Modelling a Cyber Security Model for Educational Sector: The Perspective of Privacy Calculus Theory

Adamu Abbas Adamu
Joseph Sia Kee Ming
Curtin University, Malaysia

The exponential growth of the internet interconnections has resulted to the emergence of threats to our cyber space and has significantly affect society, physical structure and economy. Cybercrimes are becoming more sophisticated with electronic gadgets continuously embedded and resulting in an increase in cyber-attacks. Trends have shown that education sector is among the top 10 most impacted sector by cybercrime. The unintentional violation of internet security guidelines is causing a serious concern to practitioners. One of the top security risks is phishing where educational sector employees may click malicious link or reply to the phishing emails which results the disclosure of confidential information such as account and password used to login to educational systems to attackers. Also, higher educational institutions (HEIs) employees may unintentionally run malicious software which impact teaching and administration systems causing sensitive and private stakeholder's records to be leaked to malicious attackers. In fact both students and staff are susceptible to be victim of this cyberattacks making HEIs a focal point of investigation. The situation is getting more sophisticated that an intervention is in dire need to forestall and prevent the attacks in the sector that is a pillar in all societies. Furthermore, the COVID-19 Pandemic has enforced the education sector to rapidly embrace the use of technology in education delivery. This has make it even more expose to the cyber world. Thus making it a potential priority for investigation by researchers. In Malaysia, cyber security particularly in the education sector is still at the infancy stage and limited studies have been conducted on cyber security with regard to non-technological aspect. The Privacy Calculus Theory (PCT) has mainly been used by the researchers in the context of economics and information technology. Applying it in an organizational perspective mainly education sector will provide new evidence on how the education industry can be protected from cyber-attacks. Therefore, this study aims to examine the antecedents of intention to disclose information within the premise of PCT in HEIs in Malaysia. Hence, we extend the PCT with information from past studies regarding intention to disclose information. The model consists of punishment severity, perceived benefits, perceived risk awareness and perceived organizational support, national culture and intention to disclose information constructs. A total of 400 questionnaires will be distributed to HEI employees in Malaysia. SmartPLS will be used to analyse the data and validate the proposed model. This study is one the few studies to be conducted on cyber security in a non-technological aspect of an educational sector. The study extended the PCT by including national culture to understand the intention to disclose information among employees in HEIs. The findings of the study are expected to promote the country image particularly in cyber security management, enhance educational information security of the country.

Keywords**:** *Intention to Disclose Information, National Culture, Perceived Benefits, Perceived Organizational Support, Perceived Risk Awareness, Punishment Severity*