Chapter 17
Towards a Student Security Compliance Model (SSCM): Factors Predicting Student Compliance Intention to Information Security Policy

Felix Nti Koranteng
https://orcid.org/0000-0001-5917-381X
University of Education, Winneba, Kumasi Campus, Ghana

ABSTRACT

Users are considered the weakest link in ensuring information security (InfoSec). As a result, users' security behaviour remains crucial in many organizations. In response, InfoSec research has produced many behavioural theories targeted at explaining information security policy (ISP) compliance. Meanwhile, these theories mostly draw samples from employees often in developing countries. Such theories are not applicable to students in educational institutions since their psychological orientation with regards to InfoSec is different when compared with employees. Based on this premise, the chapter presents arguments founded on synthesis from existing literature. It proposes a students' security compliance model (SSCM) that attempts to explain predictive factors of students' ISP compliance intentions. The study encourages further research to confirm the proposed relationships using qualitative and quantitative techniques.

INTRODUCTION

Secured management of Information Security (InfoSec) continues to be one of the most relevant issues within organizations. This is because they thrive on intense use of information, hence there is no ambiguity that InfoSec is core to its activities. Traditionally, InfoSec has focused mostly on technological solutions (Öugütçü, Testik, & Chouseinoglou, 2016). However, the need for end-user behaviour has gained attention in recent times (Safa, Von Solms, & Furnell, 2016). This is because of the inability to monitor user behaviour at all times regardless of the increased sophistication of Information and Technology infrastructure and software development. Practitioners and researchers in InfoSec have come to realize

DOI: 10.4018/978-1-6684-3698-1.ch017

that there is a need for Information Systems security solutions to cover a wider range of activities and give equal attention to all. This is because, technology alone cannot be effective for addressing information security issues (Herath & Rao, 2009). Accordingly, research in InfoSec now addresses issues in three main areas namely; people, process and technology. With regard to technology, research work targets the introduction of infrastructure and cryptographic algorithms that enhance methods for prevention, detection, and response to security breaches. Similarly, security processes within the organization have been improved to ensure minimal compromise on confidentiality, integrity, and availability of information. Research on the psychological aspect and behaviour of users has also explored users' compliance with Information Security Policies (ISPs). Consequently, a number of factors have been identified to impact security compliance.

Even though this approach has proven to be somehow effective, majority of the existing studies that have empirically evaluated factors that impact InfoSec behaviour tend to draw their samples from employees of various organizations with little attention to academic institutions. Yet, these factors cannot be generalized and thus it is expected that they may not impact especially students in the manner in which they impact employees. It is however imperative to turn attention to InfoSec issues within higher education institutions considering their high consumption, usage, and knowledge of technology (Öugütçü et al., 2016). This raises further concerns given the increased risk that is associated with cyberspaces. Worriedly, studies that analyze the factors that impact student's compliance with ISPs in developing communities such as Africa. There is enough evidence that students in such areas pay less attention to information security issues (Gross & Acquisti, 2005). Hence this study seeks to present a literature analysis on the factors that impact compliance to information security with a particular focus on African students. It is expected that the findings will provide meaningful information to researchers and practitioners on how to promote information security policy compliance among students. This study, therefore, seeks to provoke thinking and argue for the need for a tailor-made model specific to explaining students' ISP compliance.

LITERATURE REVIEW

The importance of organizations' information security cannot be overemphasized. Hence, technological as well as behavioural measures are often initiated to curb the adverse effects of improper use and policy non-conformity. However, behavioural issues top the approaches in safeguarding information (Safa et al., 2016). Therefore, scholars have explored various avenues in an attempt to explain information security behaviour. Considering that human behaviour is complex and difficult to understand (Wiafe, Nakata, Moran, & Gulliver, 2011). Mostly, the factors that determine adherence to policies meant to guide security behaviour has been explored. Extant studies agree that deterrent mechanisms such as fear appeal, threat, certainty of and severity of punishment are effective in guiding people to comply with security policies (Cheng, Li, Li, Holm, & Zhai, 2013; Herath & Rao, 2009; Safa et al., 2019). Other studies have argued that concepts such as habit strength, security support, prior experiences, self-efficacy, and perceived vulnerability are more effective in explaining information security compliance (Ifinedo, 2012; Johnston & Warkentin, 2010; Tsai et al., 2016).

As already mentioned, majority of these existing studies tend to focus on information security issues within organizations with less attention on higher education institutions. Yet, students of higher education do not have the same psychological contract as compared to employees in organizations. This is