A Comparative Assessment of Human Factors in Cybersecurity with Implications for Cyber-governance

Farkhund Iqbal
College Technological Innovation, Zayed University, Dubai, UAE

Farkhund.Iqbal@zu.ac.ae

Summary

Cybersecurity and cyber vulnerabilities are usually attributed to various physical and humanistic, or social factors. Many global institutional policymakers and governments prefer building more robust physical infrastructures to counter them. This phenomenon is also recognized as an outdated "Castle Model,"1 according to which thick defense boundaries (or walls) are built around the system to protect against security breaches. The Castle Model helps protect; however, due to cultural diversity, complex socio-technical systems, and cybersecurity awareness levels among global populations, it is challenging for governments and concerning stakeholders to eradicate these cyber risks. Therefore, a detailed evidence-based investigation of human factors and cyber risk awareness levels is required to build a holistic cybersecurity framework. According to a general observation, global Internet users possess divergent habits and behaviours while operating online. To support this point, according to the Cybersecurity Exposure Index (CEI, 2020)2, the United States of America (USA) has one of the lowest exposure rates of 0.145, whereby the United Arab Emirates (UAE) has a comparatively higher exposure index of 0.359. Consequently, the Gulf Cooperation Council (GCC) region seems more exposed to cyberattacks than the United States of America (USA). These facts illustrate that there are significant differences in the cybersecurity risk awareness of various countries. We suspect that global cybersecurity exposure scores result from behavioural aspects of human factors that influence cybersecurity awareness. For instance, the diversity between cultures, socioeconomic characteristics, digital divide, education, and beliefs of people living in the GCC countries versus the USA directly influences these rankings. Therefore, we plan to pursue an evidence-based safety and cybersecurity assessment study that provides a clear roadmap for better cyber-governance in the UAE.

---

[1] Leuprecht, C., Skillicorn, D. B., & Tait, V. E. (2016). Beyond the Castle Model of cyber-risk and cyber-security. *Government Information Quarterly*, *33*(2), 250-257.

[2] The lower the score, the lower the exposure. The Cybersecurity Exposure Index (CEI) reports the score between 0 and 1. URL: https://passwordmanagers.co/cybersecurity-exposure-index/

This working paper provides insights about cybersecurity awareness in the young, educated, and technology-savvy population of the UAE, in comparison to the USA for advancing the scholarship and practice of global cyber-governance. We conducted comparative empirical studies to identify the differences in specific human factors that affect cybersecurity behaviour in the UAE and the USA. In addition to systematically reviewing prior literature, we developed a survey to reflect on the feedback with three global cybersecurity experts, who specialize in cybersecurity awareness and cybercrimes prevention. In a thirty minutes interview, these experts helped enlist the most common cybercriminal activities in the global and GCC regional context. We then applied a thematic analysis to craft fourteen distinct human factors as survey questions. A total of 165 respondents from the UAE, and 157 respondents from the USA populations participated in the survey study. In addition, we employed several control variables to observe reliable results.

The results show that the tech-savvy and educated populations in the UAE and USA regions demonstrate cultural and behavioural differences with respect to our 'elicited' cybersecurity awareness constructs and overlooked human factors. These findings also indicate that our targeted population in the UAE is very conservative about fully exploring the extent of online services (e.g., banking, shopping, and social media) compared to the USA population. There are two possible explanations for this behaviour in the UAE respondents: a) lack of awareness about these factors, or b) lack of trust in operating safely online. Either way, this depicts an important area for further exploration. We believe that our empirical findings provide guidance for cybersecurity policymakers in the UAE and the extended GCC region to focus on these significant factors for enhancing cyber safety, awareness, and trust. We also propose various interventions that relevant stakeholders, such as governments and law enforcement agencies, can implement to reduce cyber risks in the region.