


Exploring the Relationship Between Technology Adoption and Cyber Security Compliance: A Quantitative Study of UTAUT2 Model

Mohammed Saeed A Alqahtani, University of Technology Sydney, Australia

 <https://orcid.org/0000-0003-0581-5674>

Eila Erfani, University of Technology Sydney, Australia

ABSTRACT

IT infrastructure and systems are made up of technical and social systems that work together to ensure that organization's goals and objectives are met. Security controls and measures are developed and used to protect an organization's data and information systems. To improve cyber security, organizations focus most of their efforts on incorporating new technological approaches in products and processes, leaving out the most important and vulnerable factor. So this study intends to provide some practical implications to the technology developers and policymakers while identifying the factors that affect cyber security compliance in an organization or home environment for general users, HR, IT administrators, engineers, and others. It explored the Unified Theory of Acceptance and Use of Technology 2 (UTAUT2) model and assessed the effect of its factors on cyber security compliance in organizations.

KEYWORDS

Compliance Relationship, Cyber Security Compliance, Human Behaviour, Technology Adoption, UTAUT2

INTRODUCTION

Organizations are vulnerable to cyber-attacks partially because people in the organization are unaware of or unprepared for cyber risks. People are one of the major causes of cyber security breaches (Avina et al., 2017; Huang and Pearlson, 2019). Organizations spend millions of dollars on their cyber security infrastructure that includes technical and non-technical measures, but most times leave the most important asset and vulnerability open– the human. Therefore, despite their investments, companies are not able to reap the benefits of their security investments because of human/employee's non-compliance with cyber security policies and measures. Cyber security non-compliance is a major concern for organizations (Alqahtani & Braun, 2021; Harris & Martin, 2019). For effective compliance and human acceptance of cyber security technology and compliance with cyber practices, it is crucial to identify, research, and analyse the factors that affect cyber security compliance and implementation. Furthermore, the users need to understand, take, and conform to the security measures of the organization's information security so that companies can reap the benefits of their technology investments. In Donalds and Osei-Bryson (2020) and Li et al. (2019), the authors concluded that the

DOI: 10.4018/IJEGR.2021100103

Copyright © 2021, IGI Global. Copying or distributing in print or electronic forms without written permission of IGI Global is prohibited.

behavior of employees has a direct relationship with effective information system security compliance. Many cyber security incidents have occurred due to the negligence of cyber security policies (Harris and Martin, 2019; Herath and Rao, 2009; Li et al., 2019). Institutionalization of security policies into practice makes the employees embrace the policies, which makes their behavior more compliant (Alqahtani & Braun, 2021; Harris & Martin, 2019; Li et al., 2019).

Different factors affect the behavior of employees towards cyber security compliance. For cyber security compliance, most of the times, certain new technologies also need to be adopted (Alqahtani & Braun, 2021; Baptista & Oliveira, 2015). Many theories and models are proposed in literature that affect human behavior towards technology adoption. One of the most widely accepted technology adoption models is Unified Theory of Acceptance, Use of Technology (UTAUT) (Venkatesh et al., 2003) and UTAUT2 (Venkatesh et al., 2012).

In this study, all the factors of UTAUT2 model have been explored for cyber security compliance. Limited literature is available that link constructs of UTAUT2 model with cyber security compliance. But there are several weaknesses in the previous studies. Most of the previous studies are biased towards a specific group of people and not applicable to general users or employees. For example, the detailed study conducted by Almaiah, Alamri, and Al-Rahmi (2019), Cuganesan, Steele, and Hart, (2018), D'Arcy and Greene (2014), Hu et al., (2012), Liu, Wang, and Liang (2020), S. Raschid Muller and Mary L. Lind (2020), and Simonova, (2020) is biased in several ways. They had focused on a very limited group of people with specialized professions. For example, in S. Raschid Muller and Mary L. Lind (2020), information security professionals are expected to have a better understanding of information security policies than regular employees (Ahlan, Lubis, and Lubis, 2015; Bauer, Bernroider, and Chudzikowski, 2017). Due to the limitations and bias in the previous studies related to technology adoption and security compliance, the results are very weak and difficult to digest. For example, S. Raschid Muller and Mary L. Lind (2020) suggested that UTAUT2 may not be a very good model for inspecting Information Security Policy (ISP) compliance amongst information security professionals. This may not be the case with the general public and employees of organizations because information assurance professionals usually have more knowledge and bias towards compliance. Therefore, this may not be the case for all employees. This study is performed on general users in organizations.

For this purpose, a correlational study has been performed by collecting data from 180 employees working on different positions and organizations. Several hypotheses are formulated and tested with different tests. This study reports the results of the quantitative study on the UTAUT2 factors. The main objective of this study was to assess and model the factors for cyber security compliance. The two sub-research objectives the present study addressed are; i) to explore the effect of the UTAUT2 constructs performance expectancy, effort expectancy, social influence, facilitating conditions, hedonic motivation, price value, and habit on individuals' cyber security compliance behavior (i.e., behavioral intentions); ii) to examine the effect of performance expectancy and effort expectancy both on IT and security administrator roles, as well as on general users.

THEORETICAL DEVELOPMENT AND CONCEPTUAL MODEL

Cyber security compliance is a multidimensional discipline, and these disciplines are interconnected to ensure the implementation of cyber security policies and their compliance across the organization (Alqahtani & Braun, 2021; Donalds & Osei-Bryson, 2020; Harris & Martin, 2019). If the end-user(s) and employees of the organization do not consider the importance of cyber security policies and do not practice and follow these policies, then the organization will be at risk of cyber-attack or data breach. As a result, the individual or personal behavior aspect of cyber security must be considered in the overall cyber security posture. Several studies are carried out on the impact of behavior on cyber security (Alqahtani & Braun, 2021; Avina et al., 2017; Donalds & Osei-Bryson, 2020; Harris & Martin, 2019).

21 more pages are available in the full version of this document, which may be purchased using the "Add to Cart" button on the publisher's webpage: www.igi-global.com/article/exploring-the-relationship-between-technology-adoption-and-cyber-security-compliance/289355

Related Content

An Analysis of the Impact of Business Networks on Technology Development: Using Agent-Based Modeling

Maryam Ebrahimi (2019). *Private Sector Innovations and Technological Growth in the MENA Region* (pp. 20-44).

www.irma-international.org/chapter/an-analysis-of-the-impact-of-business-networks-on-technology-development/216158

Web 2.0 and Government Transformation: How E-Government and Social Media Contribute to Innovation in Public Services

Jon E. Glasco (2012). *Digital Democracy: Concepts, Methodologies, Tools, and Applications* (pp. 1861-1882).

www.irma-international.org/chapter/web-government-transformation/67690

Policy Testing in Virtual Environments: Addressing Technical and Legal Challenges

Magdalini Kardara, Omri Fuchs, Eleni Kosta, Fotis Aisopos, Ilias Spaisand Theodora Varvarigou (2012). *International Journal of Electronic Government Research* (pp. 1-21).

www.irma-international.org/article/policy-testing-virtual-environments/70073

The Social Media, Politics of Disinformation in Established Hegemonies, and the Role of Technological Innovations in 21st Century Elections: The Road Map to US 2020 Presidential Elections

Ikedinachi Ayodele Power Wogu, Sharon Nanyongo N. Njie, Jesse Oluwafemi Katende, George Uzoma Ukagba, Morris Oziegbe Edogiawerieand Sanjay Misra (2020). *International Journal of Electronic Government Research* (pp. 65-84).

www.irma-international.org/article/the-social-media-politics-of-disinformation-in-established-hegemonies-and-the-role-of-technological-innovations-in-21st-century-elections/265514

State e-Government Portals in Malaysia: An Empirical Investigation

Aria Asadi Eskandarand Murali Raman (2013). *International Journal of Electronic Government Research* (pp. 19-46).

www.irma-international.org/article/state-government-portals-malaysia/78299