International Journal of Multidisciplinary Research and Publications
ISSN (Online): 2581-6187

Culture and Cybersecurity: Why Trust and Data Ownership Mean Different Things Around the World

Vo Thy Tran[1], Beverly Grace Clapano Oblina[2]
[1]Student, Vinschool Central Park, Ho Chi Minh City, Vietnam, 700000
[2]AP Seminar, Academic Writing, & ESL Teacher, ESL Standard Department, Vinschool Central Park, Ho Chi Minh City, Vietnam, 700000
Email address: beverlygrace90210@gmail.com

Abstract*—Norms and values influence how people react to data breach and misuse significantly. This article analyzes how a collectivist society and an individualist society will respond differently when a data security incident occurs, focusing on how trust, perceived privacy, and accountability play critical roles. Additionally, power distance impacts attitudes towards data ownership and reactions to violations, with high power distance cultures accepting corporate data ownership, whereas individuals in low power distance cultures perceive personal ownership. The study further considers the role of information-security consciousness, sectoral reactions—particularly in the health sector—and cross-cultural differences in online information revelation. The findings underscore the need for culturally sensitive cybersecurity strategies that consider societal values, power structures, and awareness levels to enhance global data protection efforts*.

***Keywords*—** *Cultural norms; data breaches; cybersecurity; power distance; collectivism; individualism; data privacy; trust*.

I. Explanation Of Terms

Individualistic cultures hold individual freedom, autonomy, and achievement paramount. Members in such societies put self-interest and one's own needs ahead of collective interests. Individualistic cultures most frequently are found in Western countries, like America and most nations of Europe, where personal and national independence, and individual accomplishment, are of great value.

Collectivist cultures prioritize group harmony, interdependence, and collective welfare over individual interests. Collectivist individuals also identify themselves in terms of their social group, family, or community and stress cooperation, loyalty, and shared responsibility as important values. This culture prevails in most Asian cultures, such as China, Japan, and Vietnam, where social harmony and collective obligations are essential values.

High power distance culture refers to societies where unequal power distribution and hierarchical organization are widely accepted and endorsed. In these societies, the power-holding authorities possess vast amounts of power, and subordinates must demonstrate obedience and respect. Centralized decision-making and limited social mobility are possible. China, India, Mexico, and the majority of Middle Eastern nations are classified as high power with strong cultural endorsement of deference to authority and rigid social hierarchies.

Low power distance culture is a society where equality, open communication, and a more decentralized distribution of power are stressed. The societies in these places have accessible authority and individuals who actively participate in decision-making. There are hierarchies but these are less institutionalized so that there is greater social mobility. Denmark, Sweden, the Netherlands, and Australia are some countries with low power distance, where egalitarian values and collaboration are valued over hierarchical systems.

II. Introduction

People don't just have inherent responses to data breaches and unauthorized usage of data—those responses are shaped by cultural norms and values. Reactions to security incidents vary across cultures due to differing perceptions of privacy, trust, and accountability. Recognizing these cultural dimensions is essential for designing cybersecurity strategies that accommodate diverse perspectives and motivations (Zoran et al, 2015).

Research Question: *How do cultural norms, including power distance and individualism-collectivism, influence responses to data breaches and cybersecurity policies?*

By analyzing cultural factors that shape attitudes toward data security, this paper aims to determine how cybersecurity policies can be tailored to different cultural contexts to maximize effectiveness. As Henry et al mentioned in the research, understanding these cultural influences is critical in creating cybersecurity strategies that gain widespread acceptance across varied populations.

III. Methodology

This research employs a qualitative, secondary data analysis approach to examine how cultural norms—specifically individualism versus collectivism and power distance—affect responses to data breaches and cybersecurity policies. The study synthesizes findings from peer-reviewed journal articles, global cybersecurity reports, and cross-cultural studies to analyze patterns of behavior and perception across different societies.

Research Scope: The study focuses on cultural dimensions across regions such as Asia, Europe, and North America, comparing societal responses to data breaches. Particular attention is given to the healthcare sector due to its heightened sensitivity to privacy concerns.

Vo Thy Tran and Beverly Grace Clapano Oblina, "Culture and Cybersecurity: Why Trust and Data Ownership Mean Different Things Around the World," *International Journal of Multidisciplinary Research and Publications (IJMRAP)*, Volume 7, Issue 11, pp. 10-12, 2025.

Limitations: This paper does not include primary data collection. As a result, the analysis is interpretive and may not capture real-time behavioral responses. Additionally, cultural values are not the sole determinants of data breach responses—legal, economic, and technological factors also play a role. Future studies should incorporate empirical methods such as surveys or interviews to validate these findings in specific national contexts.

IV. High Collectivist vs. Individualistic Cultural Responses

High collectivist cultures emphasize a sense of community, trust in society, and shared responsibility. Since data breaches jeopardize the notion of communal well-being, reactions could be much stronger in more collectivist societies. For instance, such cultures call for collective reactions, such as public demonstrations to take organizations to account, thus retrieving lost trust. (Gorkhali et al., 2024) This collective reaction also follows from the preeminence that cultures grant to the interests of society as compared to those of the individual citizen. In contrast, individualistic cultures prioritize personal impact and autonomy. Individuals in these societies may focus on seeking legal recourse or addressing the breach's implications for their personal data, reflecting a sense of ownership and individual responsibility (Ablon et al., 2016).

V. The Role of Power Distance In Data Breaches

The influence of cultural norms extends beyond collectivism and individualism. Power distance—a measure of the acceptance of unequal power distribution in society—also plays a significant role in shaping reactions to data breaches.

High power distance culture

In cultures with high power distance, individuals are more likely to view companies as having a superior status or authority in society. According to Madan et al, their research has shown that more than 75% of Asian consumers believe that the responsibility to protect their information lies in the hands of companies or the government (Yu, 2020) and hence, individuals from high power distance culture might tend to believe that the company has ownership of data submitted. Therefore, users in these cultures may feel obliged to relinquish data ownership to the company simply by using its services. This mentality is a product of a notion that the organization, as an authority, commandeers control over the data (Madan et al., 2023). Also, in high power distance cultures, individuals are more susceptible to accept companies' terms and conditions without questioning the change in ownership. Since users can perceive that the company takes ownership of the data once posted, they attribute any data loss to the company's fault. Their outrage for the breach, hence, can be minimal, and they are less likely to reduce their usage of the business.

Low Power Distance Culture

On the other hand, individuals from low power distance cultures view their data as their own and may be more likely to take responsibility for it (Demmers et al., 2021). When there is a violation, they are likely to perceive it as an encroachment of their individual rights and hence be more likely to sever their association with the company. Moreover, consumers from low power distance cultures, for whom information about them is theirs, would feel violated if there is a breach and would sever their relationships with the firm, believing the company has violated something belonging to them. In that sense, a breach would be a personal invasion of their rights; thus, more intensive feelings of distrust and discontinuing business with the organization in question can be expected to take place as 74% of U.K. consumers reported that they would not shop with an online business that had experienced a data breach in the past year (PCIPal, 2020).

VI. Global Challenges in Addressing Data Breaches

The intersection of cultural norms with power distance and information-security awareness underlines the global complexity when dealing with data breaches. Such is the case where, in a high power distance society, individuals are likely to accept the terms and conditions without giving much scrutiny, viewing data ownership is transferred to the organization. Their concern for breaches is then lower because it is a problem for the company. People in low power distance cultures question such agreements and consider the ownership of their data as theirs, thus reacting more strongly when this is breached. In other words, cultural background and values greatly influence people's responses to data breaches or unauthorized uses of data. It is within these lines that differences in privacy, trust, and responsibility exist, which culturally requires a different approach to cybersecurity strategies (Simon et al, 2017). Organizations should be aware of these cultural dimensions and adapt to them in order to meet information security challenges and engender trust among diverse populations. Integrating cultural awareness into data protection initiatives helps businesses navigate the complexities of global operations and build resilient systems that resonate with varying societal expectations.

VII. Conclusion

The study highlights the profound influence of cultural norms and values on responses to data breaches, emphasizing the role of collectivism versus individualism and power distance in shaping attitudes toward data security. In collectivist societies, individuals prioritize communal trust and may advocate for collective accountability, while those in individualistic cultures focus on personal recourse and autonomy in managing data breaches. Similarly, high power distance cultures are more likely to accept corporate ownership of data and defer responsibility to organizations, whereas low power distance cultures perceive data as personal property and react strongly to violations.

These cultural differences underscore the need for cybersecurity strategies that are not only technically robust but also culturally adaptive. Organizations must tailor their data protection efforts by considering societal attitudes toward privacy, trust, and responsibility. Integrating cultural

Vo Thy Tran and Beverly Grace Clapano Oblina, “Culture and Cybersecurity: Why Trust and Data Ownership Mean Different Things Around the World,” *International Journal of Multidisciplinary Research and Publications (IJMRAP)*, Volume 7, Issue 11, pp. 10-12, 2025.

sensitivity into cybersecurity policies can enhance compliance, build trust, and foster greater engagement in security practices across diverse populations.

Future research should incorporate empirical studies, such as surveys or interviews, to validate these cultural impacts across different regions and industries. Additionally, examining the intersection of cultural norms with legal frameworks and economic conditions would provide a more comprehensive understanding of global data protection challenges. By acknowledging cultural diversity in cybersecurity approaches, policymakers and organizations can develop more effective and inclusive strategies to mitigate data breaches and enhance global digital security.

VIII. Solutions

Technological Innovations

Culturally flexible security solutions facilitate data protection alignment with society. Regional perceptions of privacy must be envisioned in encryption, authentication, and access control (ErsinArtificial intelligence-driven cyber security solutions extend security further by identifying threats and countering them and becoming culturally attuned to risk perceptions and trust levels for effectively safeguarding the world.

Cultural Sensitivity in Cybersecurity

Security education has to respect cultural values and emphasize group or individual responsibility within collectivist and individualistic societies. Company policy has to react sensitively to differing privacy needs, establish confidence, and compliance. A culturally informed approach enhances comprehension of security and aligns organizations with both global and local regulations.

Education and Public Engagement

Public awareness campaigns need to consider cultural perceptions regarding data security to help enable greater adoption of cybersecurity practice. Implementing cybersecurity training in school curricula equips future generations with the understanding and competencies needed to safeguard their digital information, reducing threats and improving overall security awareness. (Cheung et al, 2022)

References

[1]. Simon, S. “Doc,” & Cagle, C. (2017). Culture’s impact on trust, distrust, and intentions in data theft environments: A cross-cultural exploratory study. *Journal of Global Information Technology Management*, *20*(4), 214–235. https://doi.org/10.1080/1097198X.2017.1388672

[2]. Henry, Collier., Charlotte, Morton., Dalal, Alharthi. (2023). Cultural Influences on Information Security. 22(1):143-150. https://doi.org/10.34190/eccws.22.1.1127

[3]. Madan, S., Savani, K., & Katsikeas, C. S. (2023). Privacy please: Power distance and people’s responses to data breaches across countries. *Journal of International Business Studies*, *54*(4), 731–754. https://doi.org/10.1057/s41267-022-00519-5

[4]. Ersin, Dincelli. (2018). The Role of National Culture in Shaping Information Security and Privacy Behaviors. Research Papers in Economics, 47-68. https://doi.org/10.1142/9789813149106_0003

[5]. Zoran, Milanović., Radovan, Radovanović. (2015). Information-security culture: Imperative of contemporary society. 20(3):45-65. doi: 10.5937/NBP1503045M

[6]. Anjee, Gorkhali., Rajib, Chowdhury., Wei, Chen. (2024). Are we neglecting the influence of national culture (individualism–collectivism index) in mitigating the instances of data breach?. Journal of Systems and Information Technology, https://doi.org/10.1108/JSIT-11-2023-0262

[7]. Ablon, L., Heaton, P., Lavery, D. C., & Romanosky, S. (2016). *Consumer attitudes toward data breach notifications and loss of personal information*. Santa Monica, CA: RAND Corporation. Retrieved from https://www.rand.org/pubs/research_reports/RR1187.html

[8]. Cheung, R., Jolly, S., Vimal, M., & others. (2022). Who’s afraid of genetic tests? An assessment of Singapore’s public attitudes and changes in attitudes after taking a genetic test. *BMC Medical Ethics*, *23*(5). https://doi.org/10.1186/s12910-022-00744-5

[9]. Simon, Teuscher. (2022). The Role of Gender, Age and Cultural Differences in Online Information Disclosure and Privacy: A Systematic Review. 737-751. https://doi.org/10.1007/978-3-031-09070-7_61

[10]. Demmers, J., Weihrauch, A. N., & Mattison Thompson, F. H. (2021). Your data is (not) my data: The role of social value orientation in sharing data about others. *Journal of Consumer Psychology*. https://doi.org/10.1002/jcpy.1255