SCIENTIFIC CULTURE
www.sci-cult.com

*SCIENTIFIC CULTURE, Vol. 12, No. 2.1, (2026), pp. 7913-7932*
*Open Access. Online & Print*

**DOI: 10.5281/zenodo.19713809**

# EXPLORING THE SOCIAL DIMENSIONS OF CYBERSECURITY IN SAUDI SOCIETY: TOWARDS A METHODOLOGICAL FRAMEWORK FOR UNDERSTANDING AND ANALYSIS

**Hany Mohamed Bahaa El-Din Ali Hegazy[1], Jaber Hadi F Aldosari[2] and Jasmine Nagy El-Saeed Shabar[3]**

*[1]Associate Professor of Sociology, Faculty of Arts and Sciences, Umm Al Quwain University, United Arab Emirates. Email: drhany.hegazy@uaqu.ac.ae Orcid ID: https://orcid.org/0000-0002-3696-5838*
*[2]Department of Sociology – Faculty of Arts, Suez University. Email: JaberHadi@arts.suezuni.edu.eg*
*[3]Assistant Professor of Mental Health, Faculty of Education, Suez University, Egypt. Email: Yassmen.Nagy@edu.suezuni.edu.eg Orcid ID: https://orcid.org/ 0000-0001-6378-5157*

*Received: 23/03/2026*
*Accepted: 09/04/2026*

*Corresponding Author: Jasmine Nagy (Yassmen.Nagy@edu.suezuni.edu.eg)*

## ABSTRACT

***This study explores the social representations of cybersecurity as a multidimensional social construct in Saudi society and validates a scale for analyzing its cultural, cognitive, behavioral, and institutional dimensions. Most of the literature focuses on technical aspects rather than sociological views. The study was a descriptive cross-sectional design with 755 subjects. Social dimensions were assessed using a scale developed by the researcher. To assess content validity, exploration and confirmatory factor analyses were conducted, and Cronbach's alpha, split-half reliability, and internal consistency were calculated. The results showed that the five-factor model extracted is: cyber culture and society; cyber awareness and perception; trust and privacy in the digital environment; governance and social support; and digital practices. The results showed that cybersecurity is a socially embedded phenomenon, shaped by values, risk awareness, enacting practices, and governance arrangements. The scale has validity and reliability for research in Arab contexts. The research contributes to the theoretical by investigating social representations in cybersecurity and, methodologically, offering a multidimensional instrument for measurement.***

**KEYWORDS:** Cybersecurity; Social Representations; Psychometric Measurement; Saudi Society; Digital Culture.

## 1. INTRODUCTION

In the last 20 years alone, numerous consequences of widespread digital adoption have become clear, including changes in the dynamics of social interaction, institutional arrangements, and definitions of power, trust, and privacy. Manuel Castells (2010) explores the network society, focusing on digital information flows as a key factor in the transformation of power and social relations, in which digital networks create spaces for cultural representation and the redistribution of resources and authority. In this context, cybersecurity is no longer a purely technical field; it has become a structural social issue that affects societal stability and the reproduction of social capital and modes of social regulation in cyberspace.

When said in this way, it resonates with Ulrich Beck's (1992) famous thesis of the risk society, in which late modernity spawns its own "manufactured risks" due to technological advancement itself, making risk management an integral part of social organisation. In this regard, Zygmunt Bauman's (2000) concept of liquid modernity offers related reflections on how online environments give rise to fragile social bonds, marked by fluidity and change. In this trust, identity, privacy, and belonging take on new meanings.

Despite growing global attention to cybersecurity, the literature suggests that integrative approaches are far better at managing digital risk (Anderson et al., 2019). Specifically, studies in digital culture show that common processes (i.e., socialization processes) and individual characteristics such as educational level, gender, and patterns of technology use contribute to how cyber risks are perceived (Livingstone, 2019). However, the dominant prior work stays tethered to technical or legal angles and shares few concerns with understanding cybersecurity as a social construction grounded in shared meanings and representations embedded in the social structure.

As such, and in the Saudi context specifically, digital transformation and emerging national modernization programs are counterbalanced by the pillars of Saudi Vision 2030; here, we see cybersecurity placed as an enabler that can underpin a safe digital social infrastructure. According to the National Cybersecurity Authority (2023), enhancing cybersecurity involves building a culture that goes beyond years of technical work by instilling responsible digital values and practices. This has been put to the test by major cyber incidents (most significantly, the attack on Saudi Aramco), revealing that, far from being limited to technical infrastructure, cyber threats can undermine institutional trust and societal stability (Fawzi, 2019, p. 110). Similarly, data from a survey conducted for Tenable by Forrester Consulting (2020) show that organizations in Saudi Arabia have faced increasing cyber threats. Almost half (52%) of organizations experienced a cyberattack in the past year. In comparison, 22% of Saudi respondents reported a significant increase in the number of attacks over the two previous years, highlighting the growing extent of digital risks across the business and institutional landscape.

Guided by this theoretical and contextual framework, we employ the notion of social representations to understand how individuals in Saudi society conceptualize cybersecurity, and how these conceptualizations draw on individual attitudes and practices structured by social and cultural contexts. As such, cybersecurity is then reframed as a polysemic social construct—an enacting system of awareness, practices, trust, and digital culture that manifests through an interscorer structural landscape.

This study constructs and validates a multidimensional psychometric scale to assess the social dimensions of cybersecurity. Moreover, the study provides new tools for understanding cybersecurity sociologically — recognizing it as a complex, socially embedded phenomenon by synthesizing cultural, behavioral, and institutional considerations within a single overarching analytical framework. Furthermore, it offers a measurement tool for use in cross-cultural and international research settings.

### *1.1. Research Problem*

In the last ten years, Saudi society has experienced an extraordinary, accelerated growth in its use of digital infrastructure across education, employment, government services, and finance. This metamorphosis has transformed the public sphere and modes of social interaction in accordance with Manuel Castells' (2010a) logic of the network society. However, this rapid digital growth has been accompanied by an increasing intensification of cybersecurity risks, creating a structural tension between technological progress, on the one hand, and the sustainability of social trust and social regulation, on the other.

Anyway, despite significant regulatory and institutional progress in cybersecurity, the local literature—like the predominant global approach—still primarily treats cybersecurity as an administrative and/or technical issue. On the other

hand, its analysis (as a social construct shaped by values, cultural representations, socialization patterns, and inequalities in digital capital) is less elaborated. From a sociological standpoint, none of the above-mentioned digital risks can be properly understood outside "manufactured risks" as elaborated by Ulrich Beck (1992) or social bonds' fragility in the context of digital environments underlined by Zygmunt Bauman (2000), where uneven distribution of numerous types and forms of risks relates to uneven distribution of trust via social groups.

While previous studies have identified family, education, cultural values, and gender, among other factors, as playing a role in developing cyber awareness, they have not been adequately integrated into an overarching sociological framework for understanding the emergence of social representations of cybersecurity across Saudi society and their articulation in manifested digital practices. Moreover, there are no multidimensional psychometric instruments available in the literature that enable (through empirically confirmed factorial structures) systematic exploration of this phenomenon.

Therefore, the research gap manifests in two ways: first, by reducing cybersecurity to nothing more than technical or organizational approaches; second, by failing to provide a sociological framework for conceptual analysis and understanding it as a multifaceted social construct. This study aims to fill this gap by reconstructing the concept of cybersecurity through the lens of social representations and in analysing a psychometric scale with established construct validity and factorial structure. The study, by this mechanism, redirects the domain from a procedural and technical orientation toward a more socially interpretive approach that is both measurable and amenable to international comparison. It thus makes a double contribution: theoretically, by anchoring security and cybersecurity within the framework of social representations; and methodologically, by proposing an original data-collection tool to advance comparative research and knowledge production.

Consequently, the central research question is as follows: To what extent can social representations of cybersecurity be formed at the level of social structure within Saudi society, be psychometrically measured across their five dimensions, and vary with structural and social variables?

**This main question leads to these sub-questions:**

1) What are the validity indicators for the scale of social dimensions of psychological cybersecurity in Saudi society?
2) What are the indicators of the reliability of scale measurement, Social Dimensions of Partnerships within the Concept of Psychological Cybersecurity in Saudi Society?
3) What are the reliability indicators of the scale that measure the social dimensions of psychological cybersecurity in Saudi society?

### *1.2. Significance Of the Study*

#### *1. Theoretical Significance*

This research builds on reframing cybersecurity as a multidimensional social construct and provides insight into traditional technical domains. Using a theoretical lens that incorporates network society theory (Castells, 2010), risk society (Beck, 1992), liquid modernity (Bauman, 2000), and structuration theory (Giddens, 2000), this research is framed within the evolving context of digital culture. This taxonomy provides insights into the way social representations of cybersecurity are constructed and how they affect digital behaviours and societal trust.

#### *2- Methodological Significance*

- A multi-dimensional psychometric scale for the various national value constructs of cybersecurity in Saudi society.
- Analysis of construct validity, internal reliability, and factorial structure of the scale, to guarantee its robustness and potential practical use.
- Offer a reliable tool that can be used by researchers and practitioners regionally and internationally, allowing for comparative studies, which will contribute to cumulative knowledge accumulation in cybersecurity from a social perspective.

#### *3. Practical Significance*

- Informing policymakers and the digital security industry with more granular data on social differences in awareness of, and behaviours around, digitality.
- Built using scientific approaches, including sociological exploration of cybersecurity.
- Helping build a digital culture based on trust and shared responsibility, which enables the sustainability of cybersecurity in Saudi society.

**Key Concepts and Operational Definitions**

### *1.3. Conceptual Foundations of Cybersecurity*

Etymology: The word " cyber " comes from the Greek " Kubernetes, meaning “steersman” or “guide.” Norbert Wiener reactivated this idea in his book Cybernetics: Or Control and Communication in the Animal and the Machine (1948) to explain control systems developed within a framework of organization, information, and feedback between man/machine, using an abstract model. In a rapidly digitized world, its classical cybernetic meaning has been expanded to refer to cyberspace—the socio-technical embeddedness between technological infrastructures and interacting humans and institutions —reflecting deep restructurings of social, economic, and political relations in the digital sphere.

Cybersecurity, at the international institutional level, is a comprehensive system of technical tools and policies, procedures, and guidelines for risk management that protects cyberspace and the assets of users and organizations (ITU, 2010). In this sense, however, such a definition captures an integrative approach, going beyond the ad hoc technical solutions that characterize many current initiatives and instead adopts a governance-oriented perspective grounded in risk management and institutional resilience.

For example, the U.S. National Institute of Standards and Technology (NIST) has created a cybersecurity risk management framework with five key functions: Find, Protect, Detect, Respond, and Recover in the NIST Cybersecurity Framework (CSF 2.0) (2024). Its continuous improvement and risk lifecycle approach led to the framework becoming a global standard for strengthening the governance of digitalization and building governance capacity between the public and private sectors.

In the academic literature, Craigen, Diakun, Thibault, and Purse (2014) offer a widely cited analytical definition of cybersecurity as a set of interacting processes intended to protect cyberspace and its dependent systems from deliberate actions that could contravene rights associated with digital assets. The importance of this approach lies in its conceptual shift from the defensive state as a fixed measure to an operational construct that appears from the interaction between threats and responses. At the same time, specialized literature reinforces a feeling of cybersecurity that frames it not only as a procedure for preventing technical intrusions but also as a system of policies and practices that enable continued operation and protect data from unauthorized user interference. Digital identities are an integrated economic and behavioural risk analysis (Anderson, 2008). WIN to the Mute–axis perspective: This is particularly important because it shows that the concept has multiple levels and integrates technical, administrative, legal, and social dimensions into a single analysis.

So, the concept of what cyber safety means at theoretical and institutional levels develops with its multiple components, e.g., hardware/software (so-called) technical measures (e.g., firewalls or malware detection systems), governance practices (security procedures), organizational strategies/approaches/e.g., in-house staffing/policy, as well as social behaviours over use of digital technologies. It aims to ensure data privacy, integrity, and availability, as well as trustworthiness and reliability, across the spectrum of digital activities in society.

Social ledger: Cybersecurity has implications beyond the protection of digital infrastructure; one can conceptualize it differently as a governance-oriented social framework that balances the congruence of technology and society in an era of contemporary digital transformation, reshaping schemas by recognizing new patterns in power, responsibility, and accountability within the public sphere.

### *1.4. Historical Emergence and Development of Cybersecurity*

Cybersecurity goes back as far as the early computing for use (thou didst), with a history spanning mainframe computers (mid-20th century), access control mechanisms, and permissions management in a limited technical/institutional context (Wiener, 1948; Anderson, 2008). Threats could no longer be limited to internal use with the rise of open, cross-border network structures in the 1980s and 1990s (increased reliance on computer networks). This led to the development of defensive tools both for malware and denial-of-service attacks, such as firewalls and intrusion detection systems (Anderson, 2008; Dunn Cavelty, 2008).

A more profound transformation began in the early twenty-first century, spurred by increasingly sophisticated cyberattacks, digital espionage, and politically motivated break-ins. Countries and organizations are therefore required to reintegrate cybersecurity and its implications in their national security strategies, governance frameworks, risk management (NIST, 2018), and legal compliance (NIST, 2024). This trajectory reflects a normalization of cybersecurity from an almost inchoate, narrowly defined technical defensive practice to a strategic, multi-level system in which our technical infrastructures feed back into economic, political, and cultural considerations. Thus, cybersecurity is no

longer merely a means of protecting said infrastructure; it has become a form of governance that reconfigures regimes of responsibility and risk-sharing in contemporary digital societies.

Recent research has built on prior work to outline cybersecurity not just as the threat it is to devices and systems, but also as the structures and behaviors in the social surroundings of digital residency that create that threat. The Social Cybersecurity Approach has also appeared in this context (Carley, 2020) — a discipline that seeks to protect human communities in the digital domain from malicious social influence and manipulation on social networks and platforms.

From this angle, cyber threats are recognized not as operations directed at individual technical devices or systems but against social structures — trust, digital identity, public opinion, and patterns of social interaction. This analysis emphasizes the point that cybersecurity has moved beyond its initial technical scope and, perhaps more importantly, it has further evolved towards a multi-layered paradigm characterized by technology, behavioural aspects, and social environments, which allows for investigating the effect of cyberattacks on communities and individual Behavior (Mulahuwaish et al., 2025; Carley, 2020).

**Operational definition of the Social Dimensions of Cybersecurity Scale in this theoretical framework:**

A psychometric instrument with five interrelated dimensions, this measures an individual's total responses across a series of statements that reflect their cognitive state, actions, beliefs, and environmental and regulatory context in cybersecurity. The total score was obtained based on the following sub-dimensions: cyber culture and society; cyber awareness and feeling; trust and privacy in the digital environment; governance and social support for cybersecurity; digital actions and practices.

Cybersecurity is multifaceted, with multimodal interactions and functional aspects that, in turn, shape an overall tendency. Figure 1 shows such a conceptual model of the plurality of cybersecurity features and their internal relationships (Sidorov et al., 2018). These are interlinked in dynamic, non-linear relationships: (1) cultural and social context; (2) risk awareness and perception; (3) digital practices; (4) trust (intended as an attitude towards the use of data and the internet) and privacy; (5) the regulatory framework, institutional support. The solid arrows indicate reciprocal relationships among the dimensions, while the dashed ones represent contextual influences (e.g., education, media, or previous experiences) on social representations regarding cybersecurity.

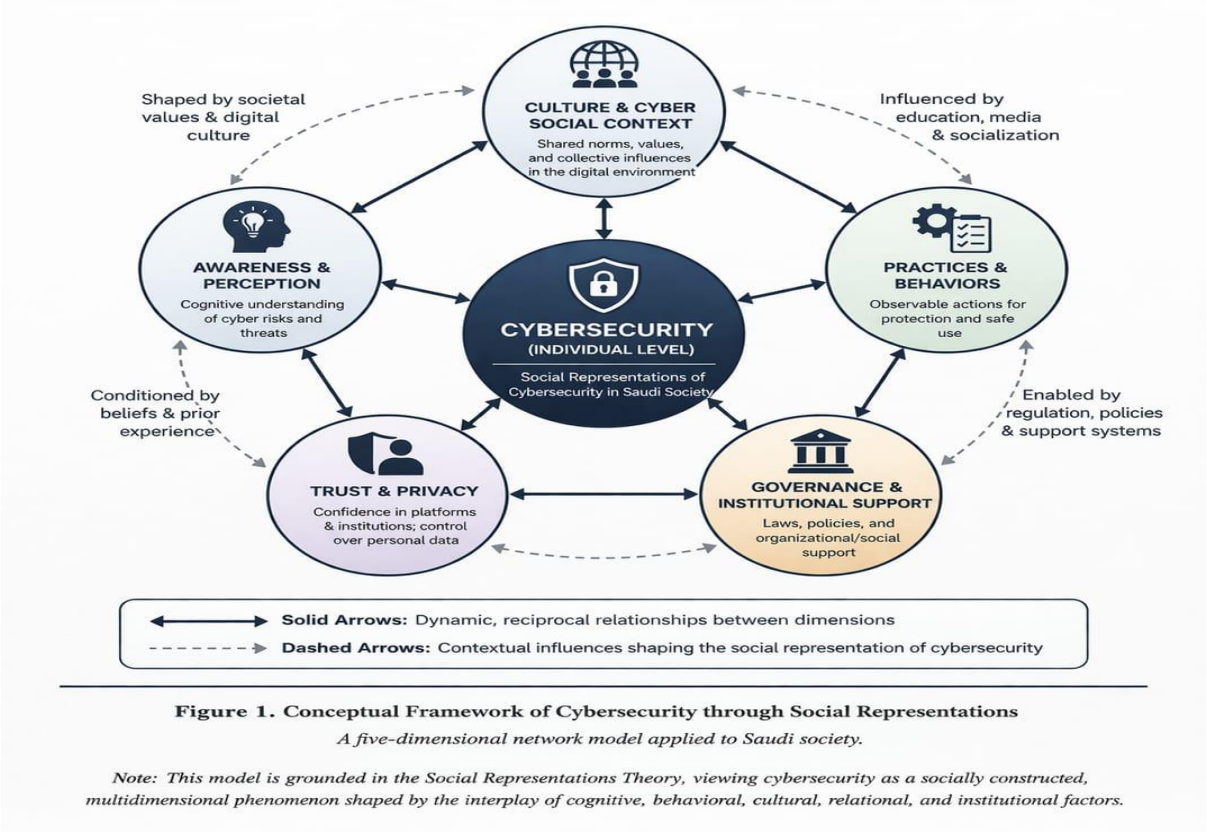


**Figure 1. Conceptual Framework of Cybersecurity through Social Representations**

*A five-dimensional network model applied to Saudi society.*

*Note: This model is grounded in the Social Representations Theory, viewing cybersecurity as a socially constructed, multidimensional phenomenon shaped by the interplay of cognitive, behavioral, cultural, relational, and institutional factors.*

By defining the dimensions of learning at CI and presenting how to measure each one in a

psychometrically relevant way, Table 1 shows the operational translation from the conceptual model to the construct.

***Table (1): Social Dimensions of Cybersecurity: Dimensions, Operational Definitions, Indicators, And Measurement Tool.***

| Variable / Dimension | Operational Definition | Key Indicators | Measurement Tool |
|---|---|---|---|
| **Social Dimensions of Cybersecurity** | The Social Dimensions of Cybersecurity Scale is operationally defined as a psychometric instrument forming five dimensions that measure individuals' responses to items reflecting their awareness, behaviour, attitudes, and social and institutional contexts related to cybersecurity. | Measured using the Social Dimensions of Cybersecurity Scale (developed by the researchers), which consists of fifty items (10 items per dimension). | 5-Point Likert Scale |
| **Dimension 1: Cyber Awareness and Perception** | The extent to which individuals are aware of cybersecurity risks and concepts (e.g., phishing, viruses, digital security), their knowledge of basic protective measures, and their appreciation of the importance of taking precautions in the digital environment. | • Knowledge of basic preventive measures • Awareness of digital risks • Self-perception as a vulnerable user • Perceived importance of cybersecurity | Ten items |
| **Dimension 2: Digital Actions and Practices** | Individuals' actual behaviors in cyberspace, i.e., the measures they take to protect themselves, their devices, and their data. | • Updating systems and software • Use of strong passwords • Verifying links and attachments • Avoiding suspicious content | Ten items |
| **Dimension 3: Trust and Privacy in the Digital Environment** | The extent to which individuals trust institutions and digital platforms to manage and protect their data, as well as their concern for digital privacy. | • Trust in digital institutions • Privacy concerns • Perceptions of digital security • Attitudes toward sharing personal data | Ten items |
| **Dimension 4: Cyber Culture and Society** | The social and cultural dimensions that influence individuals' behaviour in cyberspace, such as social norms, cultural values, and digital inclusion. | • Influence of social norms on digital behaviour • Ethical values related to technology use • Degree of digital inclusion • Influence of collective dynamics | Ten items |
| **Dimension 5: Cyber Governance and Social Support** | Individuals' feelings about the role of laws, policies, and institutions in ensuring cybersecurity, as well as the availability of social and community support in case of incidents. | in ensuring cybersecurity, as well as the availability of social and community support in case of incidents. • Awareness of laws and policies • Perception of social and community support • Reporting cybersecurity incidents • Effectiveness of support networks | Ten items |

## 2. LITERATURE REVIEW AND PREVIOUS STUDIES

### *2.1. Understanding Evolution: Information Security to Cybersecurity*

From scrutinizing the existing body of literature related to Cybersecurity research, it is exciting to observe how the discipline has evolved over the years from a technical perspective that attempted to delineate its own tangible mechanisms into a sociological frame, broadening to encompass surrounding elements: human and behavioural, as well as enterprise issues. This research domain stays populated by studies anchored in theories such as Protection Motivation Theory (PMT) and the Theory of Planned Behavior (TPB). Conversely, few studies have included contextualised, culture-specific variables in an analytical framework that links to behaviour (e.g., Alsharida et al., 2023). Research also stresses that such social arrangements and aspects of

national culture as reference points for viewing the examination results, along with their impact on effectiveness of strategies for prevention of digital risks at international level must not be disregarded; thus, factor inclusion of cultural differences between states becomes significant in search for effective solutions leading to improved state cyber safety (Creese et al., 2021). However, there is still no integrated model that can address the technical, social, and cultural aspects together, especially in a non-Western context such as the Saudi environment; therefore, we must do more to develop an integrated analytical framework.

### *2.2. Cyber Awareness and Perception*

Recent literature shows that research on cyber awareness is diverse in its thematic considerations, and that most studies use a quantitative approach to examine how awareness correlates with users' online behaviors and socio-demographic characteristics related to technology use. Recently, in Saudi Arabia, it has been demonstrated that cyber awareness improves the protective behaviour of high school students towards data (Alqarni, 2025) and that threat perception plays a mediating role in the relationship between cyber awareness and preventive behaviour, while time spent on the Internet acts as a variable moderating this relationship. This alludes to patterns of awareness, knowledge, and preventive practices on digital technologies that vary across cultures, according to international analytical studies (de Bruin & Mersinas, 2024), when adjusted for national culture, industry type, and organizational culture. However, there is a need to develop integrated psychometric models that incorporate awareness, along with cultural and behavioural elements, and adapt them into a single analytical framework that is both socially and culturally specific in Saudi society.

### *2.3. Digital Practices and Behaviors*

According to the literature, cybersecurity behavior cannot be explained solely by knowledge or technical awareness; rather, it is shaped by a combination of social, cultural, and organizational constructs that determine users' habits when using digital technologies. Systematic reviews conducted in recent years have reported that users of social media platforms face several types of digital risks and that adopting preventive behaviors is not solely due to the promotion of safer practices but also requires an understanding of the broader cultural context surrounding media use (Herath, Khanna & , Ahmed, 2022). This study, based on a Saudi framework, explored the culture of protection from digital threats among university students in Saudi Arabia and found that safe practices done in the online environment are transmitted to them is governed by a broader social and cultural system where family values and religious identity as well as peer social interactions contribute to form together what was deemed a“ culture of protection ”that regulates students ’behavior in the context of digital (Ayari et al., 2025). These results indicate that cybersecurity behavior cannot be understood in isolation from the cultural and social realities people navigate in their digital lives. However, few studies have applied advanced statistical modelling to understand better how digital behaviour is shaped by an ecology of awareness, culture, and social context; something sorely needing further development in more integrated analytical frameworks.

### *2.4. Digital Trust and Privacy*

Digital trust scores serve as a core measure in cyber governance, exerting an immediate effect on people’s openness to novel technological products and services and on the adoption of prophylactic behavior. In organizational studies, it has been observed that the mechanisms underlying Zero Trust Architecture (ZTA) can create tensions between perceived technical effectiveness and social trust among humans in institutions (Attia et al., 2020). This is because redundant implementations of ZAC-required verification procedures can erode trust and inhibit collaboration and knowledge sharing among employees with low collaborative inclinations (e.g., Keller et al. 2006). This demonstrates the importance of learning more about the interplay between technical protocols, policy, and social behavior (Oladimeji, 2025). However, no study has yet been conducted in Saudi society using reliable psychometric measures of digital trust and its relationship to privacy, leaving a distinct gap in the literature concerning the integration of organizational and technical aspects with social-theoretical factors in cyber behaviour.

### *2.5. Cyber Culture and Society*

National culture is an intervening variable that influences the transition curve of cybersecurity readiness, as prior literature indicates that social values and cultural norms can significantly shape how individuals perceive the digital risks they face and respond to them. Cross-national research confirms that far more is yielded when social and cultural perspectives are considered, as they significantly impact the threat landscape (Creese,

Dutton & ,Esteve-González, 2021). In the Saudi writing context, applied research has found that students hold certain cultural models that affect their perception of digital risks and adoption of preventive measures, highlighting the importance of developing measurement models tailored to a local context sensitive to the social and cultural features to which students belong (Ayari et al., 2025). While these studies yield fruitful insights, most models treat culture as a separate contextual factor; thus, it needs to be integrated into more comprehensive measurement frameworks that connect culture with awareness, behavior, trust, and governance.

### *2.6. Governance And Social Support*

Research shows that the analysis of cyber governance cannot be limited to technical or organizational problems; social networks, educational institutions, and families also help individuals protect themselves from threats in the digital ecosystem. Moreover, human and social factors are crucial to the success of cybersecurity strategies, according to recent systematic reviews; thus, organizational policies by themselves do not guarantee safe behaviour in cyberspace. Policies of this nature must be situated within broader educational and behavioural contexts to activate sociocultural support and ease adherence to preventive practices (Khadka & Ullah, 2025). However, there is a lack of integration between the two analytical and psychometric models for understanding governance as a local social support network, including policies that are intertwined with culture and digital behaviours. Based on the above, the study's research gaps and contributions are summarized in Table 2.

***Table (2): Summary of Research Gaps and Contributions of the Current Study.***

| Dimension / Variable | Research Gap | Impact on Current Knowledge | Proposed Contribution of the Study |
|---|---|---|---|
| **Cyber Awareness** | Cyber awareness is often measured in isolation without integrating social and cultural factors. | Limited understanding of the influence of culture and social values on preventive practices. | Integrating awareness with cultural, behavioural, and structural factors within a comprehensive psychometric model. |
| **Digital Practices & Behaviors** | A lack of studies that link digital behaviour to awareness, trust, and culture. | There is an absence of a comprehensive understanding of how preventive behaviour develops within Saudi society. | Developing a model that links behaviour with awareness, trust, and culture to analyse digital practices in a multidimensional framework. |
| **Trust & Digital Privacy** | The relationship between trust, privacy, and social structures remains underexplored. | Limited literature explaining the adoption of modern technologies and preventive practices. | Examining the dynamics of trust and privacy within Saudi society and their relationship to social representations. |
| **Cyber Culture & Social Structure** | Lack of multidimensional models integrating social representations, demographic differences, and cultural context. | Inaccurate measurement of the impact of culture on digital behaviour and cybersecurity readiness. | Integrating culture and demographic differences into a psychometric model to analyse digital readiness and preventive behaviour. |
| **Governance & Social Support** | Governance is often studied from a purely organizational perspective, neglecting social support. | Limited understanding of the role of family, institutions, and the private sector in enhancing cybersecurity. | Examining governance as an integrated social support system linking policies and institutions with behaviors and culture. |

### *2.7. The Sociological Perspective on Cybersecurity*

By integrating Risk Society, Network Society, Liquid Modernity, and Structuration Theory, this study adopts a four-framework approach to cybersecurity, treating it as a multidimensional social construct. This synthesis aims to illustrate the processes of social representation of cybersecurity and their implications for digital practices and community trust in the context of digital transformations and changing cultural forms in a network society.

### *1. Risk Society as an Analytical Driver*

Ulrich Beck's Risk Society Theory is the main perspective through which cybersecurity is examined, with manufactured risks—global and often beyond individual or state control—forming the theoretical basis. In sociological terms, cyberattacks, digital crimes, and cybersecurity failures pose direct risks to social and economic structures, requiring even more robust global risk systems for both prevention and mitigation (Beck, 1986). Globalization and digital fluidity extend risks across the globe (Beck, 2006), heightening uncertainty and restricting the ability to manage them. They encompass what we typically consider as (nature-related) external risks and human-induced ones, leading us to see in this theory a growing threat of the latter for social and economic stability. In the digital context, this framework can be used to assess

cyber risks to social networks, economic linkages, and trust in cyberspace.

Anthony Giddens highlights that manufactured risks generate a "runaway world" in which patterns of life become less stable and the uncertainty about our capacity to manage and control these risks increases. In the context of cybersecurity, this perspective enables analysis of how social relationships are reshaped by both the expansion of electronic networks and the increasing complexity of many forms of social and economic interaction, making cybersecurity a strategic need for defending both social and economic stability (Giddens, 2000).

### *2. Network Society as a Functional Structure*

The Network Society model explains these structural changes produced by digitalization in social organization: The flow of information through digital networks is increasingly becoming the structural axis of economic and social relations (Castells, 2010). By taking a closer look at this perspective, one can also argue for the existence of functional mechanisms, such as cybersecurity, that support network stability and the retention of information flows, thereby creating trust among social actors and stabilizing interactions on the net. Cybersecurity uses at interdependent levels: the technical, which involves protecting data and infrastructure; the social, which concerns trust in digital interactions; and the behavioural, which refers to individuals' and institutions' adherence to safe practices. Together, these themes will help ensure the resilience of digital networks and continuity of interactions within global networked society.

### *3. Liquid Modernity as a Dynamic Framework*

Social relationships have become temporary, liquid, and volatile, according to the Liquid Modernity model, which holds that modern societies are in a state of institutional fluidity in which rigid structures have fallen apart (Bauman, 2000). Your model presents an unfamiliar perspective on cybersecurity, not just as a form of protection but as an adaptive response system in which individuals or institutions can overcome rising cyber threats and sustain digital trust and secure awareness in times of uncertainty. This view highlights the necessity of taking initiative and adopting adaptive approaches to respond to ongoing digital transformations.

### *4. Structuration As a Mechanism of Production and Reproduction*

Structuration Theory adds a cognitive dimension to this framework, highlighting the duality of structure, i.e., the mutually constitutive nature of human action and social structure (Giddens, 2000, p. 140). Cybersecurity is shaped and reshaped in everyday practice by individuals and institutions, and it also affects the stability of social and economic structures. This framing allows us to approach the question of cybersecurity as more than a technical process; we can understand it as a social practice that disciplines digital behavior, promotes national security, and reproduces social order. As noted by Zayed (1996: 66), this Structuration Theory-based cyber application is grounded in four core pillars that capture the elements required to understand cybersecurity practices in depth.


***Figure:** An Integrative Sociological Model for Understanding Cybersecurity in Contemporary Digital Societies.*

With the integration of these four frameworks, cybersecurity can be conceptualized as a wider social construct: it is about risk management of constructed uncertainties (Beck); existing in complex digital networks (Castells) responsive to ever visible and rapid change with liquid modernity (Bauman; where norms have no truer defined constitution than their also dualistic reproduction through the daily actions of individuals or institutions under Giddens' conception's duality. In this respect, the integrative model offers a broad view of cybersecurity as an evolving socio-cultural structure that is both shaped by and shapes digitalisation practices, social trust, and economic and political hierarchies while stimulating a well-informed, sustainable culture of security.

### *2.8. Structural And Institutional Framework of Cybersecurity Representations in Saudi Society*

The representation of cybersecurity in Saudi society is being negotiated amid a fundamental structural transformation under Vision 2030, in which the relationship to cybersecurity has shifted from a technical tool for risk management to a core element in the national and digital security equation. The Path of Cyber Governance Reconfiguration, the Reconstruction of State-Society-Market Relations in Cyberspace Based on Social Trust and the Regulation Duplication of Digital Dividend Redistribution.

National surveys also reflect this analytical duality in the Saudi context: path-sprinters towards organizational and regulatory development coexist with competency deficiencies, a gulf in sectoral readiness levels, and a relative dependence (compared to domestically generated technology) on services-oriented solutions rather than value-added technologies (Almardas, 2023). In other words, governance of cyber pollution lagged far behind as individual citizens became aware of digital threats, and information deficiencies are a major factor in the nation's susceptibility to cyber extortion (Al-Taimani, 2021). This indicates a disconnect between sophisticated institutional arrangements and the cognitive-behavioral level of individual actors, evidence of what Du Toit et al. [16] refer to as "fast-track" institutionalization of regulatory frameworks that falls behind the speed at which social knowledge and behaviors are formed in fast-paced technological fields.

In 2017, the introduction of the National Cybersecurity Authority marked a watershed in restructuring cybersecurity governance, shifting from an institutional fragmentation model to a unified control model underpinned by national security standards for risk management and critical infrastructure protection. In addition, hosting the International Cybersecurity Forum enhanced the global aspect of the Saudi experience. It connected it to international digital governance networks, promoting the state's symbolic capital in this domain (Almardas, 2023).

At a societal awareness level, Alshammari & Al Mamary (2025) demonstrated the importance of cybersecurity awareness in promoting individuals' willingness to adopt modern technologies and enhancing institutional trust, asserting that encouraging a digital culture is the main driver in reshaping how Saudi society portrays cybersecurity. Bringing together higher institutional trust and lower individual awareness of security concepts, we note an opportunity for capacity-building strategies to address knowledge and behavior gaps, potentially yielding multiplicative effects for such cyber-secure practices.

Another noteworthy indicator has international stature: Saudi Arabia was classified as a Role-Modeling country in the 2024 Global Cybersecurity Index by the International Telecommunication Union, which ranked it among countries with advanced institutional and legislative cybersecurity capacity (ITU, 2024). Strengthening international partnerships and collaborations in cybersecurity, Saudi Arabia ranked first among sixty-four countries in the World Competitiveness Yearbook's cybersecurity index, published by the International Institute for Management Development (IMD) in 2024 and 2025 (IMD, 2024, 2025). However, these advances in institutional structures occur against a backdrop of persistently important levels of cyberattacks, creating a structural paradox that is not indicative of policy failures per se (Almardas, 2023). However, the result of growing digital exposure, as well as increasing digitization and dependence on connected systems, is observed across critical infrastructures.

The lack of institutional homogeneity in cybersecurity is evident in organizational readiness gaps, with heterogeneous investments in protection varying by activity type and digital asset size. Although the local cyber industry is growing quickly, it remains focused on operational services. It therefore lacks the accumulation of local industrial knowledge, which influences economic actors' perceptions of cybersecurity, leading them to regard compliance with regulations as a potentially prohibitive cost rather than as an innovative domain that contributes to their strategic goals.

On the other hand, an enabling ecosystem aids in

reimagining societal representations through capacity-building initiatives spearheaded by the Saudi Federation for Cybersecurity, Programming, and Drones, as well as by establishing the National Cybersecurity Academy to help redefine the sector around a promising profession within national human capital (Almardas, 2023). According to Al-Taimani (2021), knowledge and behavioral gaps among people must be bridged to improve societal representations of cybersecurity.

From a strategic perspective, the national approach is gradually heading towards an integrated model based on the principles of multi-level governance, proactive management of risks, enhanced applied research and development of cybersecurity technologies for localization, as well as transition from passive to anticipatory approaches and dependence on solutions by third parties to the creation of competitive in-world range national products (Almardas, 2023). The goal here is to elevate cybersecurity culture across society, with a stake for everyone, from institutions to individuals.

In response, cybersecurity literacies in Saudi society crystallize at the intersection of three layers: an institutional layer conditioned by the dictates of a legislative and regulatory landscape; an economic layer connected to market dynamics and innovation; and a societal layer centered on digital culture and modalities of trust. At this intersection, a restructuring of the relationship between state, technology, and society emerges. Cybersecurity is therefore both an object of analysis and one that requires analysis itself, making it a multi-dimensional approach that incorporates measurements at the institutional, cognitive, affective, and behavioral levels.

### *2.9. Methodological Determinants and Study Procedures*

a) **Research Method**: The current study is considered descriptive and analytical in nature, through which the researcher seeks to examine the psychometric properties of the scale of social dimensions of cybersecurity in Saudi society.

b) **Study Population and Sample**: This study was conducted on a sample of 755 participants (527 males; 227 females) from the Saudi population. It was administered to them to verify the psychometric properties of the Social Dimensions of Cybersecurity Scale. The study was conducted from October 1, 2025, to February 28, 2026; during this period, the scale was developed, standardized, and administered, and data were analyzed.

c) **Tools**: Cyber Security Social Dimensions Scale – Researchers Developed.

- *Purpose of the Scale*: The goal is to measure the social-behavioural structure of citizens' perceptions of cybersecurity and agree/disagree with binary items that assess cognitive, behavioural, affective, cultural, and institutional interactions between individuals (society) and the digital environment.
- **Rationale for Developing the Scale:**

1. Transition from a technical view of cybersecurity to a social view.
2. Human factor significance in describing cyber behavior.
3. Existing scales do not deliver a comprehensive multidimensional model.
4. The role of culture and social context in influencing cyber behaviour.
5. Governance and social support need to be merged in the measurement framework.
6. There is a shortage of Arab scales specialized in the social aspects of cybersecurity.
7. An instrument for measuring a theory developed in the Arab context.

- **Scale Development Steps: The researchers showed the following steps to develop the scale:**

1. Conducting an extensive literature review: reviewing studies, research, and existing scales tackling cybersecurity at large and the social dimensions of cybersecurity in specific. This review is based on both Arab and international sources. While many studies covered cybersecurity, most focused on technological or personal behavioral constructs, lacking a comprehensive societal approach encompassing awareness, practices, trust, and governance in cultural settings. Numerous studies emphasized the significance of human and social aspects in cybersecurity, including:

- Hadlington (2017): The psychological and cognitive factors involved in understanding risky cyber behaviors are considerable, particularly to underscore that security is not performed within a vacuum but rather because of cognitive and social processes.
- Ifinedo (2012): Organizational support and belief of personal threat drive compliance with information security procedures.
- Maalem Lahcen et al. (2020): Cyber behaviour: Behavior is not only based on technical properties; it has patterns that are behavioural, social, and cultural, which suggest the need for

scales incorporating culture and social context.

- International Telecommunication Union (ITU) Reports: Bloom that Cyber Security is a multi-layered phenomenon technically focused not just on the security of technical infrastructure but also regarding policy, legislation and regulation as well as education and culture Therefore, for the dissemination of cybersecurity culture a political, legal and regulatory, social and technical perspective should be considered rather than treating it as a purely technical issue.

Although partial scales measure only cyber behavior or policy compliance, no Arabic scale that combines the five social dimensions into a single, full-fledged model was found to support the current scale's design motivation.

- *Development of the scale:* Adaptation and validation (First version). The Social Dimensions of Cybersecurity Scale was initially developed from existing studies and scales covering five dimensions with fifty items. Item formulation was guided using the operational definition of cybersecurity as follows: "The total score achieved by an individual on its subdimensions—Cyber Culture and Society, Cyber Awareness and Perception, Digital Trust and Privacy, Cybersecurity Governance and Social Support, as well as Digital Actions and Practices measured according to the designed scale." Five key dimensions have been identified between the operational definitions and measurement indicators as outlined in Table 1 of this study: one. Cyber Awareness and Perception, 2. Digital Actions and Practices, 3. Digital Trust and Privacy, 4. Cyber Culture and Society, 5. Cybersecurity Governance and Social Support. The items of the first scale were classified along these five areas shown in Table 3.

***Table (3): Distribution of the Initial Items of the Social Dimensions of Cybersecurity Scale Across the Five Dimensions.***

| No. | Dimension | Items | Total Items |
|---|---|---|---|
| **1** | Cyber Awareness | 1-10 | 10 |
| **2** | Digital Practices & Behaviors | 11-20 | 10 |
| **3** | Trust & Digital Privacy | 21-30 | 10 |
| **4** | Cyber Culture & Social Structure | 31-40 | 10 |
| **5** | Governance & Social Support | 41-50 | 10 |
| **Total Number of Items** | - | - | 50 |

- *Scale:* The final scale instructions were worded to provide each response item with five response options of "Strongly Agree, Agree, Neutral, Disagree, Strongly Disagree." The options were presented such that the best possibility for their opinion could be marked with a (✓). They were also prompted to carefully read all statements and respond to all items, with a note about the confidentiality of information, and to clarify that responses would be used only for research purposes.

**d) Statistical Methods Used:**

1) **Content Validity:** Before proceeding with the actual analysis of the survey results, we verified that all scale items used were suitable for the domain of cybersecurity according to a panel of specialized judges.
2) **Investigatory Factor Analysis (EFA):** Performed to find out the factor design of the size Scale and evaluate its hidden dimensions.
3) **Cronbach's Alpha Reliability:** To determine the internal consistency of the scale.
4) Split-Half Method: It is used to evaluate the reliability of a scale that was divided into two half-scales and the correlation between two half-scores.
5) **Internal consistency:** Made sure that each of the scale items is related, ensuring the coherence of each dimension to the overall scale.

**Scale Sample Descriptive statistics**: The mean, standard deviation, skewness, and kurtosis were calculated for the scale sample, as reported by Gagnon et al. Table 4 summarizes the results.

***Table (4): Distribution of the Sample According to Social Characteristics (N = 755).***

| No. | Variable | Category | Frequency | Percentage | Mean | SD | Skewness |
|---|---|---|---|---|---|---|---|
| **1** | Gender | Male | 528 | 69.9% | 1.30 | 0.459 | 0.871 |
| | | Female | 227 | 30.1% | | | |
| **2** | Age | 18–<25 years | 95 | 12.6% | 2.28 | 0.675 | -0.415 |
| | | 25–<45 years | 350 | 46.4% | | | |

| | | | | | | | |
|---|---|---|---|---|---|---|---|
| | | 45 years & above | 310 | 41.1% | | | |
| **3** | Employment Status | Employed | 555 | 73.5% | 1.26 | 0.442 | 1.068 |
| | | Unemployed | 200 | 26.5% | | | |
| **4** | Occupation | Government Sector | 448 | 59.3% | 1.92 | 1.253 | 0.886 |
| | | Private Sector | 102 | 13.5% | | | |
| | | Self-employed | 26 | 3.4% | | | |
| | | Other | 179 | 23.7% | | | |
| **5** | Housing | Rent | 192 | 25.4% | 1.75 | 0.436 | -1.131 |
| | | Owned | 563 | 74.6% | | | |
| **6** | Marital Status | Single | 157 | 20.8% | 1.84 | 0.492 | -0.005 |
| | | Married | 158 | 75.2% | | | |
| | | Divorced | 25 | 3.3% | | | |
| | | Widowed | 5 | 0.7% | | | |
| **7** | Education Level | Primary | 9 | 1.2% | 3.88 | 0.738 | -0.832 |
| | | Intermediate | 16 | 2.1% | | | |
| | | Secondary | 156 | 20.7% | | | |
| | | University | 453 | 60.0% | | | |
| | | Postgraduate | 121 | 16.0% | | | |
| **8** | Technology Use | Yes | 733 | 97.1% | 1.03 | 0.168 | 5.610 |
| | | No | 22 | 2.9% | | | |

**The sample consisted of individuals, distributed across various demographic variables as follows:**

1. **Gender:** The results showed that most of the sample were male (69.9%) and a minority were female (30.1%), making up for a gender-dominated sample as well. The mean was 1.30, the standard deviation was 0.459, and the skewness coefficient was 0.871, indicating a slight positive skew in the gender distribution, with a concentration of responses in the male category**.**

2. **Age:** Sample distribution by age was 25 to under 45 years (46.4%), 45 years and above (41.1%), second one after the first group, and finally, the third was the aged from 18 to under 25 years, who formed a small percentage of the sample with only (12.6%) in this study. Results: The average was 2.28, the standard deviation was 675, and the skewness coefficient was -0.415, suggesting the distribution was balanced with a slight lean toward the older generation.

3. **Employment status:** As for the employment status, 73.5% of the total sample was employed, while only 26.5% was unemployed (showing a working sample). The mean was 1.26, the standard deviation was 0.442, and the skewness was 1.068 (positive), indicating that most observations are in the employed category.

3. **Occupation:** first - Government (59.3%), second - Other (23.7%), third- Private sector (13.5%), fourth- Self-owned/entrepreneurship (3.4%). The mean, standard deviation, and skewness were 1.92, 1.253, and 0.886, respectively, showing a tendency towards the government sector.

4. **Housing:** Most of the sample were living in owned (74.6%) rather than rented housing (25.4%). The mean was 1.75 (at the lower end of the Ownership category), the standard deviation was 0.436, and the skewness was -1.131, showing a clear left (negative) skew with responses concentrated in the Ownership category.

5. **Marital status:** Most of the sample population were married (75.2%), followed by single individuals (20.8%), divorced (3.3%), and widowed (0.7%). The mean was 1.84, the standard deviation was 0.492, and the skewness was −0.005, showing a symmetric distribution around the mean and a slight bias toward married individuals over single individuals.

6. **Education level**: University education formed the highest proportion of respondents (60.0%), followed by secondary education (20.7%) and postgraduate studies (16.0%), while primary and intermediate education had the lowest proportions of respondents at 1.2% and 2.1%, respectively. Table 4 presents the demographic characteristics of research participants during the study period. Standardized quantitative questionnaires were administered via face-to-face interviews with patients using closed-ended questions. The mean (M) was 3.88, the standard deviation (SD) was 0.738, and the skewness (g1) was −0.832, showing a negative skew with high educational levels among participants in the sample.

7. **Technology usage**: Overall, 97.1% of the sample reported using technology, while 2.9% said that they did not use any technology. For these 779 subjects, the mean was 1.03, the standard deviation was 0.168, and the skewness (for you statisticians, a measure of uniformity) equalled a very high value of 5.610, showing almost complete concentration in the category of technology users, which is to be expected for a study on cybersecurity.

The sample is overall male, middle-aged, and older, employed (particularly in the government

sector), married, with university-level education or higher, and has universal access to technology. These features are reflected in the social and occupational structure of Saudi society, where the working-age population — particularly in the government sector — constitutes a large share of the workforce. Also, the usage of technology and digital penetration is one of the highest in the world as Saudi Arabia enters the digital transformation era; thus, there exists a meaningful level of education that adds evidence of relevance for a cybersecurity study using such a sample, as digital issues are typically related to educational levels and professionals involved.

Thus, the sample represented an active, digitally connected segment of Saudi society for the study; this supports both the verification of the results and their interpretability within the local social context.

## *2.10. Confirmatory Analysis of Psychometric Properties of Cybersecurity Social Dimensions*

### *2.10.1. Scale Validity*

a) *Content Validity*: The Social Dimensions of Cybersecurity Scale was reviewed by a panel of experts from different Egyptian and Saudi universities, specializing in sociology-related disciplines. Summarizes expert reviewer ratings; agreement among reviewers on the relevance and appropriateness of each item exceeded 80%, suggesting a good degree of face validity for the scale. Then, the scale was evaluated in a sample of 755 Saudi participants to evaluate factorial validity and reliability by three different methods.

b) *Exploratory Factorial Validity (Construct Validity)*: The identification of the factorial structure of the social dimensions of cybersecurity and verifying its measurability was one of the main goals investigated in this study. To conduct this, the researchers used a new statistical method called Exploratory Factor Analysis (EFA), designed to examine relationships among variables and determine whether a smaller number of underlying latent factors explain the observed correlations. The Kaiser-Meyer-Olkin (KMO) measure of sampling adequacy and Bartlett's Test of Sphericity were performed to evaluate if the sample was suitable for factor analysis, as well as its homogeneity, and the probability that correlations among the observed variables are stronger than in partial correlations. We summarize the results in Table 5.

***Table (5): Kaiser-Meyer-Olkin (KMO) And Bartlett's Test Values for the Social Dimensions of Cybersecurity Scale (N = 755).***

| Test | Value |
|---|---|
| Kaiser-Meyer-Olkin (KMO) Measure of Sampling Adequacy | 0.957 |
| Bartlett's Test of Sphericity (Chi-square) | 18,663.489 |
| Significance (p-value) | 0.000 |

**Note: These Results Indicate That the Sample Is Adequate and Suitable for Exploratory Factor Analysis (EFA).**

The KMO test, as presented in Table 5, yielded 0.957, which is considered excellent and indicates that the sample size was appropriate for applying EFA. The results also reinforce the applicability of factor analysis, as Bartlett's Test of Sphericity yields a chi-square value of 18,663.489, significant at $p < 0.01$, supporting factor analysis since all variables correlate very highly. Thus, the required assumptions for conducting factor analysis are fulfilled in this case. To determine the reliability of the scale items, an Exploratory Factor Analysis (EFA) was conducted using Principal Component Analysis (PCA) in SPSS Statistics. The analysis was based on a sample of 755 participants. The Factor matrix derived from five-factor analysis on the scale items, following an orthogonal Varimax rotation (Table 6).

***Table (6): Explained Variance of the Five Factors of the "Social Dimensions of Cybersecurity" Scale According to Exploratory Factor Analysis (N = 755).***

| Factor | Eigenvalue | % of Variance Explained | Cumulative % of Variance Explained |
|---|---|---|---|
| **1st** | 6.409 | 15.632% | 15.632% |
| **2nd** | 5.312 | 12.956% | 28.588% |
| **3rd** | 4.461 | 10.879% | 39.467% |
| **4th** | 4.362 | 10.639% | 50.106% |
| **5th** | 3.142 | 7.663% | 57.769% |

**Note: The Five Extracted Factors Collectively Explain 57.769% Of the Total Variance, Indicating an Acceptable Factorial Structure for The Scale.**

Factorial structure. For exploratory analysis, the factorial structure of this scale was obtained using principal component analysis with varimax rotation. The results are shown in Table 6, which indicates that five latent factors were extracted. This stipulated a factorial structure, as these factors together accounted for 57.769% of the variance in the correlation matrix across the dimensions.

**The description for each factor is as follows:**

- **Factor 1:** The rotated eigenvalue for this factor was 6.409, explaining 15.632% of the total variance. Nine items loaded on this factor, which relate to social norms, cultural values, and digital inclusion. This factor was labeled **"Cyber Culture and Community."**
- **Factor 2:** The rotated eigenvalue was 5.312, explaining 12.956% of the total variance. Nine items loaded on this factor, focusing on risk awareness and knowledge of digital security. This factor was labeled **"Cyber Awareness and Perception."**
- **Factor 3:** The rotated eigenvalue was 4.461, explaining 10.879% of the total variance. Seven items loaded on this factor, relating to trust in institutions and platforms and concerns about privacy. This factor was labeled **"Trust and Privacy in the Digital Environment."**
- Factor 4: Rotated Eigenvalue = 4.362(10.639% of Total Variance). Seven items loaded on this factor, which included laws and regulations, social support, and social consequences of incidents. This determinant was named "Governance and Social Support for Cybersecurity."
- Factor 5: Rotated eigenvalue was 3.142, explaining 7.663% of total variance. Six items loaded on this factor related to the use of protective measures and resistance to phishing or cyber deception. This factor was dubbed "Digital Actions and Practices."

In the exploratory factor analysis, we used orthogonal Varimax rotation to improve the interpretability of the resulting factor structure. Rotated factor loadings for the Social Dimensions of Cybersecurity Scale with respect to the five-factor solution are shown in Appendix (A).

In the next stage of the analysis, dimensions that received a score indicating cross-loadings of 0.10 or higher were classified as poor-performing and thus removed from further analysis; the items evaluated in this regard are tabulated in Table 7.

***Table (7): Items Excluded from Factorial Validity.***

| Item Number in the Scale | Factor1 | Factor2 | Factor3 |
|---|---|---|---|
| **39** | 0.495 | - | 0.404 |
| **27** | 0.464 | - | 0.429 |

**Note: Items Were Excluded Because the Difference in Their Factor Loadings Was Less Than 0.10, Indicating Insufficient Factorial Distinction.**

The extracted factors in the exploratory factor analysis correlate well with the sub-dimensions that constitute the "Social Dimensions of Cybersecurity" concept, except for the order of the names due to item rotation. This suggests that the measure exhibits a large degree of construct validity. The researchers considered the resulting factors to reflect the sub-dimensions of the "Social Dimensions of Cybersecurity" scale.

## *2.11. Scale Reliability Verification*

The researchers used multiple techniques to confirm the scale's reliability, including exploratory factor analysis. These included a reliability coefficient calculated using Cronbach's alpha, and split-half reliability calculated using the Spearman-Brown and Guttman formulas. The results are shown in Table 8.

***Table (8): Cronbach's Alpha and Split-Half Reliability Coefficients for the Social Dimensions of Cybersecurity Scale (N = 755).***

| Scale Dimension | Cronbach's Alpha | Spearman–Brown Coefficient | Guttman Split-Half Coefficient |
|---|---|---|---|
| **Dimension 1: Cyber Culture and Society** | 0.903 | 0.881 | 0.874 |
| **Dimension 2: Cyber Awareness and Perception** | 0.904 | 0.902 | 0.901 |
| **Dimension 3: Trust and Privacy in the Digital Environment** | 0.836 | 0.804 | 0.793 |
| **Dimension 4: Governance and Social Support for Cybersecurity** | 0.873 | 0.843 | 0.835 |
| **Dimension 5: Digital Actions and Practices** | 0.715 | 0.727 | 0.719 |
| **Overall Scale Reliability** | 0.955 | 0.837 | 0.835 |

**Note: All Reliability Coefficients Indicate High Internal Consistency and Acceptable Psychometric Properties of the Scale.**

As you can see from the above table (8), the Cronbach's alpha coefficient is high, reporting 0.955 for the overall scale. The Spearman-Brown split-half reliability coefficients for the overall scale and the Guttman scale were 0.837 and 0.835, respectively; comparable results were observed. All these reliability coefficients were high (0.96; 95% CI [0.93; 0.97]; 0.87 for Test-Retest; $p < 0.01$ from T1 to T2) and statistically significant at the 0.01 level, suggesting psychometric acceptability of our measures. This

indicates that the Social Dimensions of Cybersecurity Scale has a satisfactory level of reliability, confirming the applicability for measuring social aspects of cybersecurity.

### *2.12. Internal Consistency of the Cybersecurity Social Dimensions Scale*

The correlation coefficients between each item's score on the scale and the overall total score were calculated by the researchers. This was conducted to confirm how each part relates to the scale's full format, thereby providing input for assessing its internal homogeneity. As shown in Appendix (B), the item-total correlation coefficients show the stability and consistency of the Social Dimensions of Cybersecurity Scale.

As presented in Appendix (B), the correlation between the item scores and total scale score was positive and statistically significant at the 0.01 level. This shows that the items are homogeneous and consistent with the scale's overall structure.

Furthermore, the researcher proved the internal consistency of the Social Dimensions of Cybersecurity Scale as a construct by computing correlations among the different dimensions and the total score. The outcomes are shown in Table 9.

***Table (9): Correlation Coefficients Between the Dimensions of the Social Dimensions of Cybersecurity Scale and the Total Score (N = 755).***

| Dimension | Correlation Coefficient with Total Score |
|---|---|
| **Dimension1** | 0.799** |
| **Dimension2** | 0.853** |
| **Dimension3** | 0.874** |
| **Dimension4** | 0.873** |
| **Dimension5** | 0.684** |

**Note: ** Indicates Significance at the 0.01 Level.**

As shown in Table 9. Strong, statistically significant correlations at the 0.01 level exist between the five dimensions of the Social Dimensions of Cybersecurity Scale and the scale's total score. This shows that the scale has high internal consistency, showing the homogeneity and coherence of its dimensions and their contribution to measuring the scale's overall construct.

### *2.13. Final Form of the Social Dimensions of Cybersecurity Scale*

**In total, the final scale contained thirty-nine items, divided across five dimensions. The distribution of the items is found for the Social Dimensions of Cybersecurity Scale in the table below (10):**

1) Cyber Culture and Society: This dimension includes social norms, collective influences, and ethical values regarding technology use or the extent of digital inclusivity in society, which can influence individuals' behavior in cyberspace.
2) Parallel dimension: Cyber Awareness and Cognition — This dimension disseminates individuals' awareness of cyber threats and concepts (such as phishing, viruses, digital hygiene), knowledge of basic enhanced protective measures, and recognition of the significance of safety in cyberspace.
3) Trust and Privacy in the Digital Environment: This dimension measures two key elements that provide insights into how much people trust institutions/sites and digital platforms to manage and protect their data, e.g., concern for digital privacy and warnings about the use or sharing of personal information.
4) Description: Cyber Governance and Social-Related Support: This dimension reflects the perceived role of laws, policies, and institutions in ensuring cybersecurity, as well as the presence of social/community support (e.g., reporting, assistance, support networks) during a cyber incident.
5) Digital Actions and Practices: This dimension concerns individuals' actual behaviors in cyberspace, that is, their measures to protect themselves, their devices, and their data, including system updates, strong password use, link verification, and avoiding suspicious attachments. The distribution of items across these dimensions is detailed in Table 10 below.

***Table (10): Distribution of the Final Items of the Social Dimensions of Cybersecurity Scale Across the Five Factors.***

| No. | Scale Dimensions (Five Factors) | Items of Each Dimension (Factor) | Number of Items |
|---|---|---|---|
| **1** | Dimension 1: Cyber Culture and Society | (1-9) | 9 |
| **2** | Dimension 2: Cyber Awareness and Perception | (10-18) | 9 |
| **3** | Dimension 3: Trust and Privacy in the Digital Environment | (19-25) | 7 |

| | | | |
|---|---|---|---|
| **4** | Dimension 4: Governance and Social Support for Cybersecurity | (26-33) | 8 |
| **5** | Dimension 5: Digital Actions and Practices | (34-39) | 6 |
| | Total | | 39 |

### *2.14. Social Dimensions of Cybersecurity Scale Scoring Method*

As shown in Table 11 below, researchers used a five-point Likert scale.

***Table (11): Response Levels for the Social Dimensions of Cybersecurity Scale.***

| **Response Category** | **Strongly Agree** | **Agree** | **Neutral** | **Disagree** | **Strongly Disagree** |
|---|---|---|---|---|---|
| **Score** | 5 | 4 | 3 | 2 | 1 |

Participants are required to choose the response option that they find most suitable. The chosen answer is then evaluated against the scoring key (Table 11), which assigns it a numerical score, and the item scores are summed to obtain a total score indicating the degree of social dimension in cybersecurity. (Note: The total score can vary from 39 to 195.) Scores of the Social Dimensions of Cybersecurity Scale were categorized into three levels (low [39–91], moderate [92–143], and high [144–195]). A score higher than four indicates an important level of cybersecurity, while a lower score reflects a low level of cybersecurity.

## 3. CONCLUSION

Beyond all of this, the study's findings contribute to our sociological understanding of cybersecurity by showing that it is itself a social construction, rooted in and shaped by culture, behaviour, and institutions.

Validity and reliability results show that the Social Dimensions of Cybersecurity Scale in Saudi society proves good validity and reliability. Moreover, the validity coefficients, namely face validity and content validity, were at an acceptable level, indicating that the scale items established their "Measure-Construct". In addition, the reliability analyses (Cronbach's alpha and split-half reliability) showed high internal consistency, further supporting the scale's reliability and showing that comparable results can be obtained from other samples.

The results further show that the scale's structure is clear and consistent, yielding solid markers of psychometric validity and reliability, suggesting a multidimensional depiction of positive cybersecurity. This gives rise to the need for this scale development, as a large gap exists in the psychological and sociological literature. An analysis of the existing literature shows a shortage of culturally relevant and confirmed Arabic measures addressing cybersecurity. To the best of the researchers' knowledge, there has not yet been a standardized Arabic scale for measuring cybersecurity from a multidimensional social perspective that incorporates all awareness and practices, along with trust, culture, and governance, into a single comprehensive framework. Most existing measures focus either on compliance with information security policies or on preventive digital behaviours.

As such, it is necessary for field studies in the Arab context to be conducted using instruments with strong psychometric properties (validity and reliability) that also reflect the cultural and social specificity of the target society. The current scale is designed to meet this requirement.

Thus, the present scale helps fill this gap by providing a culturally and psychometrically valid (and dependable) Arabic instrument that considers the cultural contexts of society being studied. It includes an extensive framework for calculating the five main domains: Cyber Culture and Society, Cyber Awareness and Perception, Trust and Privacy in the Digital Environment, Cyber Governance and Social Support, and Digital Actions and Practices. Factors are integrated into a single framework, providing a more complete perspective on the social aspects of cybersecurity and how they relate to one another and influence both individual and societal behavior.

Furthermore, the scale demonstrates its relevance to psychological and social research. It can serve as a valuable, reliable reference for measuring cybersecurity in future studies and for exploring psychometric properties across different populations in the Arab world.

**Acknowledgements**: The authors would like to express their sincere appreciation to the academic experts and reviewers who contributed to the validation and development of the scale through their valuable feedback and insights. The authors also extend their gratitude to all participants in this study.

**Conflict of Interest:** The authors declare no conflict of interest.

**Data Availability Statement:** The data that support the findings of this study are available from the corresponding author upon reasonable request.

**Declaration of generative AI and AI-assisted technologies in the manuscript preparation process:** The author confirms that no generative AI or AI-assisted technologies were used in the preparation of this manuscript. All intellectual content, analysis, and interpretations are solely the responsibility of the author.

## REFERENCES


Al-Mardas, N. K. (2023). Cybersecurity in the Kingdom of Saudi Arabia between reality and aspirations: A theoretical analytical study. *International Journal for Research and Studies, 5*(49).

Alqarni, A. (2025). The relationship between cybersecurity awareness and data protection behaviors among Saudi secondary school students: The mediating role of cyber threat perception and the moderating role of internet usage duration. *Humanities and Social Sciences Communications, 12*, Article 1837. https://doi.org/10.1057/s41599-025-06122-x

Alshammari, M. M., & Al-Mamary, Y. H. (2025). *Building Trust and Cybersecurity Awareness in Saudi Arabia: Key Drivers of AI-Powered Smart Home Device Adoption*. *Systems*, 13(10), 863. https://doi.org/10.3390/systems13100863

Alsharida, R. A., Al-Rimy, B. A. S., Al-Emran, M., & Zainal, A. (2023). A systematic review of multiple perspectives on human cybersecurity behavior. *Technology in Society, 73*, 102258. https://doi.org/10.1016/j.techsoc.2023.102258

Al-Taimani, M. Z. A. R. (2021). The reality of cybersecurity information awareness among individuals in Saudi society, as perceived by cybersecurity experts. *Social Service Journal, 67*(1), 263–278.

Anderson, R. J. (2008). *Security engineering: A guide to building dependable distributed systems* (2nd ed.). John Wiley & Sons.

Anderson, R; Barton, C; Bohme, R; Clayton, R; Gañán, C; Grasso, T; Levi, M; ... Vasek, M; + view all (2019) Measuring the changing cost of cybercrime. In: Proceedings of the 2019 Workshop on the Economics of Information Security. Boston College

Ayari, M., Gharbi, A., Albalawi, N., Klai, Z., Elsayed, M. S., & Maqbool, A. (2025). Cybersecurity and the culture of protection from digital danger: A sociocultural study of university students in Saudi Arabia. *Journal of Cultural Analysis and Social Change, 10*(3). https://doi.org/10.64753/jcasc.v10i3.2667

Bauman, Z. (2000). *Liquid modernity*. Polity Press.

Beck, U. (1992). *Risk society: Towards a new modernity*. Sage Publications. (Original work published 1986).

Beck, U. (2006). *World at risk: The new politics of risk*. Polity Press.

Carley, K. M. (2020). Social cybersecurity: An emerging science. *Computational and Mathematical Organization Theory, 26*, 365–381. https://doi.org/10.1007/s10588-020-09322-9

Castells, M. (2010). *The rise of the network society* (2nd ed.). Wiley-Blackwell. (Original work published 1996).

Craigen, D., Diakun-Thibault, N., & Purse, R. (2014). *Defining cybersecurity*. Technology Innovation Management Review, 4(10), 13–21. https://doi.org/10.22215/timreview835

Creese, S., Dutton, W. H., & Esteve-González, P. (2021). The social and cultural shaping of cybersecurity capacity building: A comparative study of nations and regions. *Personal and Ubiquitous Computing, 25*, 941–955. https://doi.org/10.1007/s00779-021-01569-6

de Bruin, M., & Mersinas, K. (2024). Individual and contextual variables of cyber security behaviour: An empirical analysis of national culture, industry, organisation, and individual variables of (in)secure human behaviour. *arXiv Preprint*. https://arxiv.org/abs/2405.16215

Dunn Cavelty, M. (2008). *Cyber-Security and Threat Politics: US Efforts to Secure the Information Age*. Routledge.

Fawzi, I. (2019). Cybersecurity: Social and legal dimensions — A sociological analysis. *National Social Journal, 56*(2), 99–139.

Forrester Consulting. (2020). The rise of the business-aligned security executive: The bad news? There is a disconnect between business and cybersecurity. The good news? Aligning them can make all the difference (according to a commissioned study conducted for Tenable). Tenable. https://securityleaders.com.br/download/Arthur_Capella_tenable_Final.pdf

Giddens, A. (2000). *New rules of sociological method* (2nd ed.). Stanford University Press. (Original work

published 1976).
Hadlington, L. (2017). Human factors in cybersecurity: Examining the link between Internet addiction, impulsivity, attitudes towards cybersecurity, and risky cybersecurity behaviours. *Heliyon, 3*(7), e00346.
Herath, T. B. G., Khanna, P., & Ahmed, M. (2022). Cybersecurity practices for social media users: A systematic literature review. *Journal of Cybersecurity and Privacy, 2*(1), 1–18. https://doi.org/10.3390/jcp2010001
https://doi.org/10.1186/s42400-020-00050-w
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.
Institute for Management Development. (2024). *World Competitiveness Yearbook 2024: Cybersecurity indicator – Saudi Arabia tops global cybersecurity rankings* [Annual report summary]. *Saudi Gazette*. https://www.saudigazette.com.sa/article/643719
Institute for Management Development. (2025). *World Competitiveness Yearbook 2025: Saudi Arabia maintains top cybersecurity ranking* [Annual report summary]. *Saudi Gazette*. https://www.saudigazette.com.sa/article/653249
International Telecommunication Union. (2021). *Global Cybersecurity Index 2020*. International Telecommunication Union. https://www.itu.int/en/ITU-D/Cybersecurity/Pages/GCI.aspx
International Telecommunication Union. (2024, September 12). *Global Cybersecurity Index 2024: Saudi Arabia named 'Role-modelling' in the UN Global Cybersecurity Index* [News release]. National Cybersecurity Authority. https://nca.gov.sa/en/news/1486/
ITU. (2010). Securing information and communication networks: Best practices for building a cybersecurity culture (Telecommunication Development Sector, Study Group 1, Issue 1). International Telecommunication Union.
Khadka, K., & Ullah, A. B. (2025). Human factors in cybersecurity: An interdisciplinary review and framework proposal. *International Journal of Information Security, 24*, Article 119. https://doi.org/10.1007/s10207-025-01032-0
Livingstone, S. (2019). Audiences in an Age of Datafication: Critical Questions for Media Research. *Television & New Media, 20*(2), 170–183.
Maalem Lahcen, R. A., Caulkins, B., Mohapatra, R., & Kumar, M. (2020). Review and insight into the behavioral aspects of cybersecurity. *Cybersecurity, 3*(1), 10.
Mulahuwaish, A., Qolomany, B., Gyorick, K., Bou Abdo, J., Aledhari, M., Qadir, J., Carley, K., & Al-Fuqaha, A. (2025). A survey of social cybersecurity: Techniques for attack detection, evaluations, challenges, and prospects. *Computers in Human Behavior Reports, 18,* 100668. https://doi.org/10.48550/arXiv.2504.04311
National Institute of Standards and Technology. (2018). Framework for improving critical infrastructure cybersecurity (Version 1.1). U.S. Department of Commerce. https://doi.org/10.6028/NIST.CSWP.04162018
National Institute of Standards and Technology. (2024, February). The NIST cybersecurity framework (CSF) 2.0. U.S. Department of Commerce. https://doi.org/10.6028/NIST.CSWP.29
Oladimeji, G. (2025). Rethinking trust in the digital age: An investigation into the social consequences of zero trust architecture for organizational culture, collaboration, and knowledge sharing. *arXiv Preprint*. https://doi.org/10.48550/arXiv.2504.14601
Wiener, N. (1948). *Cybernetics: Or Control and Communication in the Animal and the Machine*. John Wiley & Sons.
Zayed, A. (1996). New perspectives in sociology theory: Structuration theory. *National Journal of Sociology, 33*(1–2), 57–85.

## *Appendix A. Rotated Factor Loadings of the Social Dimensions of Cybersecurity Scale*

*Table A1: Rotated Factor Loadings of the Social Dimensions of Cybersecurity Scale (N = 755).*

| Item No. (Post-EFA) | Original Item No. | Factor1 | Factor2 | Factor3 | Factor4 | Factor5 |
|---|---|---|---|---|---|---|
| **1** | 37 | 0.780 | _____ | _____ | _____ | _____ |
| **2** | 35 | 0.771 | _____ | _____ | _____ | _____ |
| **3** | 38 | 0.766 | _____ | _____ | _____ | _____ |
| **4** | 40 | 0.725 | _____ | _____ | _____ | _____ |
| **5** | 30 | 0.683 | _____ | _____ | _____ | _____ |
| **6** | 31 | 0.661 | _____ | _____ | _____ | _____ |
| **7** | 34 | 0.593 | _____ | _____ | _____ | _____ |
| **8** | 33 | 0.555 | _____ | _____ | _____ | _____ |
| **9** | 39 | 0.495 | _____ | _____ | _____ | _____ |

| | | | | | | |
|---|---|---|---|---|---|---|
| **10** | 27 | 0.464 | _____ | _____ | _____ | _____ |
| **11** | 24 | 0.418 | _____ | _____ | _____ | _____ |
| **12** | 2 | _____ | 0.748 | _____ | _____ | _____ |
| **13** | 7 | _____ | 0.702 | _____ | _____ | _____ |
| **14** | 9 | _____ | 0.693 | _____ | _____ | _____ |
| **15** | 4 | _____ | 0.684 | _____ | _____ | _____ |
| **16** | 3 | _____ | 0.674 | _____ | _____ | _____ |
| **17** | 10 | _____ | 0.666 | _____ | _____ | _____ |
| **18** | 6 | _____ | 0.656 | _____ | _____ | _____ |
| **19** | 8 | _____ | 0.631 | _____ | _____ | _____ |
| **20** | 1 | _____ | 0.510 | _____ | _____ | _____ |
| **21** | 36 | _____ | _____ | 0.696 | _____ | _____ |
| **22** | 46 | _____ | _____ | 0.652 | _____ | _____ |
| **23** | 22 | _____ | _____ | 0.616 | _____ | _____ |
| **24** | 16 | _____ | _____ | 0.537 | _____ | _____ |
| **25** | 18 | _____ | _____ | 0.511 | _____ | _____ |
| **26** | 26 | _____ | _____ | 0.464 | _____ | _____ |
| **27** | 21 | _____ | _____ | 0.440 | _____ | _____ |
| **28** | 48 | _____ | _____ | _____ | 0.700 | _____ |
| **29** | 47 | _____ | _____ | _____ | 0.653 | _____ |
| **30** | 49 | _____ | _____ | _____ | 0.637 | _____ |
| **31** | 42 | _____ | _____ | _____ | 0.615 | _____ |
| **32** | 41 | _____ | _____ | _____ | 0.610 | _____ |
| **33** | 50 | _____ | _____ | _____ | 0.594 | _____ |
| **34** | 45 | _____ | _____ | _____ | 0.587 | _____ |
| **35** | 44 | _____ | _____ | _____ | 0.573 | _____ |
| **36** | 19 | _____ | _____ | _____ | _____ | 0.730 |
| **37** | 12 | _____ | _____ | _____ | _____ | 0.629 |
| **38** | 20 | _____ | _____ | _____ | _____ | 0.611 |
| **39** | 15 | _____ | _____ | _____ | _____ | 0.603 |
| **40** | 17 | _____ | _____ | _____ | _____ | 0.575 |
| **41** | 13 | _____ | _____ | _____ | _____ | 0.378 |

## *Appendix B. Item–Total Correlation Coefficients of the Social Dimensions of Cybersecurity Scale*

*Table A2: Item–Total Correlation Coefficients for the Social Dimensions of Cybersecurity Scale.*

| **Dimension** | **Item No.** | **Correlation with Total Score** | **Dimension** | **Item No.** | **Correlation with Total Score** | **Dimension** | **Item No.** | **Correlation with Total Score** | **Dimension** | **Item No.** | **Correlation with Total Score** | **Dimension** | **Item No.** | **Correlation with Total Score** |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| Dimension 1: Cyber Culture and Society | 1 | 0.589** | Dimension 2: Cyber Awareness and Perception | 10 | 0.674** | Dimension 3: Trust and Privacy in the Digital Environment | 19 | 0.696** | Dimension 4: Governance and Social Support | 26 | 0.727** | Dimension 5: Digital Actions and Practices | 34 | 0.649** |
| | 2 | 0.730** | | 11 | 0.723** | | 20 | 0.676** | | 27 | 0.798** | | 35 | 0.631** |
| | 3 | 0.742** | | 12 | 0.684** | | 21 | 0.593** | | 28 | 0.809** | | 36 | 0.604** |
| | 4 | 0.755** | | 13 | 0.813** | | 22 | 0.790** | | 29 | 0.794** | | 37 | 0.771** |
| | 5 | 0.763** | | 14 | 0.722** | | 23 | 0.636** | | 30 | 0.736** | | 38 | 0.645** |
| | 6 | 0.838** | | 15 | 0.804** | | 24 | 0.760** | | 31 | 0.546** | | 39 | 0.640** |
| | 7 | 0.844** | | 16 | 0.763** | | 25 | 0.798** | | 32 | 0.676** | | | |
| | 8 | 0.813** | | 17 | 0.827** | | | | | 33 | 0.776** | | | |
| | 9 | 0.778** | | 18 | 0.811** | | | | | | | | | |
| | | | | | | | | | | | | | | |

**Note: ** Indicates Significance at the 0.01 Level.**