleagues] to remember to use secure password. [...] I say your password must [be a] complicated one.*" Sportsmanship emerged in P22's remarks on adapting to security constraints: "*On the one hand it's a hindrance [...] but on the other hand it's also important so that nothing happens.*" Organizational loyalty was captured in P12's reflection: "*They've told us we have to do it [...] it's their [the company's] way of protecting us and our work.*" Organizational compliance also appeared in several responses, such as P33 who stated, "*If let's say the rules [are] already done by IT or your information security team, we just follow. We never interrupt on that.*"

ERSBs not only reflected how employees interpreted and acted on existing cues, but in many cases reshaped those cues for others. For example, participants such as P2 and P23, who frequently helped colleagues navigate security issues, helped normalize peer-driven problem solving and created informal channels of knowledge sharing. Through such actions, participants modeled good practices, promoted collective vigilance and a culture of mutual responsibility. In this way, ERSBs began to influence the very antecedents that originally shaped them, feeding back into organizational security culture. Thus, over time, these behaviors subtly influence how security is prioritized and internalized within teams and departments.

5. Discussion

The present study set out to examine how the sensemaking process contributes to the emergence of ERSBs within organizations. To do so, we first explored the relationship between organizational security culture and individual cognitive frames and emotions on sensemaking. Second, we examined how the sensemaking process transpires and shapes employees' decisions to engage in ERSBs.

5.1. Theoretical Implications

We grounded our work in sensemaking theory (Weick, 1995) as a lens to better understand the processes and factors that guide employees toward ERSBs. While previous information security research has applied sensemaking to study cyber resilience and security behaviors such as policy compliance, problem solving, and reporting (Dupont et al., 2023; Lakshmi et al., 2021; Lin & Luo, 2021), our study extends the theoretical scope by exploring how employees make sense of ERSBs. By doing so, we not only identify novel antecedents to sensemaking, but also provide a more granular understanding of the scanning, interpreting, and responding stages of extra-role security behaviors.

First, our findings show that organizational security culture is a key input to sensemaking that shapes how employees label and interpret their roles, responsibilities, and environment. Importantly, this relationship was more pronounced in teams and departments, where information sharing and informal interactions are more frequent and clear. This supports prior findings on the interplay between culture and security behavior (Lin & Luo, 2021) and extends them by situating this relationship within the context of security culture and ERSBs. These relationships may be partly explained by communication asymmetries and a lack of transparency between an organization and its employees, which previous studies (Kim, 2018) have found to hinder the sensemaking process during uncertain situations.

Second, we contribute to sensemaking theory by identifying cognitive frames (i.e., security knowledge and attitude) and emotions as influential antecedents. We show that varying levels of security knowledge and experience lead employees to interpret and evaluate security-related incidents differently (Shreeve et al., 2023). And that negative emotions, such as frustration and concern, can trigger the sensemaking process by signaling a need to interpret and respond or make sense of unexpected events (Maitlis et al., 2013) Similarly, we find that how employees feel about security and policies will play a preliminary role on the sensemaking process of ERSBs.

Third, we extend the process model of sensemaking by showing how employees move through these stages. We reveal that employees begin by scanning for cues such as policy communications, organizational expectations, and environmental cues, then proceed to interpret these cues within their roles and responsibilities. This then shapes both their willingness to improve their security education and behaviors, as well as their participation in ERSBs. Therefore, we present a novel contribution to sensemaking and information security research by offering a preliminary framework outlining how these stages transpire to guide employees towards ERSBs.

5.2. Practical Implications

Our work offers important practical implications for organizations and information security practitioners. First, organizational security culture was found to shape how employees perceive their role in maintaining security. We therefore suggest that organizations and practitioners integrate security into their everyday practices and norms to encourage open dialogue and shared responsibility, regardless of roles and levels (Lin & Luo, 2021; Wiley et al., 2020). Second, our findings indicate policy communication gaps and varying levels of security knowledge that impede how employees comprehend and process ISPs. As sensemaking is driven by clear communication (Maitlis et al., 2013), it is critical that ISPs are communicated with transparency and proper explanations to enhance policy understanding, compliance, and ERSBs. Thus practitioners should design policies with clear language and contextual examples that are self-explanatory and easy to understand (Neil et al., 2025). Third, perceptions of policies and one's role in security are shaped by how policies and security are presented and discussed. By clarifying responsibilities and emphasizing the importance of security, employees are more likely to internalize and act on these roles beyond their expected duties (Frank & Kohn, 2023). Lastly, to encourage behaviors beyond what is prescribed, organizations should not only ensure ISP clarity but also strengthen SETA programs. Our findings reveal a bidirectional relationship between ERSBs and the antecedents of sensemaking. From a practical standpoint, this underscores the strategic value for organizations to invest in strengthening security knowledge, awareness, and culture to reduce knowledge gaps and support a proactive security culture (Neil et al., 2025). Overall, our findings provide a number of indications on the importance of a strong security culture, effective communication, and well-structured policies in shaping how employees make sense of individual and organizational cues for engaging in ERSBs. By applying these insights, practitioners can better design and communicate policies, promote security dialogue, and build a security-forward environment that encourages extra-role security behaviors.

5.3. Limitations and Future Research

While our work contributes to the understanding of sensemaking for ERSBs, we acknowledge certain limitations that offer opportunities for future research. First, this study would benefit from examining whether gender differences influence the sensemaking process, as prior research has shown that gender may affect information security perceptions and behaviors (McGill et al., 2018). Another promising direction is to explore the personal rhetoric around ERSB, that is, the language used by employees when thinking about information security. This is particularly relevant given research showing that self-confidence and intrinsic motivations influence whether employees engage in ERSBs (Frank & Kohn, 2023). Although our findings provide preliminary empirical contributions to sensemaking for ERSBs, we acknowledge the need for further studies to confirm our model. A logical next step would be to conduct a multi-case analysis to assess how sensemaking and its antecedents influence ERSBs across different roles, settings, and industries. Like many qualitative studies, our sample was drawn from large international corporations. This poses a limitation, as company characteristics (e.g., size, industry), culture, and SETA influence how company-wide ISPs are interpreted and followed (Flores et al., 2014).

6. Conclusion

This study contributes to information security research by proposing a sensemaking framework of

ERSBs that aims to explain how organizational and individual factors shape such behaviors within their organizations. The results confirm the effective role that security governance, policy and role perceptions, and willingness to change have on the sensemaking process leading to ERSBs. Additional insights gained highlight the relevance of organizational and individual antecedents such as security culture, cognitive frames, and emotions on sensemaking. As more employees engage in ERSBs, these behaviors become reinforced within the organization, further influencing these antecedents. Prior to this study, little was known about how employees make sense of ISPs, security-related cues, whether personal or environmental, and their own role in ways that lead them to perform ERSBs. Therefore, our work expands sensemaking theory and adds to the extant ERSB literature to examine how the sensemaking process of ERSBs transpires and the antecedental variables that influence it. With this, organizations must transparently communicate ISPs and security-related information to cultivate a company-wide environment that prioritizes security and encourages ERSBs for all roles and levels of experience.

Acknowledgments

This work was funded by Luxembourg's National Research Fund (FNR) and PayPal – PEARL grant ref. 13342933/Gilbert Fridgen. For open access purposes, the authors have applied a CC BY 4.0 license to any Author Accepted Manuscript arising from this submission.

References

Balozian, P., James Madison University, Burns, A. J., Louisiana State University, Leidner, D. E., & University of Virginia. (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. https://doi.org/10.17705/1jais.00798

Barr, P. S., & Huff, A. S. (1997). Seeing isn't Believing: Understanding Diversity in the Timing of Strategic Response. *Journal of Management Studies*, *34*(3), 337–370. https://doi.org/10.1111/1467-6486.00054

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

Daft, R. L., & Weick, K. E. (1984). Toward a Model of Organizations as Interpretation Systems^.

D'Arcy, J., & Greene, G. (2014). Security culture and the employment relationship as drivers of employees' security compliance. *Information Management & Computer Security*, *22*(5), 474–489. https://doi.org/10.1108/IMCS-08-2013-0057

Dupont, B., Shearing, C., Bernier, M., & Leukfeldt, R. (2023). The tensions of cyber-resilience: From sensemaking to practice. *Computers & Security*, *132*, 103372. https://doi.org/10.1016/j.cose.2023.103372

Flores, W., Antonsen, E., & Ekstedt, M. (2014). Information security knowledge sharing in organizations: Investigating the effect of behavioral information security governance and national culture. *Computers & Security*, *43*, 90–110. https://doi.org/10.1016/j.cose.2014.03.004

Frank, M., & Kohn, V. (2023). Understanding extra-role security behaviors: An integration of self-determination theory and construal level theory. *Computers & Security*, *132*, 103386. https://doi.org/10.1016/j.cose.2023.103386

Gioia, D. A., Corley, K. G., & Hamilton, A. L. (2013). Seeking Qualitative Rigor in Inductive Research: Notes on the Gioia Methodology. *Organizational Research Methods*, *16*(1), 15–31. https://doi.org/10.1177/1094428112452151

Hahn, T., Preuss, L., Pinkse, J., & Figge, F. (2014). Cognitive Frames in Corporate Sustainability: Managerial Sensemaking with Paradoxical and Business Case Frames. *Academy of Management Review*, *39*(4), 463–487. https://doi.org/10.5465/amr.2012.0341

Harris, S. G. (1994). Organizational Culture and Individual Sensemaking: A Schema-Based Perspective. *Organization Science*, *5*(3), 309–321. https://doi.org/10.1287/orsc.5.3.309

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 [Publisher: INFORMS]. *Information Systems Research*, *26*(2), 282–300. https://doi.org/10.1287/isre.2015.0569

Jaeger, L., & Eckhardt, A. (2018). When Colleagues Fail: Examining the Role of Information

Security Awareness on Extra-Role Security Behaviors.

Kim, Y. (2018). Enhancing Employee Communication Behaviors for Sensemaking and Sensegiving in Crisis Situations: Strategic Management Approach for Effective Internal Crisis Communication. *Journal of Communication Management*, *22*(4), 451–475.

Lakshmi, R., Naseer, H., Maynard, S., & Ahmad, A. (2021). Sensemaking in Cybersecurity Incident Response: The Interplay of Organizations, Technology, and Individuals. https://arxiv.org/abs/2107.02941

Li, Y., Stafford, T., Ellis, S., & Fuller, B. (2021). Beyond Extra-Role Security Behaviors in Large Corporate Settings: The Case of 'Tribal Security'. *SSRN Electronic Journal*. https://doi.org/10.2139/ssrn.3870574

Lin, C., & Luo, X. (2021). Toward a unified view of dynamic information security behaviors: Insights from organizational culture and sensemaking. *ACM SIGMIS Database: The DATABASE for Advances in Information Systems*, *52*(1), 65–90.

Maitlis, S., & Christianson, M. (2014). Sensemaking in organizations: Taking stock and moving forward [Place: United Kingdom Publisher: Taylor & Francis]. *The Academy of Management Annals*, *8*(1), 57–125. https://doi.org/10.1080/19416520.2014.873177

Maitlis, S., Vogus, T. J., & Lawrence, T. B. (2013). Sensemaking and emotion in organizations. *Organizational Psychology Review*, *3*(3), 222–247. https://doi.org/10.1177/2041386613489062

McGill, T., Thompson, N., & Curtin University, AU. (2018). Gender Differences in Information Security Perceptions and Behaviour. In *Australasian Conference on Information Systems 2018*. University of Technology, Sydney. https://doi.org/10.5130/acis2018.co

Myers, M. D., & Newman, M. (2007). The qualitative interview in IS research: Examining the craft. *Information and Organization*, *17*(1), 2–26. https://doi.org/10.1016/j.infoandorg.2006.11.001

Neil, L. C., Healy, C., & Haney, J. (2025). "A five-year-old could understand it" versus "This is way too confusing": Exploring Non-expert Understandings and Perceptions of Cybersecurity Definitions. https://doi.org/https://doi.org/10.1145/3706598.3713820

Podsakoff, P. M., MacKenzie, S. B., Lee, J.-Y., & Podsakoff, N. P. (2003). Common method biases in behavioral research: A critical review of the literature and recommended remedies. *Journal of Applied Psychology*, *88*(5), 879–903. https://doi.org/10.1037/0021-9010.88.5.879

Saldaña, J. (2013). *The coding manual for qualitative researchers* (2. ed). SAGE Publ.

Shreeve, B., Gralha, C., Rashid, A., Araújo, J., & Goulão, M. (2023). Making Sense of the Unknown: How Managers Make Cyber Security Decisions. *ACM Trans. Softw. Eng. Methodol.*, *32*(4), 83:1–83:33. https://doi.org/10.1145/3548682

Silverio, S. A., Sheen, K. S., Bramante, A., Knighting, K., Koops, T. U., Montgomery, E., November, L., Soulsby, L. K., Stevenson, J. H., Watkins, M., Easter, A., & Sandall, J. (2022). Sensitive, Challenging, and Difficult Topics: Experiences and Practical Considerations for Qualitative Researchers. *International Journal of Qualitative Methods*, *21*, 16094069221124739. https://doi.org/10.1177/16094069221124739

Van Dyne, L., Cummings, L., & McLean Parks, J. (1995). Extra-role behaviours: In pursuit of construct and definitional clarity (a bridge over muddied waters). *17*, 215–285.

Vedadi, A., Mirsadikov, A., & Warkentin, M. (2025). Unraveling the Psychological Links Between Organizational Security Climate and Extra-Role Security Behaviors. *Information & Management*, 104181. https://doi.org/10.1016/j.im.2025.104181

Weick, K. E. (1995). *Sensemaking in organizations* (Nachdr.). Sage Publ.

Weick, K. E., Sutcliffe, K. M., & Obstfeld, D. (2005). Organizing and the Process of Sensemaking. *Organization Science*, *16*(4), 409–421. https://doi.org/10.4337/9781849807630

Wiley, A., McCormac, A., & Calic, D. (2020). More than the individual: Examining the relationship between culture and Information Security Awareness. *Computers & Security*, *88*, 101640. https://doi.org/10.1016/j.cose.2019.101640

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. https://doi.org/10.1111/isj.12488