Cross-Cultural Social Media Cybersecurity Governance in the Middle East

Vinden J. Wylde and Abbas Fadhil Aljuboori
Gulf College, Oman

vinden@gulfcollege.edu.om
abbas.aljuboori@gulfcollege.edu.om

Abstract: Social media platforms have evolved into critical socio-technical infrastructures through which communication, information exchange, and civic engagement increasingly occur. As these platforms scale globally, they create persistent exposure to cyber risks that extend beyond isolated technical vulnerabilities to include behavioural dynamics and governance limitations. This study examines social media cybersecurity through a cross-cultural lens, focusing on the Middle East, a region characterised by rapid digital adoption, evolving regulatory frameworks, and diverse socio-cultural contexts. Drawing on a structured synthesis of threat intelligence, behavioural cybersecurity research, and governance literature, the analysis integrates three analytical dimensions: structural misalignments between platform design and regulatory safeguards, cross-cultural variation in digital literacy and institutional preparedness, and challenges in operationalising legal and ethical accountability. The findings show that cybersecurity risk emerges from the interaction of these dimensions rather than from failures within any single domain. Platform architectures create persistent exposure conditions, user behaviour mediates how risk materialises across populations, and governance frameworks constrain the translation of regulatory ambition into enforceable safeguards. Building on these insights, the paper proposes a cross-cultural social media cybersecurity governance model that conceptualises risk management as a multi-layered process spanning users, institutions, platforms, and regulators, offering policy and governance implications for strengthening accountability and resilience in rapidly evolving digital environments.

Keywords: Social Media Cybersecurity, Cybersecurity Governance, Cross-cultural Behaviour, Digital Literacy, Middle East

1. Introduction

Social media platforms now function as essential socio-technical infrastructures through which individuals, organisations, and governments communicate, access information, and coordinate activity. Their pervasive influence has intensified exposure to an evolving cyber-threat landscape in which malicious actors exploit behavioural, organisational, and governance gaps. Contemporary threat intelligence indicates that platform misuse, information manipulation, and identity compromise are embedded features of the digital ecosystem rather than isolated anomalies, highlighting the need for cybersecurity perspectives that integrate cultural, regulatory, and institutional dimensions. The 2024 Verizon Data Breach Investigations Report (DBIR) documents 10,626 confirmed breaches across 94 countries, with 68% involving a human element and phishing remaining a dominant initial vector (Verizon Business Group, 2024). Exploitation of software vulnerabilities has also increased significantly, reinforcing that cybersecurity outcomes are shaped as much by behavioural and organisational processes as by technical safeguards. The European Union Agency for Cybersecurity (ENISA) Threat Landscape 2025 similarly, highlights the geopolitical shaping of threat activity, with public administration accounting for 38.2% of incidents in the European Union (EU), and phishing responsible for 60% of initial infections (ENISA, 2025). ENISA further emphasises the growth of Foreign Information Manipulation and Interference (FIMI) campaigns, demonstrating how social media ecosystems are leveraged to influence narratives that erode institutional trust. Together, these reports illustrate the difficulty of aligning regulatory expectations with safeguards across globally scaled platforms. Generative Artificial Intelligence (AI) has accelerated the production and diffusion of misleading content, intensifying societal polarisation and geopolitical tension. Empirical research supports this concern: Vosoughi, Roy, and Aral (2018) demonstrate that false information spreads farther and faster than truthful content, driven primarily by human amplification rather than automated bots. These behavioural dynamics are particularly salient in culturally diverse environments, where trust norms, linguistic variation, and socio-political context shape how information is interpreted and shared.

Figure 1: Core analytical clusters underpinning the study: the global social media cybersecurity threat landscape, cross-cultural cybersecurity behaviour and digital literacy, and platform governance and regulatory context. The figure delineates the conceptual scope of the analysis prior to methodological synthesis, without implying causal relationships or integrative outcomes between domains.

At a conceptual level, debates on digital governance question the sufficiency of compliance-focused regulation. Floridi's distinction between soft and hard digital ethics suggests that legal adherence alone is inadequate in "onlife" environments where online and offline domains overlap (Floridi, 2018). Effective governance therefore requires ethical, organisational, and cultural mechanisms that extend beyond formal regulation and shape behaviour within socio-technical systems. Taken together, this evidence indicates that social media cybersecurity cannot be addressed solely through technical controls or regulatory expansion. Persistent threat escalation, behavioural vulnerability, and governance limitations interact to produce systemic risk (Wylde et al., 2022b), particularly in cross-cultural environments characterised by diverse norms, uneven digital literacy, and evolving institutional capacity. In response, this study adopts a cross-cultural analytical perspective that integrates structural platform risks, behaviourally mediated user dynamics, and governance constraints. Through this approach, the paper develops a multi-layered social media cybersecurity governance model that aligns platform accountability, institutional capacity, and user context within rapidly evolving digital ecosystems in the Middle East. This paper therefore contributes a cross-cultural governance perspective that conceptualises social media cybersecurity as a socio-technical phenomenon emerging from the interaction between platform architectures, user behaviour, and governance frameworks. In doing so, the study provides a conceptual reference point for future research examining cross-cultural cybersecurity governance within globally scaled social media ecosystems. Accordingly, the study addresses the following research question:

RQ: How do structural platform risks, cross-cultural user behaviour, and governance frameworks interact to shape cybersecurity risk within social media ecosystems in the Middle East? To explore this question, the study examines three supporting analytical questions:

- RQ1: How do platform architectures and threat dynamics create structural exposure to cybersecurity risks within social media ecosystems?
- RQ2: How do cultural norms, digital literacy, and organisational contexts influence user cybersecurity behaviour?
- RQ3: How effectively do governance frameworks translate regulatory expectations into operational safeguards across social media platforms?

These analytical questions correspond to the three thematic clusters developed in the literature review.

2. Background and Related Work

2.1 Global Social Media Cybersecurity Landscape (Cluster 1)

Social media ecosystems now operate as globally scaled information infrastructures whose security failures increasingly spill into political, economic, and civic domains. The expansion of online social networks has increased not only information-sharing capacity but also the attack surface available to malicious actors.

Shah, Varshney, and Mehrotra (2025) report that Online Social Network (OSN) platforms have grown from fewer than one billion users in 2010 to over five billion by 2023, generating unprecedented volumes of publicly accessible personal data and intensifying privacy and security risk. Threats within social media environments can be broadly categorised as traditional, advanced persistent, and targeted forms. Parallel research highlights misinformation and manipulative content flows as among the most socially disruptive harms within social media environments. Pfänder and Altay's 2025 systematic review of 67 studies (*n* = 194,438) shows that users are not uniformly credulous; most can distinguish true from false information and often err toward scepticism. However, scepticism varies across contexts.

Beyond content manipulation, intelligence-driven analyses show how adversaries leverage publicly available social media data within broader cyber threat intelligence (CTI) workflows. Avrahami, Zwilling, and Hajaj (2025) report that open-source intelligence (OSINT) now accounts for over 80% of intelligence in some sectors, with social networks serving as primary sources Avrahami et al. (2025). OSINT supports profiling, early threat detection, and real-time situational awareness for both public and private actors. However, its accessibility and low cost also generate challenges, including information overload, inconsistent data quality, and legal or ethical constraints. Social media platforms therefore function simultaneously as intelligence reservoirs for attackers, defenders, and state actors, reinforcing their strategic role within the global threat landscape. The growing complexity of social media threats has prompted calls for improved taxonomies and data resources. Shah, Varshney, and Mehrotra (2025) highlight a lack of publicly available datasets for OSN-specific security analysis, constraining the development and validation of defensive tools. Similarly, misinformation research remains geographically uneven, with experimental evidence concentrated largely in Western contexts, limiting global generalisability (Pfänder and Altay, 2025). Overall, the literature characterises social media platforms as structurally complex threat environments where technical vulnerabilities, information manipulation, and intelligence exploitation intersect. Cybersecurity risk within these ecosystems is therefore systemic rather than episodic, embedded in platform architecture, global information flows, and adversarial adaptation. This cluster establishes the structural conditions of exposure that inform subsequent analysis of behavioural variation and governance constraints.

2.2 Cross-cultural Cybersecurity Behaviour and Digital Literacy (Cluster 2)

Cybersecurity behaviours vary significantly across populations, shaped not only by technical competence but also by cultural expectations, organisational norms, and digital literacy. The literature consistently shows that cybersecurity readiness is inseparable from the socio-cultural environments in which digital practices occur. Behavioural responses to cyber threats emerge from interactions among attitudes, beliefs, communication norms, and habitual practices, influencing whether individuals recognise threats, comply with guidance, or inadvertently contribute to risk. Troublefield (2025) analyses how culturally mediated psychological tendencies shape risk perception and decision making in multinational contexts.

Sutton and Tompson's (2025) rapid evidence review further synthesises behavioural drivers of cybersecurity actions. Across studies, consistent determinants include awareness, social norms, habitual device use, self-efficacy, and security attitudes. However, knowledge alone does not guarantee secure behaviour. Users may diverge from recommended practices when organisational norms discourage reporting, when routines override conscious risk assessment. Communication climate functions as a critical moderator: punitive environments suppress incident disclosure and increase latent risk, whereas supportive climates promote transparency and adaptive response. Organisational culture adds another layer shaping behavioural outcomes. Handri, Sensuse, and Tarigan's "Q" methodology study in 2024 identifies divergent interpretations of cybersecurity within organisations, ranging from compliance focused adherence to more adaptive, collective understandings grounded in learning and collaboration. Rigid, rule-bound cultures may produce superficial compliance without deeper understanding, limiting resilience against emerging threats. In contrast, cultures characterised by open communication, feedback, and psychological safety foster shared responsibility and sustained engagement with cybersecurity practices.

2.3 Governance and Regulatory Developments in the Middle East (Cluster 3)

Digital platforms increasingly function as critical socio-technical infrastructures shaping information flows, economic participation, and civic engagement. As their scale and complexity expand, governance challenges emerge at the intersection of regulation, ethics, technological design, and social consequence. The literature consistently indicates that platform governance cannot be reduced to legal compliance alone but instead involves layered interactions between formal regulation, ethical interpretation, institutional responsibility,

and user experience. Pan et al.'s review conceptualises digital platform governance as a hybrid construct positioned between hierarchical control and market coordination Pan et al. (2025). Platforms rely on mixed mechanisms, including formal rules, algorithmic control, user policies, and ecosystem coordination, rather than direct managerial authority.

The interpretive limits of regulation are further clarified through Floridi's 2018 distinction between hard and soft digital ethics. Hard ethics shapes legal development through normative contestation, while soft ethics operates post-compliance, guiding behaviour where legal provisions remain ambiguous, incomplete, or technologically outpaced. Applied to data protection frameworks such as the EU General Data Protection Regulation 2016/679 (GDPR), this distinction highlights grey areas surrounding algorithmic profiling, automated decision-making, and large-scale data aggregation. Governance effectiveness therefore depends not only on statutory enforcement but also on organisational willingness to engage in ethical interpretation and responsible self-regulation. Practical implementation challenges reinforce this point. Thanvi's case study of the United Arab Emirates (UAE) Personal Data Protection Law No. 45 of 2021 (PDPL) demonstrates that formal compliance provisions do not automatically translate into effective protection Thanvi (2023).

Emerging technologies further complicate governance, particularly in relation to generative AI. Holistic governance research highlights the limitations of traditional regulatory paradigms in addressing the speed, scale, and autonomy of generative AI systems Song et al. (2025). Identified risks include erosion of human agency, misuse, and large-scale digital exploitation. In response, holistic models advocate coordinated responsibility across governments, organisations, developers, civil society, and users, emphasising adaptive governance structures capable of responding dynamically to evolving ethical risk. Governance challenges also extend to the social consequences experienced by users. Rega and Medrado's Stepping into Visibility model 2023, demonstrates how increased social media visibility can simultaneously empower and endanger marginalised communities.

Figure 2: Mixed-methods secondary evidence synthesis framework illustrating how quantitative threat evidence and qualitative behavioural and governance insights are analysed independently and integrated through comparative synthesis to generate unified explanatory insights into social media cybersecurity.

Overall, the literature shows that platform governance operates across legal, ethical, institutional, technological, and social dimensions. While regulation establishes necessary baselines, effective governance depends on ethical interpretation, institutional capacity, adaptive responses to emerging technologies, and sensitivity to user vulnerability. These insights provide the foundation for examining how

governance mechanisms can be operationalised within socio-technical environments characterised by scale, cultural diversity, and rapid technological change. The following section outlines the methodological approach adopted to examine how these dynamics manifest within the selected research context.

3. Methodology

3.1 Research Design

This study employs a mixed-methods secondary evidence synthesis to examine social media cybersecurity as a socio-technical phenomenon shaped by technical threat environments, human behaviour, and governance structures. Rather than introducing new primary data, the analysis integrates quantitative indicators reported in established cybersecurity studies with qualitative interpretive insights from behavioural and regulatory scholarship. This design supports the systematic integration of heterogeneous evidence from technical, behavioural, and governance domains, enabling explanatory analysis of how structural exposure, user behaviour, and institutional frameworks interact within social media ecosystems. It is therefore well suited to research questions requiring conceptual integration across multiple disciplinary perspectives rather than additional empirical measurement.

3.2 Literature Selection Criteria

Sources were identified through structured searches of major academic databases, including Scopus, Web of Science, and IEEE Xplore, using combinations of keywords such as *social media cybersecurity*, *digital literacy*, *platform governance*, and *cyber behaviour*. Publications from 2018 to 2025 were prioritised to capture contemporary developments in platform ecosystems and digital governance. Searches used Boolean combinations of keywords (e.g., “social media cybersecurity”, “digital literacy”, “platform governance”, “cyber behaviour”) applied to titles, abstracts, and keywords within the selected databases. Studies were included if they addressed one or more of the following areas: (1) cybersecurity threats within social media environments, (2) behavioural cybersecurity or digital literacy influencing user security practices, or (3) governance and regulatory frameworks relevant to digital platforms. Editorial commentary, non-peer-reviewed material, and purely technical cybersecurity studies unrelated to social media contexts were excluded. In total, approximately 60 sources were screened, of which 24 were retained for structured synthesis across the three analytical clusters. Screening was conducted in two stages: an initial title and abstract review followed by full-text evaluation against the inclusion criteria. To strengthen analytical rigour, retained studies were assessed using three quality indicators: methodological transparency, relevance to social media cybersecurity contexts, and evidential contribution to one of the three analytical clusters. Studies lacking clear methodological description or empirical grounding were excluded during screening. This quality appraisal helped ensure that the synthesis was informed by credible and methodologically sound sources. While the search was structured rather than fully systematic in the PRISMA sense, explicit screening and quality criteria were applied to support transparency and consistency.

3.3 Evidence Base and Analytical Scope

The methodological framework is anchored in three interrelated thematic clusters developed through the preceding literature review. Cluster 1 provides empirical evidence on the scale, distribution, and characteristics of cybersecurity threats across social media platforms. Cluster 2 contributes interpretive insights into cross-cultural cybersecurity behaviour, digital literacy, and organisational norms shaping user responses to those threats. Cluster 3 contextualises these dynamics within broader regulatory, ethical, and platform governance frameworks. Together, these clusters provide complementary perspectives on the same underlying phenomenon, enabling synthesis across technical, behavioural, and institutional dimensions. The clusters were derived through thematic grouping of the literature, allowing structurally similar studies to be analysed together while preserving distinctions between technical threat environments, behavioural cybersecurity dynamics, and governance mechanisms.

3.4 Analytical Strategy

Quantitative analysis was conducted through structured synthesis of secondary empirical findings reported in Cluster 1 sources, focusing on recurring threat patterns, exposure dynamics, and response characteristics across platforms and contexts. Qualitative analysis drew on interpretive material from Clusters 2 and 3 to

examine the social, cultural, and governance mechanisms that help explain these empirical patterns, including processes of risk normalisation, interpretive ambiguity, and variation in expectations of institutional responsibility. Quantitative and qualitative strands were analysed independently prior to integration to maintain analytical distinction and evidential clarity. The analytical process followed three stages: identification of recurring empirical patterns within cybersecurity threat data, interpretive analysis of behavioural and governance explanations, and cross-cluster synthesis to derive integrative explanatory insights. Cross-cluster comparison was used to identify convergent explanatory patterns linking empirical threat prevalence with behavioural response dynamics and governance implications. This process enabled the development of integrative meta-inferences across the three analytical clusters.

3.5 Integration, Rigour and Validation

Integration is achieved through explicit alignment of empirical threat patterns with behavioural and governance interpretations using comparative analytical matrices. This process supports the development of meta-inferences that synthesise technical prevalence, human response, and institutional context into unified explanatory statements. Methodological rigour is supported through established quality criteria for mixed-methods research, with validation understood as a pluralistic process grounded in evidential coherence, structured cross-cluster comparison to reduce interpretive bias, and sensitivity to the consequences of interpretation Dellinger and Leech (2007); Hirose and Creswell (2023).

4. Findings and Analysis

The findings are organised around the three analytical questions introduced earlier, examining structural platform risks (RQ1), cross-cultural behavioural dynamics (RQ2), and governance implementation challenges (RQ3).

4.1 Structural Exposure in Social Media Platform Ecosystems

The analysis indicates that cyber risk within social media platform ecosystems is structural and platform-mediated rather than episodic or attributable to isolated technical failures. Social media platforms function as high-exposure environments in which scale, connectivity, and data visibility amplify both the frequency and impact of threats. Risk is therefore embedded in platform architecture and operational design rather than arising primarily from anomalous misuse or individual error.

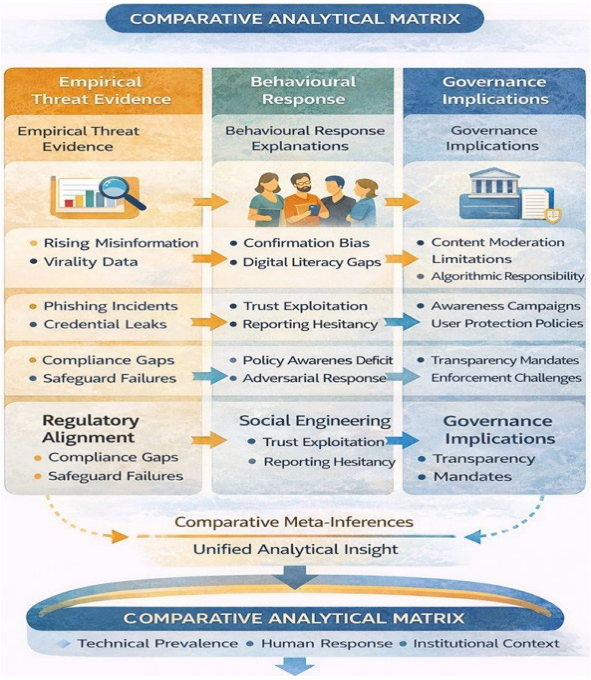

Figure 3: Comparative analytical matrix illustrating the alignment of empirical threat evidence with behaviourally mediated responses and governance implications. The matrix supports integrative synthesis by linking quantitative prevalence patterns with qualitative behavioural and regulatory interpretation.

A consistent pattern across the evidence base is the normalisation of persistent threat activity. Phishing, social engineering, account compromise, and information manipulation appear as routine features of platform operation rather than exceptional incidents. This persistence suggests that safeguards operate predominantly in a reactive mode, addressing manifestations of exploitation without fundamentally altering the exposure conditions generated by scale and design. As user bases and platform complexity expand, adversarial exploitation scales correspondingly, increasing systemic vulnerability. Although threat categories remain broadly consistent across contexts, their severity and consequences vary according to institutional preparedness, regulatory maturity, and patterns of platform use. In regions experiencing rapid digital adoption, exposure is often intensified by uneven safeguard deployment and limited organisational response capacity. These differences reflect variation in resilience and impact rather than in the underlying nature of cyber threats.

The analysis also highlights reliance on a combination of technical controls and user vigilance as primary mitigation mechanisms. Platform safeguards, such as authentication measures and automated detection systems, function as frontline defences, supplemented by user reporting and behavioural compliance. However, the scale and diversity of platform populations create asymmetries in capability and awareness, constraining the effectiveness of user-centred mitigation strategies. A central tension therefore emerges between engagement-driven platform architectures and fragmented regulatory and technical controls. While platform design prioritises openness and rapid information exchange, regulatory frameworks emphasise accountability and harm reduction but often struggle to operationalise enforceable safeguards across jurisdictions. Overall, the findings from Cluster 1 indicate that social media cybersecurity risk is best understood as a systemic property of platform ecosystems shaped by architectural design, scale effects, and persistent adversarial adaptation. These insights establish the structural conditions necessary for integrating behavioural and governance dimensions in the subsequent clusters.

4.2 Digital Literacy and Institutional Preparedness Gaps

Analysis of cross-cultural cybersecurity behaviour and digital literacy indicates that user interaction with cyber risk on social media platforms is socially embedded and contextually mediated rather than determined solely by technical knowledge. Behavioural responses emerge from the interaction of cultural norms, organisational climates, and individual literacy levels, shaping how users interpret risk, comply with guidance, and engage with platform safeguards. A central pattern is the persistent disconnect between awareness and behaviour. Users may understand cybersecurity risks in principle, yet this knowledge does not consistently translate into secure practice. Habitual platform use, social expectations, and perceived role boundaries frequently override deliberate risk assessment. Cultural and organisational contexts strongly influence behavioural outcomes. Variations in authority structures, communication norms, and responsibility expectations determine whether users act proactively, defer to specialists, or disengage from security processes. In hierarchical or punitive reporting environments, incident disclosure declines and latent risk increases. By contrast, contexts characterised by openness, shared responsibility, and psychological safety demonstrate stronger behavioural resilience, even without advanced technical controls.

Digital literacy further differentiates preparedness. Uneven understanding of online authenticity, trust cues, and privacy controls contributes to variable risk exposure across demographic and socio-economic groups. Early misconceptions may persist into adulthood, shaping long-term interaction patterns with social media platforms. As a result, cyber risk is unevenly distributed, with structurally disadvantaged populations experiencing heightened vulnerability due to disparities in education and digital access. The analysis also highlights reliance on individual responsibility as a primary risk-management mechanism. Awareness campaigns, training initiatives, and user guidance are frequently positioned as frontline defences against social engineering and manipulation. However, their effectiveness is constrained by contextual factors that limit users' capacity or willingness to act, particularly where reporting is discouraged or where secure practices conflict with prevailing social norms. Behaviourally centred mitigation strategies therefore struggle to address systemic exposure.

Overall, the findings from Cluster 2 indicate that cybersecurity behaviour on social media platforms is shaped by cultural context, organisational climate, and digital literacy inequalities rather than awareness alone. While this analysis explains variation in user responses to comparable exposure conditions, it does not address the architectural mechanisms that generate risk or the governance structures that define

accountability. These limitations require integration with the structural and governance perspectives developed in the adjacent clusters.

4.3 Challenges in Operationalising Ethical and Legal Expectations

Analysis of governance and regulatory developments indicates that social media cybersecurity is shaped by multilayered and fragmented governance structures rather than uniform or directly enforceable regimes. Governance therefore emerges as a hybrid construct in which legal frameworks, ethical principles, institutional capacity, and platform self-regulation interact unevenly, producing variable accountability outcomes across jurisdictions.

Figure 4: Integrated representation of the three analytical clusters following thematic analysis, highlighting the alignment and misalignment between threat prevalence, behaviourally and culturally mediated user response, and governance and regulatory mechanisms identified in the findings.

A central pattern is the persistent gap between regulatory ambition and operational enforceability. Legal instruments increasingly articulate expectations regarding accountability, transparency, and user protection, yet these expectations often outpace the institutional mechanisms required for consistent implementation. Governance effectiveness therefore depends not only on regulatory presence but also on the capacity of organisations and platforms to interpret, operationalise, and sustain compliance within complex socio-technical systems. Ethical obligations further shape governance outcomes, particularly where formal regulation is ambiguous or technologically outpaced. Statutory compliance alone cannot fully address challenges associated with algorithmic decision-making, large-scale data aggregation, or automated moderation (Wylde et al., 2023). Ethical interpretation therefore functions as a supplementary layer guiding behaviour beyond minimum legal thresholds and influencing how governance principles are translated into practice. Contextual variation further complicates implementation: regulatory maturity, enforcement capability, and institutional preparedness differ significantly across regions. In jurisdictions with limited enforcement capacity, governance mechanisms may exist formally but lack practical effect, whereas stronger institutional environments are better positioned to translate regulatory intent into enforceable controls.

This strand also highlights reliance on organisational interpretation and platform self-regulation to bridge gaps between legal requirements and operational realities. Platforms are expected to embed regulatory and ethical expectations within technical and procedural systems, yet this generates structural tension. Global platforms operate across multiple legal regimes while maintaining unified technical architectures, limiting the extent to which governance can be locally tailored or consistently enforced. Jurisdiction-bound frameworks struggle to oversee transnational infrastructures, while ethical expectations lack direct enforcement mechanisms. These misalignments weaken accountability and constrain the capacity of governance structures to meaningfully reduce systemic cyber risk. Overall, the findings from Cluster 3 indicate that governance effectiveness depends less on the existence of regulation than on interpretive capacity, institutional readiness, and integration of ethical principles into operational systems. While this analysis clarifies how accountability expectations are articulated and constrained, it does not address the architectural sources of exposure or the behavioural dynamics shaping user response. Integration with

structural and behavioural perspectives is therefore necessary to develop a comprehensive account of social media cybersecurity governance.

5. Discussion

This study examined social media cybersecurity through three interrelated themes: structural misalignment between platform risk and safeguards, cross-cultural variation in user literacy and preparedness, and operational gaps in governance and accountability. Taken together, the findings indicate that persistent cybersecurity risk within social media ecosystems cannot be attributed to any single domain. Instead, risk emerges from the interaction of platform architectures that embed exposure, user behaviour that mediates how that exposure materialises, and governance frameworks that struggle to translate regulatory ambition into enforceable control (Wylde et al., 2022a). Structural misalignment establishes baseline vulnerability, behavioural variability shapes how risk is realised across populations, and governance limitations constrain institutional response. This interaction helps explain why domain-specific interventions, technical hardening, awareness campaigns, or regulatory expansion, have achieved limited impact when applied in isolation. Viewed through a cross-cultural lens, these dynamics demonstrate that cybersecurity outcomes are contingent on social, organisational, and cultural context. Preparedness does not scale predictably with awareness or policy intent. Cultural norms influence perceptions of authority, responsibility, and acceptable risk, shaping whether users act proactively, defer to institutions, or disengage from security processes. Organisational climate further mediates these behaviours, particularly where reporting mechanisms are perceived as punitive or misaligned with local expectations. As a result, identical platform features or regulatory requirements may produce divergent outcomes across regions, underscoring the importance of cultural and institutional context in shaping social media cybersecurity resilience.

The findings also clarify why governance frameworks developed within Western regulatory contexts do not translate seamlessly to the Middle East. Such approaches often assume relatively high digital literacy, mature enforcement capacity, and institutional readiness to operationalise legal mandates. In contrast, many Middle Eastern contexts combine rapid digital adoption with evolving regulatory systems and diverse cultural norms governing authority, trust, and information exchange. Under these conditions, formal compliance may exist without substantive operational effect, producing misalignment between governance design and socio-technical reality. Recognising this as a contextual rather than purely regulatory challenge highlights the need for locally responsive governance strategies. Overall, the analysis supports multi-layered governance models that explicitly account for interactions between users, institutions, regulators, and platforms. Effective social media cybersecurity governance therefore depends on alignment across these layers rather than reliance on isolated controls. Where alignment is weak, risk persists despite regulatory expansion and investment. Framing social media cybersecurity as a socio-technical governance challenge emphasises the need for adaptive, context-sensitive governance capable of accommodating cultural diversity, operational constraints, and platform scale.

6. Framework and Policy Recommendations

6.1 A Cross-cultural Social Media Cybersecurity Governance Model

Figure 5 presents the proposed cross-cultural social media cybersecurity governance model, illustrating the relational alignment between user, institutional, platform, and regulatory layers identified through the preceding analysis. Building on the integrated findings, this study proposes a cross-cultural social media cybersecurity governance model that conceptualises risk management as a coordinated, multi-layered process spanning users, institutions, platforms, and regulators. Rather than treating cybersecurity as a problem confined to a single domain, the model reflects the interaction between structural exposure, behaviourally mediated risk, and governance constraint identified across the three analytical clusters. At the foundational layer, the model recognises users and cultural context as critical mediators of cybersecurity outcomes. User behaviour is shaped by digital literacy, social norms, organisational expectations, and perceptions of authority and responsibility. This layer emphasises that awareness alone is insufficient to ensure secure behaviour and that cybersecurity practices must align with local cultural and organisational conditions to be effective.

The institutional layer captures the role of organisations, educational bodies, and public institutions in translating governance expectations into operational practice. Institutions act as intermediaries between

users and broader regulatory or platform-level controls, shaping behavioural norms through training, reporting mechanisms, and organisational culture. Institutional capacity and organisational climate therefore influence whether cybersecurity policies are enacted meaningfully or remain symbolic. At the platform and regulatory layer, the model incorporates both formal governance mechanisms, such as legal and regulatory frameworks, and platform-level controls, including design choices and moderation systems. These mechanisms establish accountability expectations and define the boundaries within which platforms operate. However, governance implementation is constrained by jurisdictional fragmentation, platform scale, and interpretive ambiguity, particularly within cross-border digital environments. Crucially, the model is relational rather than hierarchical: effective governance emerges from alignment across layers rather than top-down control. By making these interactions explicit, the proposed model provides a conceptual foundation for governance approaches that are sensitive to cultural diversity, operational realities, and the global scale of social media platforms.

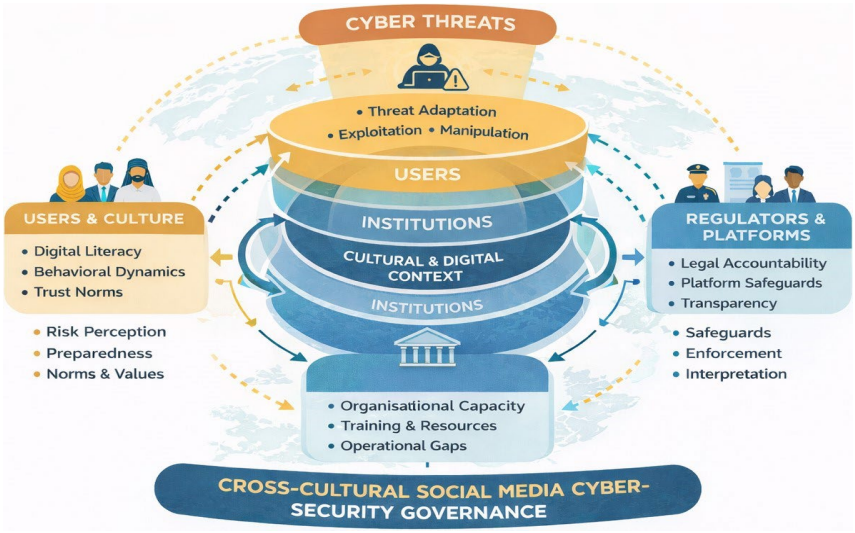

Figure 5: Cross-cultural social media cybersecurity governance model illustrating the interaction between cyber threats, user behaviour and cultural context, organisational capacity, and regulatory and platform-level accountability. The model illustrates how systemic cyber risk emerges through alignment, or misalignment between these layers rather than from any single domain.

6.2 Policy and Practice Implications

The proposed governance model carries clear implications for policy and practice, particularly in cross-cultural contexts such as the Middle East where rapid digital adoption intersects with evolving regulatory and institutional frameworks. At the regulatory level, effective governance requires flexibility and contextual sensitivity alongside formal legal instruments. Regulators should prioritise interpretive clarity, institutional capacity-building, and cross-jurisdictional coordination rather than relying solely on prescriptive compliance requirements that may prove difficult to operationalise. For institutions and organisations, the findings emphasise embedding cybersecurity within organisational culture rather than treating it as a purely technical or compliance-driven function. Training and awareness initiatives should align with local norms, emphasising shared responsibility and psychological safety in incident reporting. Institutions therefore act as intermediaries between regulatory expectations and user behaviour, requiring internal processes that translate governance principles into everyday operational practice. At the platform level, design choices must account for behavioural diversity and uneven digital literacy across user populations. Interface design, reporting mechanisms, and automated safeguards interact with local usage patterns and trust norms, particularly in cross-cultural environments. While platform self-regulation remains necessary, it should be complemented by transparent accountability mechanisms that recognise the limits of user-centred mitigation strategies.

At the user level, policy and practice must move beyond individualised notions of responsibility. Users operate within structural and institutional constraints that limit independent risk management. Effective cybersecurity governance therefore depends on coordinated action across regulatory, institutional, platform, and user layers rather than assuming behavioural change alone can compensate for architectural

exposure or fragmented governance. Overall, these implications reinforce the need for adaptive, multi-layered governance strategies that reflect the socio-technical realities of global social media ecosystems.

7. Conclusion

While this study provides an integrative synthesis of structural, behavioural, and governance dimensions of social media cybersecurity, it is based on secondary evidence rather than primary empirical data. The findings should therefore be interpreted as a conceptual and analytical framework rather than a directly validated empirical model. Future research may extend this work through empirical investigation across specific regional or platform contexts.

The analysis demonstrates that cybersecurity risk within social media ecosystems does not arise from isolated technical shortcomings, user negligence, or regulatory absence, but from the systemic interaction of structural exposure, behaviourally mediated risk, and governance constraint. Through a cross-cultural analysis focused on the Middle East, the findings show that platform architectures embed persistent exposure conditions, user behaviour shapes how that exposure materialises across populations, and governance frameworks struggle to operationalise accountability at global scale. These dynamics help explain the persistence of cyber risk despite increasing regulatory attention, technological investment, and awareness initiatives. This study contributes a cross-cultural governance perspective that integrates structural, behavioural, and regulatory dimensions of social media cybersecurity within a unified analytical framework.

By integrating these dimensions, the study reframes social media cybersecurity as a socio-technical governance challenge rather than a problem confined to any single domain. This perspective helps explain why governance models and policy approaches developed within Western institutional contexts often translate poorly to regions characterised by rapid digital adoption, evolving regulatory ecosystems, and diverse cultural norms. Recognising such misalignment as contextual rather than deficient is essential for avoiding ineffective policy transfer and superficial compliance. The proposed cross-cultural governance model contributes an integrated analytical framework that aligns users, institutions, platforms, and regulators, highlighting the interdependence of these actors in shaping social media cybersecurity outcomes. While derived from secondary evidence synthesis, the model contributes an integrated explanatory account of structural, behavioural, and governance dynamics. Future research may empirically test and refine this model across specific regional or platform contexts, but the central implication remains clear: effective social media cybersecurity governance requires coordinated, multi-layered approaches that reflect cultural diversity, operational realities, and the global scale of digital platforms.

Ethics Declaration

This study is based on secondary analysis of published literature and did not require formal ethical approval.

AI Declaration

AI-assisted tools were used for editorial refinement and visual rendering of conceptual figures. All intellectual content, analysis, and interpretations are the authors' own.

References

Avrahami, Z., Zwilling, M., and Hajaj, C. (2025). Leveraging OSINT for Advanced Proactive Cybersecurity: Strategies and Solutions. *IEEE Access*. https://doi.org/10.1109/ACCESS.2025.3603868.

Dellinger, A. and Leech, N. (2007). Toward a Unified Validation Framework in Mixed Methods Research. *Journal of Mixed Methods Research*, 1(4), 309–332. https://doi.org/10.1177/1558689807306147.

European Union Agency for Cybersecurity (ENISA) (2025). ENISA Threat Landscape 2025. https: //www.enisa.europa.eu/sites/default/files/2025-10/ENISA%20Threat%20Landscape%202025% 20Booklet.pdf. Accessed 10 December 2025.

Floridi, L. (2018). Soft Ethics: Its Application to the General Data Protection Regulation and its Dual Advantage. *Philosophy and Technology*, 31(2), 163–167. https://doi.org/10.1007/s13347-018-0315-5.

Handri, E., Sensuse, D., and Tarigan, A. (2024). Developing an Agile Cybersecurity Framework With Organizational Culture Approach Using Q Methodology. *IEEE Access*, 12, 108835–108850. https://doi.org/10.1109/ACCESS.2024.3432160.

Hirose, M. and Creswell, J. (2023). Applying Core Quality Criteria of Mixed Methods Research to an Empirical Study. *Journal of Mixed Methods Research*, 17(1), 12–28. https://doi.org/10.1177/15586898221086346.

Pan, Q., Luo, W., Liu, Z., and Zhang, J. (2025). Digital Platform Governance: Literature Review and Research Outlook. *Journal of Organizational Computing and Electronic Commerce*, (pp. 1–25). https://doi.org/10.1080/10919392.2025.2470646.

Pfänder, J. and Altay, S. (2025). Spotting False News and Doubting True News: A Systematic Review and MetaAnalysis of News Judgements. *Nature human behaviour*, (pp. 1–12). https://doi.org/10.1038/s41562-02402086-1.

Rega, I. and Medrado, A. (2023). The Stepping into Visibility Model: Reflecting on Consequences of Social Media Visibility–a Global South Perspective. *Information, Communication and Society*, 26(2), 405–424. https://doi.org/10.1080/1369118X.2021.1954228.

Shah, A., Varshney, S., and Mehrotra, M. (2025). Threats on Online Social Network Platforms: Classification, Detection, and Prevention Techniques. *Multimedia Tools and Applications*, 84(16), 17083–17115. https://doi.org/10.1007/s11042-024-19724-5.

Song, X., Ma, C., Yang, Z., and Mao, C. (2025). Towards Holistic Governance: The Application Prospect, Ethical Risk and Governance Logic of Generative AI. In *2025 International Conference on Artificial Intelligence and Digital Ethics (ICAIDE)* (pp. 20–27). https://doi.org/10.1109/ICAIDE65466.2025.11189699.

Sutton, A. and Tompson, L. (2025). Towards a Cybersecurity Culture-Behaviour Framework: A Rapid Evidence Review. *Computers and Security*, 148, 104110. https://doi.org/10.1016/j.cose.2024.104110.

Thanvi, I. (2023). Challenges in Implementation of Personal Data Protection Law No. 45 of 2021: A Case Study of The United Arab Emirates. *Cyber Law Reporter*, 2(3), 1–15. https://journal.thelawbrigade.com/cylr/article/view/922.

Troublefield, T. (2025). Cultural Dimensions of Cybersecurity: A Cyberpsychology Analysis of Multinational Corporate Security. *Journal of Information Security*, 16(3), 359–380. https://doi.org/10.4236/jis.2025.163019.

Verizon Business Group (2024). 2024 Data Breach Investigations Report. https://www.verizon.com/business/resources/reports/2024-dbir-data-breach-investigations-report.pdf. Accessed 10 December 2025.

Vosoughi, S., Roy, D., and Aral, S. (2018). The Spread of True and False News Online. *science*, 359(6380), 1146–1151. https://doi.org/10.1126/science.aap9559.

World Economic Forum (2025). The Global Risks Report 2025: 20th Edition. https://reports.weforum.org/docs/WEF_Global_Risks_Report_2025.pdf. Accessed 10 December 2025.

Wylde, V., Prakash, E., Hewage, C., and Platts, J. (2022a). The Use of AI in Managing Big Data Analysis Demands: Status and Future Directions. *Artificial Intelligence and National Security*, (pp. 47–67). https://doi.org/10.1007/978-3-031-06709-9_3.

Wylde, V., Prakash, E., Hewage, C., and Platts, J. (2023). Ethical Challenges in the Use of Digital Technologies: AI and Big Data. In *Digital Transformation in Policing: The Promise, Perils and Solutions* (pp. 33–58). Springer. https://doi.org/10.1007/978-3-031-09691-4_3.

Wylde, V., Rawindaran, N., Lawrence, J., Balasubramanian, R., Prakash, E., Jayal, A., Khan, I., Hewage, C., and Platts, J. (2022b). Cybersecurity, Data Privacy and Blockchain: A Review. *SN Computer Science*, 3(2), 1–12. https://doi.org/10.1007/s42979-022-01020-4.

Xu, Y. and Li, H. (2025). Cybersecurity Matters for Primary School Students: A Scoping Review of the Trends, Challenges, and Opportunities. *IEEE Transactions on Learning Technologies*. https://doi.org/10.1109/TLT.2025.3564610.