Department of Digital Business
Journal of Artificial Intelligence and Digital Business (RIGGS)
Homepage: https://journal.ilmudata.co.id/index.php/RIGGS
Vol. 5 No. 1 (2026) pp: 2122-2129
P-ISSN: 2963-9298, e-ISSN: 2963-914X

Reframing Cybersecurity Risk in Social Media through Digital Intimacy and Relational Exposure

Fajrul Khairati[1], Hasdi Putra[2]
[1]Department of Information Systems, Universitas Adzkia, Padang, Indonesia
[2] Faculty of Science and Technology, Universiti Sains Islam Malaysia, Nilai, Malaysia
[3]Department of Information Systems, Universitas Andalas, Padang, Indonesia
[1]khairatif@adzkia.ac.id , [3]hasdiputra@it.unand.ac.id

Abstract

Cybersecurity research has traditionally focused on technical vulnerabilities, malicious attacks, and organizational safeguards to protect digital infrastructure. Although socio-technical perspectives have gained attention, everyday digital practices remain insufficiently examined as sources of cybersecurity risk. Concurrently, social media platforms have normalized digitally mediated intimacy, including public displays of affection (digital PDA), which embed emotionally salient and relational data into platform-based information systems. These practices introduce exposure mechanisms that are not adequately captured by conventional, technically bounded, and intent-based cybersecurity models. This article reframes cybersecurity risk by conceptualizing digital PDA as a distinct form of behavioural and relational exposure. Through an integrative conceptual synthesis of cybersecurity risk management, behavioural cybersecurity, and digital intimacy literature, the study demonstrates that digital PDA differs fundamentally from general digital oversharing. Digital PDA is relationally embedded, emotionally driven, cumulative over time, and amplified by platform affordances such as algorithmic recommendation, data persistence, and content resurfacing. As a result, intimacy-driven disclosures generate exposure that extends beyond individual users and evolves independently of the original act of sharing. The article develops conceptual frameworks that position digital PDA across multiple cybersecurity risk domains, including human, procedural, platform, and governance risks. By foregrounding relational exposure, this study advances behavioural cybersecurity beyond awareness and compliance-centric assumptions and contributes to information systems research by clarifying how platform design and governance shape cybersecurity risk. The findings provide a foundation for future empirical research and more context-sensitive cybersecurity and digital governance strategies in social media–driven environments.

Keywords*: Cybersecurity Risk, Digital Intimacy, Relational Exposure, Behavioural Cybersecurity, Social Media*

1. Introduction

Cybersecurity research has traditionally focused on technical vulnerabilities, malicious attacks, and organizational safeguards designed to protect digital infrastructures [1], [2]. As digital systems have become increasingly interconnected, this focus has expanded to include socio-technical considerations such as human error, insider threats, and governance failures [3], [4]. Despite this expansion, cybersecurity risk continues to be conceptualized primarily through enterprise-centric and technically oriented lenses, leaving everyday digital practices underexplored as sources of security vulnerability.

In parallel, social media platforms have transformed how individuals express intimacy, relationships, and emotional attachment. Practices such as sharing a couple of photographs, affectionate captions, partner tagging, and commemorative posts, commonly referred to as digital public displays of affection (PDA), have become normalized features of online interaction [5], [6]. While these practices support identity expression and social bonding, they also contribute to the accumulation of relational and contextual data within social media–based information systems, potentially exposing users to profiling, inference, stalking, and other cybersecurity risks [7], [8]. Existing cybersecurity frameworks remain limited in their ability to explain such risks. Although human factors are increasingly acknowledged, behaviour is often framed as an awareness or compliance issue rather than as a primary source of risk [9], [10]. This framing underestimates how emotionally driven and socially reinforced practices shape exposure, overlooking the fact that many risky digital behaviours are relationally embedded rather than the result of ignorance or negligence. Recent studies in behavioural cybersecurity and digital privacy further highlight the limitations of rational-choice assumptions when emotional salience and social validation influence disclosure decisions [11], [12].

This article addresses this gap by reframing cybersecurity risk through the lens of digital intimacy and relational exposure. Drawing on recent work in cybersecurity risk management and behavioural studies, the article conceptualizes digital PDA as a distinct form of behavioural cybersecurity risk. Unlike general digital oversharing, digital PDA is inherently relational, emotionally salient, cumulative over time, and amplified by platform affordances embedded in social media platforms [13], [14]. These characteristics generate exposure mechanisms that extend beyond individual users and challenge intent-based and technically bounded definitions of cybersecurity risk. From an information systems perspective, this reframing highlights how platform features, data persistence, and algorithmic visibility actively shape relational exposure and risk generation within social media-based systems.

The objectives of this article are threefold. First, it critically examines the limitations of existing cybersecurity risk perspectives in capturing risks arising from everyday digital intimacy practices. Second, it introduces relational exposure as a key analytical concept for understanding how digital PDA translates into cybersecurity vulnerabilities. Third, it proposes conceptual frameworks that position digital PDA within broader cybersecurity risk domains, providing a foundation for future empirical research and policy development relevant to information systems and technology research [15].

2. Research Methods

This study adopts a conceptual and integrative research design to reframe cybersecurity risk through the lenses of digital intimacy and relational exposure. A conceptual approach is particularly suitable for advancing theory in emerging research areas where existing models remain fragmented or insufficient to explain observed phenomena [16], [17]. Rather than generating empirical data or conducting a systematic literature review, this study synthesizes and reinterprets established research to develop new theoretical insights for information systems and cybersecurity scholarship.

To enhance transparency and analytical clarity, the overall conceptual process adopted in this study is summarized in Figure 1, which illustrates how distinct bodies of literature are integrated and translated into the conceptual outputs discussed in Section 3.

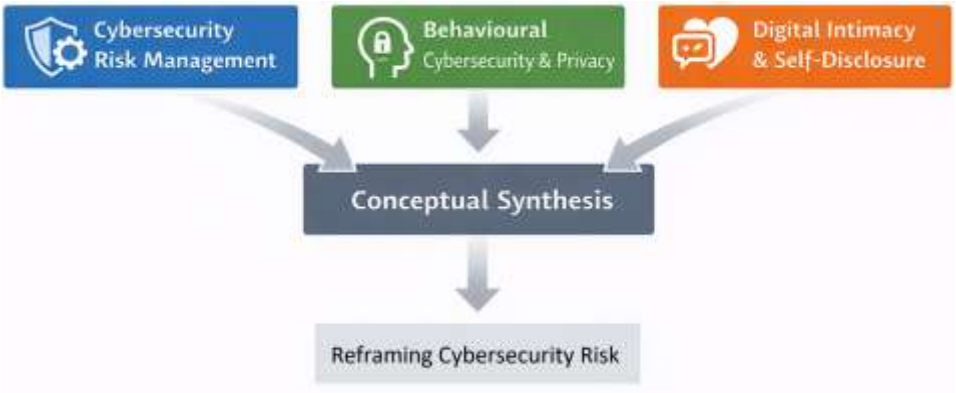

Figure 1. Conceptual Research Design and Synthesis Process

2.1. Research Design

The study is grounded in a conceptual synthesis methodology, which integrates insights from multiple literature streams to construct novel theoretical explanations [16]. This approach is widely used in information systems research to extend existing theories, challenge dominant assumptions, and clarify under-theorized phenomena [17] [10]. In the context of this study, conceptual synthesis enables the systematic integration of cybersecurity risk management with behavioural and socio-technical perspectives, moving beyond descriptive reviews toward theory development.

As depicted in Figure 1, the research design positions conceptual synthesis as an interpretive bridge between established literature domains and the proposed reframing of cybersecurity risk.

2.2. Sources of Literature

The conceptual synthesis draws on three interrelated bodies of literature. First, research on cybersecurity risk management and digital transformation provides the dominant framing of cybersecurity risk, emphasizing technical controls, governance mechanisms, and organizational safeguards [18], [19]. Second, studies in

DOI: https://doi.org/10.31004/riggs.v5i1.6069

behavioural cybersecurity and digital privacy contribute insights into user behaviour, emotional decision-making, and non-malicious risk exposure in digital environments [20], [21]. Third, literature on digital intimacy and online self-disclosure contextualizes how relational and emotionally mediated practices operate within social media–based information systems [22], [23].

Rather than seeking exhaustive coverage, literature selection was guided by theoretical relevance and conceptual contribution, consistent with best practices for integrative conceptual research [17]. These literature streams and their points of convergence are visually summarized in Figure 1.

2.3. Analytical Approach

The analysis followed a structured conceptual process involving thematic abstraction and cross-domain mapping [16]. Key concepts related to cybersecurity risk, human behaviour, and digital intimacy were identified across the selected literature and examined comparatively to surface recurring patterns and conceptual gaps. These concepts were then reorganized to articulate how emotionally mediated and relationally embedded practices generate cybersecurity exposure beyond conventional technical or individual-centric explanations.

The analytical dimensions and conceptual categories guiding this synthesis are summarized in Table 1, which functions as the methodological scaffold for the study. Table 1 outlines how insights from cybersecurity risk management, behavioural cybersecurity, and digital intimacy literature were abstracted and aligned to support subsequent conceptual development.

Table 1. Analytical Dimensions and Conceptual Categories Guiding the Synthesis

Key Finding	Description	Theoretical Implication
Technical bias in cybersecurity risk models	Existing frameworks prioritize technical vulnerabilities and organizational controls while marginalizing everyday digital practices	Limits the explanatory power of cybersecurity theory in social media contexts
Behaviour as a distributed risk source	Risk emerges not only from individual actions but from relational and socially embedded behaviours	Challenges individual-centric assumptions in behavioural cybersecurity
Relational exposure as a distinct mechanism	Exposure is produced through shared identities, mutual tagging, and cumulative relational traces	Extends behavioural cybersecurity beyond awareness and compliance
Digital PDA as non-malicious yet exploitable behaviour	Emotionally driven intimacy practices generate persistent and inferable data	Calls for reframing intent-based definitions of cybersecurity risk
Platform affordances amplify exposure	Algorithmic amplification and content persistence intensify relational risks	Highlights the active role of information systems in risk generation

As illustrated in Figure 1, this analytical process progresses from literature abstraction to conceptual integration, yielding the core analytical outputs. Specifically, the characteristics of digital PDA are consolidated in Table 2, the cross-domain positioning of associated risks is mapped in Table 3, and these relationships are visually integrated in Figures 2 and 3 within the Results and Discussion section.

2.4 Scope and Limitations

As a conceptual study, this article does not empirically test the proposed frameworks. Its primary contribution lies in theoretical reframing and synthesis, which prior research identifies as a necessary foundation for subsequent empirical investigation in emerging research areas [16], [21]. The analysis focuses on public-facing digital intimacy practices on mainstream social media platforms, leaving private or encrypted communication contexts for future research

3. Results and Discussions

The results of the research follow a logical sequence to form a story. The contents show facts/data. Can use Tables and Numbers, but do not repeat the same data in pictures, tables, and text. To further clarify the description, can use subtitles. Discussion is the basic explanation, relationship and generalization shown by the results. The description answers a research question. If there are any dubious results, then show them objectively.

3.1. Limitations of Existing Cybersecurity Risk Perspectives

Prevailing cybersecurity risk models remain predominantly technical and organization-centric, emphasizing system vulnerabilities, compliance mechanisms, and formal governance structures. Although socio-technical perspectives have received increasing attention, everyday digital practices remain marginally addressed as primary

DOI: https://doi.org/10.31004/riggs.v5i1.6069

sources of cybersecurity risk [3]. As a result, existing frameworks struggle to account for risks that emerge outside formal organizational settings, particularly those embedded in routine social media use.

This limitation is especially pronounced in information systems contexts where platforms are designed to facilitate social interaction rather than security-critical tasks. Consequently, benign and normalized behaviours such as sharing personal milestones or relational content remain largely invisible within conventional risk assessments, despite their capacity to generate persistent and exploitable exposure [23], [24].

Taken together, these constraints reveal a conceptual gap in prevailing cybersecurity perspectives: risk is primarily assessed in terms of technical failure or policy non-compliance, while socially embedded and emotionally mediated practices receive limited analytical attention. Addressing this gap requires expanding cybersecurity risk models beyond enterprise boundaries to incorporate how everyday interactions within social media–based information systems contribute to cumulative exposure.

3.2. Behavioural and Relational Exposure as Emerging Cybersecurity Risks

Recent advances in behavioural cybersecurity research increasingly acknowledge human behaviour as a critical component of cybersecurity risk, particularly in relation to non-malicious actions such as oversharing, tagging, and routine disclosure on digital platforms [10], [20]. However, much of this literature continues to conceptualize behaviour primarily at the level of individual decision-making, emphasizing awareness, compliance, and rational risk assessment. While valuable, this framing remains limited in its ability to explain mechanisms of socially embedded, emotionally mediated exposure. A key limitation of individual-centric perspectives is their tendency to treat risk as the outcome of discrete user actions, detached from broader relational and contextual dynamics. In contrast, emerging studies in digital privacy and social media research suggest that exposure often arises through relational disclosure, in which information about one individual simultaneously reveals others within a social or intimate network [25]. Such exposure is not necessarily intentional, nor is it fully under the control of a single user, as it unfolds through repeated interactions, shared visibility, and networked data traces.

Within this context, relational exposure represents an important extension of behavioural cybersecurity thinking. Rather than framing risk solely as a failure of individual judgment, relational exposure highlights how cybersecurity vulnerabilities can emerge from socially reinforced practices and emotionally salient interactions. Studies indicate that emotionally charged contexts, such as expressions of intimacy or affiliation, can weaken privacy calculus and increase tolerance toward potential risk, even among users who are otherwise security-aware [26]. Importantly, relational exposure is often amplified by platform affordances that shape how content circulates, persists, and is recombined over time. Algorithmic recommendation, content resurfacing, and cross-context visibility extend the lifespan and audience of relational disclosures, transforming ephemeral expressions into durable data points that may be exploited for profiling, inference, or social engineering [27]. From an information systems perspective, this underscores that cybersecurity risk is not solely a function of user intent but a product of the interaction among behaviour, relational context, and system design.

Taken together, these insights suggest that behavioural cybersecurity must move beyond awareness-based and individualistic models toward approaches that account for relational, emotional, and platform-mediated dimensions of exposure. Recognizing relational exposure as a distinct risk mechanism provides a necessary conceptual bridge between everyday digital practices and broader cybersecurity risk frameworks, laying the foundation for the analysis of digital PDA as a specific, under-theorized form of behavioural cybersecurity risk.

3.3 Digital Public Displays of Affection as a Distinct Cybersecurity Risk Phenomenon

The synthesis presented in this study identifies digital public displays of affection (PDA) as a distinct and under-theorized form of behavioural cybersecurity risk, differentiated from generic digital oversharing by its relational, emotional, and cumulative characteristics. As summarized in Table 2, digital PDA encompasses practices such as sharing a couple of photographs, affectionate captions, partner tagging, and commemorative posts, all of which embed relational signals and contextual cues that extend beyond individual self-disclosure.

Unlike transactional or informational disclosure, digital PDA is characterized by emotional salience and relational dependency, which shape how users perceive and manage risk. As indicated in Table 2, the motivation underlying digital PDA is often social affirmation and relational visibility rather than information exchange. This distinction is critical, as emotionally motivated disclosure has been shown to weaken privacy calculus and increase tolerance toward potential security risks, even when users are aware of general threats [26].

Table 2 further highlights the cumulative and persistent nature of digital PDA exposure. Relational content is rarely isolated; instead, it accumulates over time through repeated postings, anniversaries, and shared interactions. When combined with platform affordances such as algorithmic resurfacing, memory features, and recommendation

DOI: https://doi.org/10.31004/riggs.v5i1.6069

systems, these practices generate durable relational data traces that can be aggregated and inferred across contexts [23], [24].

Importantly, as shown in Table 2, digital PDA involves shared and distributed exposure, in which the disclosure of one individual simultaneously reveals information about partners, routines, social networks, and emotional ties. This relational spillover distinguishes digital PDA from individual-centric oversharing and reinforces the argument that associated cybersecurity risks are not fully controllable by single users. Instead, exposure emerges from interconnected identities and platform-mediated visibility.

Taken together, the characteristics summarized in Table 2 position digital PDA as a form of non-malicious but exploitable behaviour, where intimate relational practices become potential attack surfaces without malicious intent. This conceptualization provides a necessary bridge between behavioural cybersecurity research and socio-technical analyses of digital intimacy, and it sets the foundation for the cross-domain risk mapping developed in Table 3 and visualized in Figure 3.

Table 2. Conceptual Characteristics of Digital PDA–Driven Cybersecurity Risk

Dimension	Digital PDA Characteristics	Cybersecurity Relevance
Emotional salience	Content driven by affection, attachment, and emotional expression	Weakens privacy calculus and increases risk tolerance
Relational dependency	Disclosure involves multiple individuals and shared identities	Extends risk beyond a single user
Temporal accumulation	Content persists and accumulates over time	Enables longitudinal profiling and inference
Audience ambiguity	Unclear or shifting visibility of content	Increases unintended exposure
Platform mediation	Algorithms amplify, recommend, and resurface content	Transforms benign behaviour into systemic risk

Taken together, these mechanisms render digital PDA non-malicious yet systematically exploitable, highlighting the limitations of intent-based and awareness-centric cybersecurity models. From a behavioural cybersecurity perspective, digital PDA exemplifies how emotionally mediated and socially reinforced practices can function as a latent attack surface, even in the absence of negligence or malicious intent.

3.4 Reframing Cybersecurity Risk through Digital Intimacy

Building on the characteristics summarized in Table 2, this study reframes cybersecurity risk by foregrounding digital intimacy as a core driver of exposure rather than a peripheral social practice. The table demonstrates that digital PDA is emotionally salient, relationally embedded, cumulative over time, and amplified by platform affordance properties that are insufficiently captured by conventional, intent-based risk models. These properties necessitate a shift from viewing risk as an outcome of isolated user actions toward understanding it as a socio-technical process shaped by affect, relationships, and system design.

Figure 2 operationalizes this reframing by visualizing how intimacy-driven practices translate into relational exposure through mediating mechanisms such as audience ambiguity, temporal persistence, and algorithmic amplification. Rather than implying linear causality, the figure depicts cybersecurity risk as an emergent outcome arising from the interaction of emotionally motivated behaviour and platform-level affordances. This aligns with evidence that emotionally charged contexts weaken the privacy calculus and recalibrate risk tolerance, even among users with general security awareness.

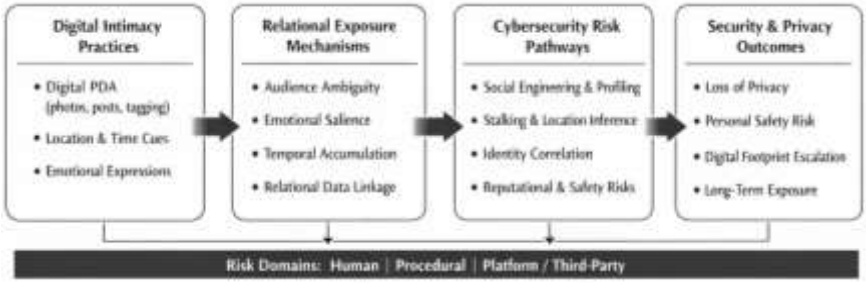

Figure 2. Reframing Cybersecurity Risk through Digital Intimacy and Relationship Exposure

From an information systems perspective, this reframing clarifies why traditional awareness-centric and compliance-oriented interventions struggle to address risks associated with digital PDA. As relational disclosures accumulate and circulate across system features such as memories, recommendations, and cross-context visibility,

DOI: https://doi.org/10.31004/riggs.v5i1.6069

exposure becomes decoupled from the original act of sharing and increasingly shaped by infrastructural mediation. Consequently, cybersecurity risk cannot be adequately explained without accounting for the co-production of exposure by users and platforms.

By integrating the empirical characteristics in Table 2 with the conceptual structure in Figure X, this study positions digital intimacy as a foundational lens for understanding contemporary cybersecurity risk. This reframing extends behavioural cybersecurity beyond individual cognition and toward a relational, affective, and platform-mediated account of exposure, providing a coherent bridge to the cross-domain risk positioning developed in Table 3 and discussed in Section 3.

This reframing also resonates with recent organizational control research in information systems, which conceptualizes control not as a static structure but as an emergent and relational practice enacted through everyday activities and system affordances. Such studies demonstrate that digitally mediated risks and controls often arise from fragmented interactions across actors, processes, and technologies rather than from centralized design alone [28], [29]. Viewed through this lens, cybersecurity risk associated with digital intimacy can be understood as a similarly emergent outcome of relational behaviour and platform-mediated enactment.

3.5 Cross-Domain Nature of Digital PDA Risks

The findings of this study indicate that cybersecurity risks associated with digital public displays of affection (PDA) cannot be attributed to a single source or actor. Instead, digital PDA is best understood as a cross-domain, emergent risk phenomenon arising from the interaction of human behaviour, procedural gaps, platform-level affordances, and governance arrangements. As summarized in Table 3 and visually articulated in Figure 3, digital PDA is positioned at the intersection of multiple cybersecurity risk domains rather than along a linear or deterministic risk pathway

Table 3. Mapping Digital PDA to Cybersecurity Risk Domains

Risk Domain	Manifestation of Digital PDA Risk	Example Exposure Mechanism
Human risk	Emotionally driven disclosure and reduced risk awareness	Oversharing intimate moments despite known risks
Procedural risk	Lack of policies addressing relational data exposure	Absence of guidelines for couple-based or relational content
Platform / third-party risk	Algorithmic amplification and data reuse	Content resurfacing via “memories” or recommendations
Governance risk	Fragmented responsibility between users and platforms	Unclear accountability for relational exposure
Privacy & security overlap	Blurring of privacy loss and security threat	Stalking, social engineering, or inference attacks

From a human risk perspective, emotionally driven disclosure and relational attachment reduce the salience of risk awareness, increasing the likelihood of intimate oversharing even when users possess general knowledge of privacy and security threats. Procedurally, the absence of intimacy-specific policies and the lack of mechanisms to account for relational context create institutional blind spots, leaving digital PDA largely unaddressed. At the platform or third-party level, algorithmic amplification, data persistence, and content resurfacing transform relational disclosures into durable and inferable data traces, thereby extending exposure beyond the original moment of sharing [23].

Importantly, Figure 3 does not depict a direct causal link between digital PDA and security threats. Instead, the privacy–security overlap is conceptualized as a conditional zone of escalation, in which relational exposure may escalate into security risks such as stalking, social engineering, or inference attacks. This positioning reflects the argument that cybersecurity risks associated with digital intimacy are mediated, cumulative, and context-dependent, rather than inherent consequences of individual behaviour. Risk emerges through the convergence of multiple domains over time, not through a single act of disclosure.

This cross-domain framing challenges user-centric and technically bounded approaches to cybersecurity risk management. It underscores the limitations of interventions that focus exclusively on awareness, compliance, or technical safeguards, while neglecting the relational and systemic conditions that enable risk escalation. By conceptualizing digital PDA as an emergent outcome of interacting risk domains, this study reinforces the need for integrated governance strategies that distribute responsibility across users, platforms, and institutional actors, rather than assigning blame to individual users alone [30].

DOI: https://doi.org/10.31004/riggs.v5i1.6069

Figure 3. Positioning Digital PDA within Cybersecurity Risk Domains

Taken together, the positioning of digital PDA in Figure 3 reinforces the idea that cybersecurity risk does not stem from intimate disclosure per se, but rather emerges from the interaction of emotional behaviour, procedural blind spots, and platform-mediated data persistence. This emergent and cross-domain nature of risk underscores the need to move beyond user-centric security models toward governance approaches that recognize relational exposure as a structurally mediated cybersecurity concern [31].

3.6 Future Research Direction

This study opens several promising avenues for future research to extend and empirically validate the conceptual insights developed in this article. First, future studies should undertake empirical investigations of digital public displays of affection (PDA) to examine how intimacy-driven disclosure translates into measurable cybersecurity outcomes. Survey-based and experimental designs could assess the relationship between emotional salience, relational context, and users' tolerance toward privacy and security risks, building on prior work in behavioural cybersecurity and privacy calculus. Second, future research should explore mechanisms of platform-mediated exposure using log data, trace analysis, or mixed-methods approaches. Such studies could investigate how algorithmic amplification, content persistence, and resurfacing features (e.g., memories and recommendations) contribute to the cumulative and distributed nature of relational exposure identified in Table 2 and Figure 3. This direction would enable a more precise understanding of how information systems actively shape cybersecurity risk beyond user intent. Third, comparative and contextual analyses represent an important research direction. Cross-platform studies could examine how differences in design, governance models, and default visibility settings influence intimacy-driven risk, while cross-cultural research may reveal how social norms surrounding intimacy and disclosure moderate relational exposure. Such perspectives would help assess the generalizability of the cross-domain risk positioning outlined in Table 3 across different socio-technical contexts. Finally, future research should investigate the governance and regulatory implications of digital intimacy-driven cybersecurity risk. This includes examining how data protection regulations, platform accountability frameworks, and organizational cybersecurity policies address or overlook relationship-based disclosure and emotionally mediated exposure. Integrating legal, ethical, and technical perspectives may support the development of more holistic governance models that reflect the emergent and relational nature of cybersecurity risk highlighted in this study.

4. Conclusion

This study reframes cybersecurity risk by demonstrating that everyday digital intimacy practices, particularly public displays of affection on social media, constitute a distinct form of behavioural and relational exposure. Through a conceptual synthesis of cybersecurity and behavioural literature, the article shows that digital PDA represents non-malicious yet exploitable behaviour that falls outside the explanatory scope of traditional, technically oriented risk models. Digital PDA differs from general oversharing due to its relational nature, emotional salience, cumulative exposure, and platform-level amplification, all of which intensify cybersecurity risks over time. The proposed frameworks illustrate how intimacy-driven practices translate into security and privacy vulnerabilities and position digital PDA at the intersection of human, procedural, and platform-related risk domains. This cross-domain positioning highlights the limitations of awareness-based interventions and isolated technical controls. By extending cybersecurity analysis to include relational and emotionally mediated practices, this study contributes a more context-sensitive and human-centred understanding of digital risk. While conceptual, the article provides a foundation for future empirical research and policy development to address behavioural and relational cybersecurity risks in contemporary digital environments.

DOI: https://doi.org/10.31004/riggs.v5i1.6069

References

[1] M. Nizamuddin, "Investigating the cybersecurity risks of remote work: a systematic literature review of organizational vulnerabilities and mitigation strategies," *Int. J. Inf. Secur.*, vol. 24, no. 4, p. 187, Aug. 2025, doi: 10.1007/s10207-025-01095-z.
[2] R. Acheampong, D.-M. Popovici, T. C. Balan, A. Rekeraho, and I.-A. Oprea, "A Cybersecurity Risk Assessment for Enhanced Security in Virtual Reality," *Information*, vol. 16, no. 6, p. 430, May 2025, doi: 10.3390/info16060430.
[3] M. Alshaikh, "Developing cybersecurity culture to influence employee behavior: A practice perspective," *Comput. Secur.*, vol. 98, p. 102003, Nov. 2020, doi: 10.1016/j.cose.2020.102003.
[4] M. Ţălu, "Cyberattacks and Cybersecurity: Concepts, Current Challenges, and Future Research Directions," *Digit. Technol. Res. Appl.*, vol. 4, no. 1, pp. 44–60, Apr. 2025, doi: 10.54963/dtra.v4i1.919.
[5] N. P. Shetty, B. Muniyal, N. Yagnik, T. Banerjee, and A. Singh, "A Privacy Preserving Framework to Protect Sensitive Data in Online Social Networks," *J. Cyber Secur. Mobil.*, vol. 11, no. 4, pp. 575–600, Nov. 2022, doi: 10.13052/jcsm2245-1439.1144.
[6] L. Hapsari and A. H. Muhammad, "Online self-disclosure dan display of affection di media sosial online," *J. Soc. Ind. Psychol.*, vol. 13, no. 1, pp. 15–23, 2024, [Online]. Available: https://journal.unnes.ac.id/journals/sip/article/view/10167
[7] R. Gupta and D. Saraf, "Privacy and Security Challenges in Online social media: A Case Study Analysis," *Rev. Rev. Index J. Multidiscip.*, vol. 3, no. 3, pp. 01–07, Sep. 2023, doi: 10.31305/rrijm2023.v03.n03.001.
[8] T. I. Supti *et al.*, "Digital Dependency and Security Risk: Investigating the Connections Between Fear of Missing Out, Problematic Social Media Use, and Vulnerability Perceptions," *J. Technol. Behav. Sci.*, Apr. 2025, doi: 10.1007/s41347-025-00515-0.
[9] F. Ben Salamah, M. A. Palomino, M. Papadaki, M. J. Craven, and S. Furnell, "Evaluating the Risks of Human Factors Associated with Social Media Cybersecurity Threats," in *IFIP Advances in Information and Communication Technology*, vol. 674, 2023, pp. 349–363. doi: 10.1007/978-3-031-38530-8_28.
[10] A. Hardin, C. Schneider, and R. M. Davison, "Established theory rejection," *Inf. Syst. J.*, vol. 32, no. 1, pp. 1–4, Jan. 2022, doi: 10.1111/isj.12360.
[11] A. J. Burns, T. L. Roberts, C. Posey, and P. B. Lowry, "The adaptive roles of positive and negative emotions in organizational insiders' security-based precaution taking," *Inf. Syst. Res.*, vol. 30, no. 4, pp. 1228–1247, 2019, doi: 10.1287/isre.2019.0860.
[12] M. Ahmead, N. El Sharif, and I. Abuiram, "Risky online behaviors and cybercrime awareness among undergraduate students at Al Quds University: a cross sectional study," *Crime Sci.*, vol. 13, no. 1, 2024, doi: 10.1186/s40163-024-00230-w.
[13] D. Zulli, M. Liu, and R. Gehl, "Rethinking the 'social' in 'social media': Insights into topology, abstraction, and scale on the Mastodon social network," *New Media Soc.*, vol. 22, no. 7, pp. 1188–1205, Jul. 2020, doi: 10.1177/1461444820912533.
[14] E. A. Vogels and M. Anderson, "Dating and relationships in the digital age," *Pew Res. Cent. Internet Technol.*, vol. n.a., no. May, pp. 3–33, 2020, [Online]. Available: https://www.pewresearch.org/internet/2020/05/08/dating-and-relationships-in-the-digital-age/
[15] D. Kocur *et al.*, "To hug or not to hug? Public and private displays of affection and relationship satisfaction among people from Indonesia, Nepal, and Poland," *PLoS One*, vol. 20, no. 6, p. e0326115, Jun. 2025, doi: 10.1371/journal.pone.0326115.
[16] E. Jaakkola, "Designing conceptual articles: four approaches," *AMS Rev.*, vol. 10, no. 1–2, pp. 18–26, Jun. 2020, doi: 10.1007/s13162-020-00161-0.
[17] C. Post, R. Sarala, C. Gatrell, and J. E. Prescott, "Advancing Theory with Review Articles," *J. Manag. Stud.*, vol. 57, no. 2, pp. 351–376, Mar. 2020, doi: 10.1111/joms.12549.
[18] R. von Solms and J. van Niekerk, "From information security to cyber security," *Comput. Secur.*, vol. 38, pp. 97–102, Oct. 2013, doi: 10.1016/j.cose.2013.04.004.
[19] S. Pournouri, S. M. Mousavi, and B. Vahdani, "Cybersecurity risk management in digital transformation: A governance perspective," *Am. J. Eng. Technol.*, vol. 6, no. 2, pp. 45–58, 2024.
[20] T. Sommestad, H. Karlzén, and J. Hallberg, "The Theory of Planned Behavior and Information Security Policy Compliance," *J. Comput. Inf. Syst.*, vol. 59, no. 4, pp. 344–353, Jul. 2019, doi: 10.1080/08874417.2017.1368421.
[21] J.-S. Lee, Y.-C. Chen, C.-J. Chew, C.-L. Chen, T.-N. Huynh, and C.-W. Kuo, "CoNN-IDS: Intrusion detection system based on collaborative neural networks and agile training," *Comput. Secur.*, vol. 122, p. 102908, Nov. 2022, doi: 10.1016/j.cose.2022.102908.
[22] R. Berryman and M. Kavka, "'I Guess A Lot of People See Me as a Big Sister or a Friend': the role of intimacy in the celebrification of beauty vloggers," *J. Gend. Stud.*, vol. 26, no. 3, pp. 307–320, May 2017, doi: 10.1080/09589236.2017.1288611.
[23] A. E. Marwick and D. Boyd, "Networked privacy: How teenagers negotiate context in social media," *New Media Soc.*, vol. 16, no. 7, pp. 1051–1067, Nov. 2014, doi: 10.1177/1461444814543995.
[24] C. Lutz and G. Ranzini, "Where Dating Meets Data: Investigating Social and Institutional Privacy Concerns on Tinder," *Soc. Media Soc.*, vol. 3, no. 1, pp. 1–12, 2017, doi: 10.1177/2056305117697735.
[25] M. Haim, J. Breuer, and S. Stier, "Do News Actually 'Find Me'? Using Digital Behavioral Data to Study the News-Finds-Me Phenomenon," *Soc. Media + Soc.*, vol. 7, no. 3, pp. 1–13, Jul. 2021, doi: 10.1177/20563051211033820.
[26] A. Acquisti, L. Brandimarte, and G. Loewenstein, "Privacy and human behavior in the age of information," *Science (80-.).*, vol. 347, no. 6221, pp. 509–514, Jan. 2015, doi: 10.1126/science.aaa1465.
[27] S. Odorico, "From Love Meetings (Pier Paolo Pasolini, 1964) to Vlogs," *M/C J.*, vol. 28, no. 4, Oct. 2025, doi: 10.5204/mcj.3214.
[28] H. Putra, A. Wibisono, and M. Er, "Unveiling organisational control dynamics: a comprehensive literature review," *J. Decis. Syst.*, vol. 35, no. 1, Jan. 2026, doi: 10.1080/12460125.2026.2616678.
[29] H. Putra, R. Qatrunnada, J. Rahmadoni, and F. Khairati, "Enhancing Organizational Control Through Business Intelligence: Monitoring and Automated Alerts," *Electron. J. Educ. Soc. Econ. Technol.*, vol. 6, no. 1, pp. 112–120, Feb. 2025, doi: 10.33122/ejeset.v6i1.222.
[30] J. von Solms, "Digital transformation in treasury, risk and finance: covid-19 to accelerate establishment of smart analytical centres in these departments," *J. Risk Manag. Financ. Institutions*, vol. 14, no. 4, p. 381, 2021, [Online]. Available: https://www.scopus.com/inward/record.uri?partnerID=HzOxMe3b%5C&scp=85117147062%5C&origin=inward
[31] W. Lertyingyod and N. Benjamas, "Stock price trend prediction using Artificial Neural Network techniques: Case study: Thailand stock exchange," in *20th International Computer Science and Engineering Conference, ICSEC 2016*, Department of Computer Science, Faculty of Science, Khon Kaen University40002, Thailand: Institute of Electrical and Electronics Engineers Inc., 2017. doi: 10.1109/ICSEC.2016.7859878.

DOI: https://doi.org/10.31004/riggs.v5i1.6069