June 2026

Boundary Management And Cybersecurity Behavior In Remote Work: Insights From An Empirical Study.

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

Daria Levaniuk
LUT University, daria.levaniuk@lut.fi

Sandra Ebojoh
University West, sandra.ebojoh@hv.se

Bilal Naqvi
LUT University, syed.naqvi@lut.fi

BOUNDARY MANAGEMENT AND CYBERSECURITY BEHAVIOR IN REMOTE WORK: INSIGHTS FROM AN EMPIRICAL STUDY.

Completed Research Paper

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

Daria Levaniuk, LUT University, Lappeenranta, Finland, daria.levaniuk@lut.fi

Sandra Ebojoh, University West, Trollhättan, Sweden, sandra.ebojoh@hv.se

Bilal Naqvi, LUT University, Lappeenranta, Finland, syed.naqvi@lut.fi

Abstract

This study investigates how remote workers' boundary management strategies shape cybersecurity behavior in everyday contexts. Drawing on Boundary Management Theory and qualitative data from 14 interviews with remote workers across Europe, we identified three strategies: segmentation, integration, and blurred boundaries that influence how individuals engage with cybersecurity routines. Our findings show that boundary strategies affect the stability, consistency, and cognitive demands of secure behavior. Clear boundaries support routine compliance, while blurred boundaries increase risk through distraction, fatigue, and role conflict. Organizational factors such as policy clarity, tool usability, and leadership expectations further shape how employees sustain secure practices in distributed work settings. This study contributes to IS security research by highlighting boundary management as an important context for understanding behavioral cybersecurity in remote work. We offer practical implications for designing boundary-aware policies and tools that better support secure practices in remote and hybrid environments

Keywords: Boundary Management, Remote work, Cybersecurity, Organizations.

1 Introduction

Remote work has permanently redefined how individuals and organizations interact with digital systems. Accelerated by the COVID-19 pandemic, remote work has transitioned from an emergency adaptation to a mainstream employment model across sectors (Galanti et al., 2021). This shift has brought significant benefits in terms of flexibility and productivity, but also profound cybersecurity challenges. The expansion of the security perimeter beyond traditional office settings, especially through remote work, has introduced new vulnerabilities driven more by human behavior and employee practices than by technology alone (Jayarao et al., 2024; Nwankpa & Datta, 2023). Existing security architectures are grounded in assumptions of centralized infrastructure, controlled environments, and standardized routines. Evolving threats, emerging technologies, and the variability of user behavior in dynamic work settings increasingly challenge these assumptions (McLaughlin & Gogan, 2018). Remote workers, however, often operate in decentralized and blended environments, relying on a mix of personal and organizational devices, unsecured home networks, and external communication channels that fall outside the organization's direct control (Qollakaj et al., 2025). These conditions increase exposure to phishing, credential theft, and accidental data leakage. However, more critically, they require individuals to self-regulate cybersecurity behavior without immediate oversight, a task complicated by fatigue, digital stress, and context-switching (Alashwali et al., 2025; Maleksaeedi et al., 2025; Singh et al., 2022).

While Information Systems (IS) research has made significant strides in understanding security policy compliance, threat avoidance, and awareness (Donalds & Barclay, 2022; Herath & Rao, 2009; Liang et al., 2010; Nastjuk et al., 2025), these models often treat user behavior as a reaction to perceived threats or deterrents. Recent studies indicate that remote work environments reshape this relationship, with user values, personal routines, and daily life structures emerging as key determinants of secure behavior (Alashwali et al., 2025; Torres & Crossler, 2025). However, the IS field has yet to fully examine how blended work–life boundaries in remote contexts influence cybersecurity behavior and related routines. Boundary Management Theory (Ashforth et al., 2000) offers a promising lens to address this gap. It helps explain how people balance work and personal life, either by keeping them separate or blending them depending on their routines, preferences, and environment. While this theory has been widely applied in organizational and HR research (Kossek et al., 2023; Piszczek & Berg, 2014; Zhao, 2023), its relevance to cybersecurity behavior in information systems remains underexplored. Given the behavioral and environmental complexities of remote work, understanding how boundary strategies influence secure behavior is critical to IS research.

Moreover, recent IS literature has called for greater attention to the contextual and cultural dimensions of security behavior, moving beyond individual intention toward understanding how routines, stressors, and environments shape actual outcomes (Crossler et al., 2013; Posey et al., 2015). For example, Amo et al.(2022) highlight that perceived control over technology use (or rather, the lack thereof, in the form of restrictions) plays a significant role in how technological entitlement manifests in risky behaviors, while lack of organizational support often forces employees to improvise insecure solutions (Nwankpa & Datta, 2023).

To address this gap, our study investigates how remote workers' boundary management strategies influence their cybersecurity behavior in everyday work contexts. We seek to identify how these strategies enable or hinder the adoption of secure practices in remote work contexts through qualitative interviews with remote workers. The following research question guides this study:

RQ: How do boundary management strategies influence cybersecurity behavior among remote workers?

This study explores how behavioral security is shaped by the spatial, temporal, and cognitive dynamics of remote work, with particular attention to how individuals manage boundaries across life domains.

2 Literature Review

2.1 Cybersecurity in Remote Work Contexts

As organizations shift toward remote and hybrid models, cybersecurity threats become more diffuse and behavior dependent. Recent studies show that remote access mechanisms such as VPNs, remote desktops, and cloud-based services are increasingly targeted by attackers exploiting weak endpoints and user misconfigurations (Qollakaj et al., 2025). The shift to remote and hybrid work has exposed the limits of traditional, perimeter-based security, replacing institutional control with individual responsibility and requiring new forms of digital trust, leadership, and vigilance to sustain secure behavior in decentralized environments (Nwankpa & Datta, 2023; Östergård et al., 2025). Employees may trade convenience for security in remote settings, such as bypassing multi-factor authentication or disabling security tools under time pressure or connectivity constraints. Simultaneously, organizational readiness to support secure remote work remains uneven. Jayarao et al. (2024) note that many firms, particularly small and medium-sized enterprises (SMEs), lack proactive policies and infrastructure to address remote-specific risks. As a result, the human element becomes central; when organizational tools are insufficient or cumbersome, employees often resort to informal workarounds or shadow IT solutions to maintain productivity (Haag & Eckhardt, 2024). These adaptive behaviors highlight a disconnect between formal security protocols and the lived realities of remote work, raising critical questions about how security policies align with actual work practices.

A recent interdisciplinary review of human factors in cybersecurity highlights that technology alone cannot close security gaps; instead, factors such as organizational culture, trust, fatigue, cognitive load, and behavioral patterns must be addressed in an integrated manner (Khadka & Ullah, 2025). The review calls for socio-technical frameworks that combine user psychology, training, and incentive structures with system design to foster more sustainable and secure behavior in complex work environments. Alotaibi et al. (2023) emphasize the importance of personalization in cybersecurity, noting that different professional groups may require tailored security policies and interface designs. This challenges the effectiveness of one-size-fits-all approaches, particularly in the context of diverse and distributed remote workforces. While prior research by Nizamuddin (2025) has acknowledged cybersecurity challenges in remote work, there is a limited understanding of how and why users deviate from policy regarding boundary management practices, especially when work-life boundaries conflict.

2.2 Human-Centered and Behavioral Security in IS

IS scholars have long studied the human and behavioral dimensions of cybersecurity, primarily through models such as Protection Motivation Theory (PMT), Theory of Planned Behavior (TPB), and Technology Threat Avoidance Theory (TTAT) (Herath & Rao, 2009; Ifinedo, 2012; Liang et al., 2010). These frameworks highlight perceived severity, self-efficacy, response cost, normative pressures, and intention–behavior relationships. However, a common critique of intention-based models is that they overlook the situational and contextual factors that influence behavior in practice, failing to account for deviations that occur in everyday work settings (Siponen et al., 2024). For example, an employee may intend to comply with security policies but neglect them during extended work sessions due to fatigue or distraction, factors often overlooked in traditional intention-based models.

Recent studies are pushing toward more context-aware, dynamic models. Hwang and Cha (2018) demonstrate that security-related technostress can erode compliance intention, particularly in environments where organizational commitment is low and role-related stress is high, highlighting the importance of context in shaping secure behavior. Similarly, Grobler et al. (2021) advocate for a shift toward human-centric cybersecurity, emphasizing the need to foreground usability, cognitive load, and human error in system and policy design. Complementing this, Hilowle et al. (2023) discuss human error, social engineering, and insider mistakes as significant concerns in human-centric cybersecurity and suggest that strategies must include behavioral countermeasures and training. This human-centered security research reframes compliance as a dynamic negotiation between users, systems, and organizational context. In remote work, this negotiation intensifies as employees navigate boundaries

and greater autonomy. Security behavior increasingly depends on how individuals manage roles, routines, and environments.

2.3 Boundary Management Theory & Work–Life Boundaries

Boundary Management Theory (Ashforth et al., 2000) offers a valuable lens for understanding how individuals navigate the overlap between work and personal life, particularly in remote or hybrid work environments where spatial and temporal boundaries are less defined. The theory proposes that individuals fall along a continuum between segmentation and integration. Segmenters prefer clear separation between work and personal roles, while integrators are more comfortable blending these domains. These preferences shape how individuals manage their time, space, and behaviors throughout the workday.

To maintain their preferred boundary structures, individuals adopt a range of boundary management techniques. Carlson et al. (2016) identify four key techniques: temporal, physical, behavioral, and communicative. Temporal techniques involve setting strict work hours, scheduling breaks, or turning off work-related notifications after hours. Physical strategies involve creating spatial separation, for example, by establishing dedicated workspaces within the home environment. Behavioral strategies include actions that signal role transitions, such as logging out of work systems or avoiding work-related applications during personal time. Communicative strategies involve setting expectations with colleagues or family members about availability and work boundaries (Carlson et al., 2016; Pensar & Rousi, 2023).

These boundary techniques help individuals manage role transitions and reduce work–life conflict, but they may also affect cybersecurity practices. For example, remote work environments that rely on personal devices or home networks may introduce vulnerabilities, including insecure connections, device misuse, and increased exposure to phishing and social engineering risks (Nizamuddin, 2025). Boundary strategies, therefore, influence not only work–life balance but also how and when digital systems are accessed, monitored, and protected.

Building on this perspective, this study applies Boundary Management Theory to examine how remote workers' boundary strategies shape cybersecurity behavior in everyday work contexts. By analyzing how segmentation, integration, and boundary blurring influence security practices, the study seeks to reveal how routine boundary management choices can support or undermine consistent cybersecurity behavior in distributed work environments.

3 Methodology

This study adopts an interpretivist qualitative research approach to understand how remote workers' boundary management strategies shape cybersecurity behaviors. The interpretivist stance assumes that reality is socially constructed and emphasizes understanding meanings and behaviors through participants' lived experiences within specific contexts (Klein & Myers, 1999; Walsham, 2006).

We selected semi-structured interviews as our data collection method to explore how individuals make sense of, enact, and navigate security behaviors within the boundaries of remote work. Qualitative inquiry is particularly suited for examining context-dependent practices that are not easily captured through surveys or controlled experiments (Myers & Newman, 2007). Our focus on experiences, routines, and organizational contexts aligns with a growing stream of human-centered IS research examining user behavior, compliance, and security culture through interpretive methods (Schuetz et al., 2025).

3.1 Sampling

We used purposive sampling (Campbell et al., 2020) to identify remote workers with meaningful experience in remote or hybrid work contexts. Eligibility criteria included:

1. Working remotely at least two days per week.

2. Engaging in regular digital or information-oriented tasks as part of remote work (e.g., communication, document handling, system use, or online collaboration).
3. Exposure to cybersecurity-relevant routines, tools, or policies.

A total of 14 participants were recruited from Finland, Sweden, the United Kingdom, and the Netherlands, across both large and small-to-medium organizations. Participants varied by gender, role, and organizational support structures to ensure diverse perspectives on boundary and security practices (see Table 1). Recruitment was conducted through professional networks and academic contacts, following purposive sampling strategies common in interpretive IS research, where depth and contextual relevance are prioritized over representativeness (Walsham, 2006).

Category	**Summary**
Gender	Female: 8; Male: 6
Remote Work Models	Fully Remote: 5; Hybrid: 9
Industries Represented	IT, Education/Academia, Journalism, Consultancy, Marketing
Countries Represented	Finland: 7; Sweden: 4; UK: 2; Netherlands: 1
Remote Work Experience	Median duration = 3.5 years
Total Respondents	14

Table 1: Demographic breakdown of the study participants'

3.2 Data Collection

Three research team members participated in data collection, enabling broad engagement with participants and mitigating individual researcher bias. Semi-structured interviews were conducted remotely through Microsoft Teams between October 2024 and March 2025. The interviews lasted between 45 and 60 minutes. All interviews were recorded with participant consent, transcribed, and anonymized to ensure confidentiality.

The interview guide focused on three thematic areas:

1. Remote Work: Participants described their remote work setup, frequency, tools used, and organizational policies.
2. Boundary Management Practices: We explored how participants manage the separation or integration of their work and personal lives, including strategies related to time, space, behavior, and communication.
3. Cybersecurity Practices: The final section examined participants' cybersecurity behaviors, awareness, and how their boundary management strategies may influence secure or insecure practices when working remotely.

This design allowed for depth while maintaining structure across the interviews. As Myers and Newman (2007) recommended, we used open-ended questions, and interviewees could freely express their experiences in their own words. This approach helped reduce bias and obtain rich, detailed information.

3.3 Data Analysis

We conducted a thematic analysis using a collaborative, multi-stage process to ensure analytical depth and interpretive rigor. Given the sample size, we opted for manual coding to enable close, researcher-led engagement with the data. Our analysis followed Braun and Clarke's (2006) six-phase framework, enriched by a structured coding process inspired by Gioia et al. (2013), as is commonly used in interpretive IS research (e.g., Laato et al., 2025). In the familiarization phase, all four researchers independently read and annotated the transcripts, maintaining reflexive notes to identify early patterns and reduce bias. The first author then conducted detailed, line-by-line open coding to generate first-

order codes grounded in participant language and experiences. These codes captured behaviors, routines, emotional responses, and organizational conditions related to cybersecurity in remote work. The team collaboratively developed second-order themes through iterative discussions that challenged interpretations and built consensus, enhancing theoretical sensitivity. Coding disagreements were resolved through negotiated agreement, with all researchers revisiting transcript segments until a shared understanding was reached. We also examined possible cross-country differences by reviewing country-coded data, but no systematic variation emerged, allowing us to treat the dataset holistically while acknowledging contextual nuances. The final thematic structure coherently linked boundary strategies, organizational conditions, and cybersecurity behavior.

3.4 Ethical Considerations

Ethical approval was secured through the lead institution's ethics review board. Participants were given an information sheet outlining the study's purpose, their rights, and data-handling protocols. Informed consent was obtained before interviews. All transcripts were anonymized and securely stored.

4 Findings

Participants reported diverse and often contrasting experiences across three interconnected areas: remote work setups, boundary management practices, and cybersecurity behaviors. These accounts reveal that security outcomes in remote settings are shaped not only by technology but also by daily routines, work environments, and the degree of organizational support. In this context, secure behavior emerges as much from lived experience as from formal systems and tools.

4.1 Physical Boundaries as Foundations for Boundary Management

Although participants' remote work arrangements varied widely (see Table 2), physical boundaries within home environments played a central role in shaping their daily routines and security behavior. Boundary Management Theory notes that spatial boundaries are a primary mechanism through which individuals regulate transitions between work and personal life (Ashforth et al., 2000). Our findings show that these spatial conditions provided the foundation for boundary strategies, influencing workers' ability to maintain stable, secure routines.

Participants with dedicated workspaces, such as home offices or secluded desk areas, described greater control over interruptions, privacy, and device separation. These spatial boundaries enabled clearer psychological separation between roles and supported consistent security practices. As one participant explained, *"I close the door, so I don't get distracted; it keeps me focused on work" (P7*). Such environments align with segmented boundary strategies and facilitate behaviors such as careful email checking and reduced device sharing.

By contrast, participants working from shared or makeshift spaces such as kitchen tables, living rooms, or bedrooms experienced blurred boundaries marked by noise, movement, and limited privacy*: "We do not have space to put an additional office" (P3)*. These conditions undermined workers' ability to manage transitions, leading to increased multitasking and security lapses.

Employer support further shaped boundary conditions. Full remote-work kits reinforced spatial and digital segmentation, while limited support increased reliance on personal devices and unsecured networks. Physical environments served as core enablers or limitations, shaping boundary strategies and influencing cybersecurity behavior.

Physical Boundary Condition	Summary	Boundary Shaping Strategy
Dedicated workspace	Home office, defined desk area, door separation	Supports segmentation by creating clear spatial cues and reducing role overlap

Shared or makeshift spaces	Kitchen table, living room, shared bedroom	Produces blurred boundaries due to noise, interruptions, and limited privacy
Employer-provided equipment	Secure laptops, monitors, and docking stations	Reinforces digital separation and strengthens segmentation
Use of personal equipment	Limited employer support	Weakens spatial and digital boundaries; encourages integration or blurred boundaries
Low environmental control	Noise, light, temperature, and shared household areas	Makes segmentation difficult and increases blurred-boundary conditions

Table 2: Remote Work Physical Boundary Conditions

4.2 Boundary Management Practices

How remote workers manage the boundary between work and personal life has significant implications for cybersecurity, often more than organizations anticipate. In our study, participants described three distinct boundary management approaches: segmented, integrated, and blurred. These approaches shaped how individuals structured their daily routines and consistently adhered to secure practices in remote work settings (see Table 3).

4.2.1 Segmenters: Drawing the Line

Several participants demonstrated segmentation strategies that separated work from personal life. This emerged from recurring patterns where some participants described fixed working hours, distinct workspaces, and device separation. For example, one participant noted, *"I have two laptops, one for work, one for personal stuff" (P6),* while another explained, *"I converted a spare room into a private office with the door closed to minimize distractions" (P7).* These behaviors reflected deliberate efforts to create spatial and temporal boundaries.

The findings also showed that segmentation supported more stable cybersecurity routines. Participants described how separating devices and spaces reduced multitasking with sensitive information and discouraged the use of personal applications for work. One participant explained that removing work email from their phone *"helps me disconnect" (P6),* reducing opportunities for cross-use of accounts or data. These patterns align with Boundary Management Theory, which argues that stronger spatial and temporal boundaries support clearer role transitions and more consistent behavior.

However, segmentation was not absolute. None of the participants described explicit communicative boundaries, such as negotiated expectations with family or colleagues, leaving even structured arrangements vulnerable to interruption during stress or an increased workload. This suggests that segmentation supported secure practices but remained incomplete.

4.2.2 Integrators: Blending Work and Life by Design

In contrast to segmenters, some participants adopted integration as a deliberate boundary strategy, blending work and personal life throughout the day. One participant said, *"It is all mixed." (P3).* These individuals did not attempt to maintain strict separation between domains but instead designed routines that allowed for constant switching between roles. For example, participants described moving between virtual meetings and caregiving tasks, often using Bluetooth headsets to stay connected while attending to non-work responsibilities. *"I use a Bluetooth headset to allow me to walk over to the kitchen or something, even if I am on a call." (P1).* Others practiced time blocking to balance professional and personal commitments or intentionally used the same device for both contexts.

This integration was not accidental but strategic, designed to optimize flexibility, autonomy, and responsiveness. However, this fluidity introduced new complexities for cybersecurity behavior. The

absence of clear temporal or spatial boundaries made it more difficult to sustain consistent security routines. Multitasking increased the risk of oversight, such as clicking on phishing links or failing to log out of sensitive systems, as one participant described*: "I was a victim of this cybersecurity phishing scam, and I lost €600." I was traveling, I was at the airport, "I didn't check the actual e-mail. I only saw the initials and then the person's name, thinking it was my professor, but the actual e-mail was rubbish." "It was just right after I sent it that the IT replied that this particular e-mail has been classified as a phishing e-mail."(P4)*. This incident demonstrates that boundary integration can support flexibility and responsiveness but also weaken cybersecurity vigilance by enabling decisions outside of secure, focused work contexts. Furthermore, shared devices and unclear role contexts increased the risk of data exposure, particularly when organizational tools lacked usability or context-aware safeguards.

4.2.3 Blurred Boundaries: When Structure Breaks Down

A distinct pattern involved participants whose boundaries between work and personal life had collapsed. This emerged from accounts in which integration was not a deliberate preference but a response to environmental or organizational constraints. One participant described using a single phone for all work and personal activities, email, messaging, social media, and authentication, stating*, "My phone is also my work phone, it's all connected" and "I think it might be possible to get on my computer via my phone" (P5).* Although aware of security risks, such as not using a VPN, some participants reported lacking alternatives due to device or policy limitations. These narratives indicated boundary blurring driven by necessity, not choice.

Participants working from shared spaces with limited privacy or inconsistent routines described similar challenges. Without stable physical, temporal, or digital boundaries, they struggled to maintain secure practices. For example, *(P2)* stated, *"If my husband is at home in the evening, then it's harder to concentrate"*. This pointed to chances of data exposure, mixed-use behaviors, and fatigue-induced errors. Consistent with Boundary Management Theory, blurred boundaries undermined workers' ability to regulate role transitions, making it difficult to sustain secure behavior. In these contexts, lapses reflected constraints, not individual negligence.

Boundary Strategy	**Sub-Theme**	**Boundary practices**
Segmentation	Temporal/Spatial	Fixed work hours, scheduled breaks, and structured start/end routines, dedicated home office, closed door, defined desk area
	Behavioral	Mental cues (e.g., closing laptop, post-work exercise); role-switching rituals.
	Technological	Use of separate devices for work/personal use; disabling notifications after work hours.
Integration	Role integration	Flexible schedules that align with personal responsibilities (e.g., childcare, errands); shared device use with intentional time blocking; seamless transitions between personal and work tasks.
Blurred Boundaries	Boundary erosion and instability	Little to no separation between work and personal life; shared devices and spaces; difficulty disconnecting; frequent task switching without clear transitions

Table 3: Boundary Management Practices

Participants across industries described conditions in which boundaries between work and personal life eroded to the point of collapse. This emerged from recurring accounts of physical constraints, cultural expectations, and emotional pressures that collectively produced blurred boundary conditions. Physically, several participants reported working from shared or unstable spaces, *"We have the kitchen table, that is also my working space." (P2); "I just have my laptop, and then I use the normal kitchen table and a kitchen chair, so there is nothing extra. I can just pick up and go anywhere." (P8).* These environments lacked the spatial cues necessary to maintain separation, leading to continuous movement and interruptions. Cultural pressures further weakened boundaries. Some organizations operated with

limited planning or buffer time, generating expectations of constant responsiveness*: "They do not plan, I'm in a position where I am forced to react in a short period of time." (P3).* This reactivity intensified role overlaps, making it difficult for participants to regulate transitions. Emotional strain added another layer. Feelings of guilt, isolation, and helplessness were frequently mentioned: *"I can't complain and say, ' No, I don't want to do it because that's what they pay me for." So, it's kind of like let us hope nothing bad happens." "It's not optimal, but at the moment, I just have to deal with it."(P9).* Another indicated, *"I would love to allocate time if it were possible, but at the moment it's not because of how the work is." (P11).* These emotional states reduced the capacity for sustained focus.

These conditions illustrated blurred boundary strategies as described in Boundary Management Theory. As physical, temporal, and cultural boundaries weakened, some participants reported experiencing fewer stable moments in which to enact secure practices. Participants described lapses linked to fatigue, rushing, or multitasking, including missed alerts, reused passwords, and accidental data exposure. Thus, blurred boundaries directly undermined the attentional stability required for cybersecurity resilience

4.3 Boundary Conditions and Cybersecurity Practices

Participants demonstrated awareness of basic cybersecurity principles, but our analysis revealed a consistent gap between knowledge and practice, largely shaped by two interacting factors: (1) the strength of participants' boundary structures, and (2) the degree of organizational support available to them. These conditions determined whether secure practices could be sustained in daily routines.

Although many participants reported using tools such as VPNs, 2FA, and password managers, implementation varied. Some described efforts to act securely, *"I try to do what I can, like not put my password in public places and change it" (P12).* Another indicated, *"I also like to delete many of the old accounts I do not use."(P13).* However, others lacked the technical means or support to maintain secure behavior: *"They do not have any VPN, so I might be more vulnerable to attacks at home." "They needed training themselves." "They do not take it seriously." (P14).* In contrast, participants whose organizations enforced onboarding procedures or automated compliance described more consistent routines: *"I had to meet the chief security person to go through the protocol and the policies." "If you do not change your password, you just get kicked out of your own systems." (P6).*

Cybersecurity practices were closely shaped by the boundary conditions under which employees worked. Segmentation cues, such as dedicated workspaces, predictable routines, and clear organizational guidance, helped stabilize security behaviors and support consistent practices, such as routine VPN use and regular password updates. In contrast, integration cues and boundary blurring, including multitasking, device convergence, and shared work environments, disrupted these routines and increased the likelihood of shortcuts or inconsistent security practices. These patterns illustrate how cybersecurity knowledge was enacted differently across everyday work contexts. Table 4 summarizes how segmentation cues, integration cues, and boundary blurring influenced the enactment of common cybersecurity practices and shaped employees' ability to maintain secure behavior in remote work environments.

Cybersecurity Practice	**Segmentation Cues**	**Integration Cues**	**Blurring Pressures**
Use of VPN / Secure Networks	Dedicated work device; routine login patterns; stable workspace with reliable network access	Switching between devices; using one device for all accounts; concurrent personal–work tasks	No VPN provided; unstable workspace; reliance on shared household networks
Multi-Factor Authentication (MFA)	Mandatory enforcement; integrated authentication systems; predictable work hours	Checking authentication codes while multitasking; MFA prompts arriving across personal and work apps	Device convergence, rushed logins, and a lack of policy clarity

Device Separation	Separate work and personal devices; physical workspace cues that signal "work mode."	Using one phone/laptop for everything	No employer-provided hardware; shared spaces; constant movement
Password Management	Enforced resets, password managers, and clear protocols	Saving passwords across apps; reusing credentials for convenience	Stress, fatigue, or interruptions
Avoidance of Risky Networks	Routine of working in a stable environment; clear expectations	Using mobile hotspots for both personal and work tasks.	Public Wi-Fi use due to mobility; improvised setups
Secure Communication	Using organization-approved tools (Teams, encrypted email)	Switching between unapproved tools for work–personal coordination	Lack of policy clarity; fragmented toolsets
Organizational Policies & IT Support	Clear protocols; responsive IT; integrated digital systems	Occasional reliance on personal troubleshooting; hybrid use of personal apps	Lack of digital maturity; ad hoc support
Challenges in Compliance	Usable tools; supportive routines; stable segmentation	Multitasking, emotional strain, and guilt-driven responsiveness	Unpredictable schedules; interruptions; resource constraints

Table 4: Boundary Conditions and Cybersecurity Practices

4.3.1 Security Falls to the Individual

Although boundary strategies involve personal regulation, our findings show that individual responsibility for cybersecurity often emerged not by choice but by necessity. Participants repeatedly described minimal organizational guidance, weak policies, and overstretched IT support, which left them to manage security independently. As one participant noted, *"100% of my cybersecurity knowledge comes from my line of work, not the organization" (P2).* In this context, employees may improvise routines that sometimes introduce risk, such as storing both personal and work content on a single device or reusing credentials. Stress intensified these patterns, as reflected in accounts such as *"We do what we do when we are stressed" (P10).*

These behaviors do not simply reflect personal preferences but responses to structural limitations. When organizations lack clear policies, usable tools, or reliable support, responsibility for maintaining cybersecurity shifts to individual employees. Participants' accounts show how workers fill these gaps with improvised solutions, often under conditions of time pressure or uncertainty. As a result, security practices become inconsistent, and vulnerabilities increase, illustrating how weak organizational structures place the burden of cybersecurity management on individuals.

4.3.2 Training: Inconsistent, Infrequent, and Ignored

Cybersecurity training was widely described as inconsistent, infrequent, and poorly aligned with the realities of remote work. Participants recalled basic onboarding modules: *"We have an annual cybersecurity training that everyone has to take." (P1).* That focused mainly on phishing: *"If there is a real threat like phishing, we get emails or warnings, sometimes even pop-ups in the system." (P4).* Beyond this initial exposure, the quality and relevance of training varied considerably, and some questioned whether the trainers themselves possessed adequate knowledge. *"They needed cybersecurity training themselves. They do not know how to promote any of those things." (P3).* Many found the material repetitive or outdated, *"It is the same thing every year." (P12).* and disconnected from emerging threats, including AI-enabled *attack "They do not talk about new stuff like deepfakes or AI phishing attacks." (P13).*

The effectiveness of this training became clearer when viewed through the lens of boundary strategies. Participants with segmented boundary structures, dedicated workspaces, predictable schedules, and

device separation described fewer barriers to integrating training recommendations into daily routines. Their stable environments created moments of continuity in which secure practices could be performed. In contrast, those working within blurred boundaries encountered substantial difficulty applying training principles. Accounts of interruptions, shared-device arrangements, and rapid context switching highlighted conditions that training materials did not anticipate, leaving participants without strategies to manage security during fragmented or multitasking work.

Annual slide-based modules offered little guidance for workers shifting between household responsibilities, moving across spaces, or relying on personal devices. As a result, employees in blurred boundary conditions often reverted to ad hoc decisions or habitual shortcuts, not because of negligence, but because training did not align with the environments in which security decisions were made. The shortcomings of training reflected a broader misalignment between organizational expectations and the boundary structures shaping remote workers' daily practices.

4.3.3 Boundaries as Predictors of Risk

Our analysis showed that employees' boundary strategies were strongly associated with their exposure to cybersecurity risk. Blurred boundaries, including working outside fixed hours, sharing devices, and juggling personal and professional tasks, were repeatedly linked to lapses such as missed phishing cues or mishandling sensitive information due to fatigue or cognitive overload. In contrast, segmented boundaries supported clearer routines and reduced error rates, as indicated by one participant,*" Cybersecurity training stipulates technical separation between private life and university life." (P6).* These strategies, however, were shaped by organizational conditions: employees in flexible, well-supported environments managed risk more effectively, whereas those facing rigid or unsupported arrangements relied on unsafe workarounds.

The patterns that followed from these boundary conditions showed that weak or unstable boundaries consistently aligned with higher cybersecurity exposure. Situations such as device convergence, after work hours, and blurred physical spaces created recognizable points of vulnerability, whereas stronger segmentation tended to support more stable and secure routines. These outcomes were shaped by the broader organizational environment: employees with clear policies, usable tools, and ongoing training were better able to sustain secure practices, while those in rigid or unsupported settings often relied on improvised workarounds that increased their risk. (see Table 5).

Boundary Breakdown	**Cybersecurity Risk Pattern**
Blurred Boundaries	Reduced vigilance; higher susceptibility to phishing and accidental exposure
Personal Device Usage	Security controls bypassed; Mixing work and personal data
After-Hours Accessibility	Fatigue-driven errors; missed warnings during periods of low attention
Fatigue and Distractions	Impaired decision-making; weakened adherence to security practices.
Strong Segmentation	Improved security compliance and reduced exposure to security risk.
Organizational Gaps	Employees forced into improvised or inconsistent security practices
Inflexible Security Protocols	Workarounds that introduce unintended vulnerabilities

Table 5: Boundary-Driven Cybersecurity Risk Patterns

4.4 Organizational Boundary Support

Building on the individual-level boundary dynamics discussed earlier, participants also described organizational conditions that shaped the stability of those boundaries. These institutional factors, ranging from digital maturity to the clarity of security protocols, formed the broader frame within which individual boundary strategies operated. A recurring pattern involved contrasts between structured organizational environments, where security expectations were integrated into daily workflows, and

more fragmented settings lacking consistent support. Participants who described coherent organizational infrastructures reported greater stability in their boundary management. Integrated authentication systems and clear protocols supported predictable routines and reduced reliance on personal discretion.

As one participant noted, *"We cannot log in, for example, to Teams without the company's verification; the hardware needs to be registered to the company." (P6).* Leadership cues also played a role in reinforcing secure habits, with some employees recounting small but consistent reminders from managers that helped maintain separation between work and personal tasks: *"My old boss would always type 'I am the best boss ever' in Word whenever I forgot to lock my computer, just to remind me to log off when I left my desk." (P14).*

In contrast, participants embedded in less digitally mature or loosely organized environments experienced blurred boundaries and greater vulnerability. Limited IT support, resistance to digital tools, or inconsistent guidance required employees to improvise security practices. One participant explained, *"They are very old school, and they also try to refuse everything digital."(P3).* These conditions made it difficult to establish stable routines, particularly when combined with interruptions or resource constraints within the home environment.

This inconsistency extends Boundary Management Theory by showing that boundary strength in remote work is materially shaped not only by personal preference or spatial conditions but also by organizational arrangements. When institutional structures are weak, employees rely on stopgap strategies shaped by contextual pressures, increasing inconsistency and exposure to risk.

5 Discussion

This study examined how remote workers' boundary management strategies shape cybersecurity behavior. While prior IS security research has largely focused on intentions, awareness, and compliance, our findings show that cybersecurity behavior is also structured by everyday boundary conditions that organize how work is performed in remote environments. Drawing on Boundary Management Theory (Ashforth et al., 2000) and interview data from remote workers across multiple sectors and countries, we demonstrate how segmentation, integration, and blurred boundaries operate as behavioral infrastructures that shape how security practices are enacted in daily work. Importantly, our findings extend existing literature by showing that these boundary conditions do not simply influence work-life balance but also create predictable patterns of cybersecurity resilience and vulnerability. In doing so, we introduce boundary management as an explanatory lens for understanding how secure and insecure practices emerge in remote work contexts. These insights contribute to IS security research by reframing cybersecurity behavior as a contextually embedded phenomenon shaped by the interaction between personal boundary strategies and organizational environments. We outline these theoretical contributions and their practical implications below.

5.1 Cybersecurity as Boundary-Embedded Behavior

Cybersecurity behavior in remote work environments is closely shaped by the boundary structures through which employees organize everyday work. Rather than functioning solely as individual compliance decisions, security practices emerge within routines structured by spatial, temporal, and technological boundaries. When these boundaries are stable, employees are better able to sustain repeatable security routines because attentional resources remain focused and work tasks are organized in predictable ways.

In contrast, environments characterized by interruptions, multitasking, and overlapping personal and professional activities create conditions that fragment attention and increase the likelihood of security lapses. Similar dynamics have been linked to work–home interference and reduced attentional capacity in boundary management research (Brogle et al., 2024; Trieu et al., 2021). Viewed through this lens, boundary management operates as a behavioral infrastructure that shapes when and how cybersecurity practices are enacted in distributed work environments.

5.2 Boundary–Security Typology of Remote Workers

Building on the role of boundary structures in shaping cybersecurity behavior, the study identified three recurring boundary strategies through which security practices are enacted in remote work environments: segmentation, integration, and boundary blurring. These strategies do not simply reflect individual preferences but rather represent distinct ways in which employees organize work routines and manage security-related tasks in everyday practice. Segmented boundary structures tend to stabilize cybersecurity routines by supporting predictable work patterns, while integration and boundary blurring introduce interruptions, device convergence, and competing demands that make consistent security behavior more difficult to sustain.

This boundary–security typology highlights how employees' work–life structures influence the enactment of cybersecurity practices. In doing so, it addresses an important gap in existing IS security research, which has largely examined security behavior through individual-level factors such as knowledge, attitudes, or compliance intentions (Karjalainen et al., 2019). This perspective suggests that cybersecurity behavior is shaped not only by individual motivations but also by the boundary conditions within which employees organize their everyday work routines.

5.3 Organizational Conditions and Boundary Coherence

While the boundary–security typology highlights how employees organize their work routines, the findings also suggest that the effectiveness of these boundary strategies depends strongly on the organizational environments in which they are enacted. Our analysis indicates that employees' ability to maintain secure routines depends on organizational factors, including policy clarity, available security tools, IT support, and leadership expectations. Mixed signals, for example, promoting work–life balance while expecting constant availability, can undermine otherwise stable boundary structures.

These observations align with prior IS security research suggesting that security compliance emerges through organizational structures and support mechanisms rather than individual effort alone (Connolly et al., 2017; Hina et al., 2019). From this perspective, cybersecurity behavior reflects not only employees' boundary strategies but also the degree to which organizational policies and infrastructures support those boundary conditions in distributed work environments (Wang et al., 2021).

5.4 Implications for Human-Centric Security Design

Our findings have important implications for the design of cybersecurity practices in remote work environments. Traditional security models often assume stable work settings and uninterrupted attention, conditions that rarely characterize remote work contexts. Our findings suggest that security practices should instead account for the diverse boundary environments in which employees operate.

First, organizations should consider boundary-aware training approaches that account for the situational contexts in which employees perform security tasks. Short, targeted interventions delivered within everyday work routines may be more effective than infrequent, generalized training modules. For example, instead of annual slide-based courses, organizations could deploy short, context-based reminders triggered when employees connect to external networks or access sensitive systems from home.

Second, organizations should invest in low-friction security tools that integrate smoothly into daily workflows. Adaptive authentication methods, context-aware VPNs, and mobile-optimized security controls can reduce the friction that often encourages employees to bypass safeguards. For example, authentication systems could request additional verification only when employees log in from unfamiliar devices or home networks, while allowing faster access when they use approved work devices.

Finally, organizations should provide role-sensitive security support that acknowledges differences in employees' work environments. Workers managing shared spaces, caring for others, or dealing with constant interruptions may require different forms of security guidance than employees in stable office-like settings. Providing flexible security support channels, such as rapid-response IT assistance or

simplified secure access tools, can help employees maintain secure practices even in unpredictable work environments

These implications suggest that cybersecurity in remote work environments should be approached not only as a technical or compliance challenge but also as a human-centered design problem shaped by the boundary conditions of everyday work.

Future Research Directions

While this study focused primarily on how remote workers' boundary strategies shape cybersecurity practices, the findings also suggest several avenues for future research. In particular, the analysis revealed differences in how employees experience cybersecurity support across organizational contexts, especially between larger organizations and smaller firms. Although these observations emerged from participant accounts, the present study did not aim to systematically examine organizational size as an explanatory factor. Future research could therefore investigate how organizational scale influences the alignment between boundary management strategies and cybersecurity practices in remote work settings.

Larger organizations typically possess more formalized security policies, structured training programs, and dedicated IT resources, which may help stabilize security routines even when employees experience blurred work–life boundaries. Smaller organizations, by contrast, may rely more heavily on informal practices and individual initiative, potentially shifting greater responsibility for cybersecurity management onto employees. Examining these dynamics across a broader range of organizational contexts would help clarify how structural resources, institutional governance, and leadership practices shape alignment of boundary security. This could advance IS security research by integrating organizational context into boundary management perspectives and by identifying how institutional conditions enable or constrain secure behavior in increasingly distributed work environments.

Limitations of the study

This study draws on a purposive sample of remote workers across industries and organizational sizes. While the interpretive approach yields rich, context-specific insights, findings are not statistically generalizable. Data is based on self-reported perceptions rather than observed behavior, and although multi-researcher coding and participant validation were employed, researcher bias remains a possibility. The study also lacks longitudinal data and technological monitoring, which could enhance understanding of behavioral stability over time. Despite these limitations, the qualitative lens is appropriate for theory development, offering foundational insights into how boundary strategies shape cybersecurity behavior in distributed work settings.

6 Conclusions

This study advances a behavioral perspective on cybersecurity that situates secure action within the lived boundaries of work and personal life. By showing how segmentation, integration, and boundary blurring shape everyday security practices, we shift the conversation beyond compliance intention toward contextual enablement.

The implications are significant. As digital and physical spheres become increasingly entangled, the future of cybersecurity depends not only on technical controls but on our understanding of the boundaries within which individuals think, feel, and act securely.

By introducing boundary management as a lens for examining cybersecurity behavior, this study highlights the value of considering how everyday work routines shape secure practices. This perspective suggests that aligning security measures with employees' boundary environments may support more sustainable cybersecurity behavior in distributed work settings.

References

Alashwali, E., Peca, J., Lanyon, M., & Cranor, L. F. (2025). Work from home and privacy challenges: What do workers face and what are they doing about it? Journal of Cybersecurity, 11(1), tyaf010.

Alotaibi, S., Furnell, S., & He, Y. (2023). Towards a framework for the personalization of cybersecurity awareness. International Symposium on Human Aspects of Information Security and Assurance, 143–153.

Amo, L. C., Grijalva, E., Herath, T., Lemoine, G. J., & Rao, H. R. (2022). Technological entitlement: It's my technology and I'll (Ab) Use it how I want to. MIS Quarterly, 46(3), 1395–1420.

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

Braun, V., & Clarke, V. (2006). Using thematic analysis in psychology. Qualitative Research in Psychology, 3(2), 77–101.

Brogle, S. E., Kerksieck, P., Bauer, G. F., & Morstatt, A. I. (2024). Managing boundaries for well-being: A study of work-nonwork balance crafting during the COVID-19 pandemic. Current Psychology, 43(43), 33626–33639.

Campbell, S., Greenwood, M., Prior, S., Shearer, T., Walkem, K., Young, S., Bywaters, D., & Walker, K. (2020). Purposive sampling: Complex or simple? Research case examples. Journal of Research in Nursing, 25(8), 652–661.

Carlson, D. S., Ferguson, M., & Kacmar, K. M. (2016). Boundary management tactics: An examination of the alignment with preferences in the work and family domains. Journal of Behavioral and Applied Management, 16(2).

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

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

Donalds, C., & Barclay, C. (2022). Beyond technical measures: A value-focused thinking appraisal of strategic drivers in improving information security policy compliance. European Journal of Information Systems, 31(1), 58–73. https://doi.org/10.1080/0960085X.2021.1978344

Galanti, T., Guidetti, G., Mazzei, E., Zappalà, S., & Toscano, F. (2021). Work from home during the COVID-19 outbreak: The impact on employees' remote work productivity, engagement, and stress. Journal of Occupational and Environmental Medicine, 63(7), e426–e432.

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.

Grobler, M., Gaire, R., & Nepal, S. (2021). User, usage and usability: Redefining human centric cyber security. Frontiers in Big Data, 4, 583723.

Haag, S., & Eckhardt, A. (2024). Dealing Effectively with Shadow IT by Managing Both Cybersecurity and User Needs. MIS Quarterly Executive, 23(4), 5.

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

Hilowle, M., Yeoh, W., Grobler, M., Pye, G., & Jiang, F. (2023). Users' Adoption of National Digital Identity Systems: Human-Centric Cybersecurity Review. Journal of Computer Information Systems, 63(5), 1264–1279. https://doi.org/10.1080/08874417.2022.2140089

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

Hwang, I., & Cha, O. (2018). Examining technostress creators and role stress as potential threats to employees' information security compliance. Computers in Human Behavior, 81, 282–293.

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

Jayarao, G. B., Ray, S., & Panigrahi, P. K. (2024). Information security threats and organizational readiness in nWFH scenarios. Computers & Security, 140, 103745.

Karjalainen, M., Sarker, S., & Siponen, M. (2019). Toward a theory of information systems security behaviors of organizational employees: A dialectical process perspective. Information Systems Research, 30(2), 687–704.

Khadka, K., & Ullah, A. B. (2025). Human factors in cybersecurity: An interdisciplinary review and framework proposal. International Journal of Information Security, 24(3), 1–13.

Klein, H. K., & Myers, M. D. (1999). A set of principles for conducting and evaluating interpretive field studies in information systems. MIS Quarterly, 67–93.

Kossek, E. E., Perrigino, M. B., & Lautsch, B. A. (2023). Work-life flexibility policies from a boundary control and implementation perspective: A review and research framework. Journal of Management, 49(6), 2062–2108.

Laato, J., Mäntymäki, M., Kordyaka, B., & Laato, S. (2025). Automating Qualitative Data Analysis with Chain-of-Thought Reasoning Models: A Study with the Gioia Method. *2025 Americas Conference on Information Systems*, 2130.

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

Maleksaeedi Ghasraldashti, M., Högberg, K., & Willermark, S. (2025). The Silent Struggle: Uncovering Digital Stress in Hybrid Work. Americas Conference on Information Systems, AMCIS 2025, Montreal, Canada, 14 August 2025-16 August 2025, 3783–3792.

McLaughlin, M.-D., & Gogan, J. L. (2018). Challenges and best practices in information security management. MIS Q. Executive, 17(3), 6.

Myers, M. D., & Newman, M. (2007). The qualitative interview in IS research: Examining the craft. Information and Organization, 17(1), 2–26.

Nastjuk, I., Rampold, F., Trang, S., & Benitez, J. (2025). A field experiment on ISP training designs for enhancing employee information security compliance. European Journal of Information Systems, 34(4), 565–588. https://doi.org/10.1080/0960085X.2024.2359460

Nizamuddin, M. (2025). Investigating the cybersecurity risks of remote work: A systematic literature review of organizational vulnerabilities and mitigation strategies. *International Journal of Information Security*, *24*(4), 187.

Nwankpa, J. K., & Datta, P. M. (2023). Remote vigilance: The roles of cyber awareness and cybersecurity policies among remote workers. Computers & Security, 130, 103266.

Östergård, N., Högberg, K., & Lundh Snis, U. (2025). Trust and leadership in the hybrid workplace. 58th Hawaii International Conference on System Sciences 2025 (HICSS), 5427–5436.

Pensar, H., & Rousi, R. (2023). The resources to balance–Exploring remote employees' work-life balance through the lens of conservation of resources. Cogent Business & Management, 10(2), 2232592.

Piszczek, M. M., & Berg, P. (2014). Expanding the boundaries of boundary theory: Regulative institutions and work–family role management. Human Relations, 67(12), 1491–1512.

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.

Qollakaj, K., Larsson, L. E., & Memeti, S. (2025). Cybersecurity of remote work migration: A study on the VPN security landscape post Covid-19 outbreak. Array, 100437.

Schuetz, S., Gewald, H., Johnston, A., & Thatcher, J. B. (2025). What Goals Drive Employees' Information Systems Security Behaviors? A Mixed Methods Study of Employees' Goals in the Workplace. Journal of the Association for Information Systems, 26(5), 1390–1422.

Singh, P., Bala, H., Dey, B. L., & Filieri, R. (2022). Enforced remote working: The impact of digital platform-induced stress and remote working experience on technology exhaustion and subjective wellbeing. Journal of Business Research, 151, 269–286.

Siponen, M., Rönkkö, M., Fufan, L., Haag, S., & Laatikainen, G. (2024). Protection motivation theory in information security behavior research: Reconsidering the fundamentals. Communications of the Association for Information Systems, 53(1), 1136–1165.

Torres, C. I., & Crossler, R. E. (2025). Promoting security behaviors in remote work environments: Personal values shaping information security policy compliance. Information Systems Research, 36(2), 1183–1195.

Trieu, V.-H., Cooper, V. A., & Pallegedara, D. (2021). Employee's Unauthorized Disclosure of Organizational Information on Social Media: The Role of Emotions and Boundary Permeability. ICIS.

Walsham, G. (2006). Doing interpretive research. European Journal of Information Systems, 15(3), 320–330.

Wang, B., Liu, Y., Qian, J., & Parker, S. K. (2021). Achieving effective remote working during the COVID-19 pandemic: A work design perspective. Applied Psychology, 70(1), 16–59.

Zhao, A. T. (2023). Employee boundary management practices and challenges. In The Palgrave handbook of fulfillment, wellness, and personal growth at work (pp. 401–423). Springer.