Chapter 21
Modelling Cyber-Crime Protection Behaviour among Computer Users in the Context of Bangladesh

Imran Mahmud
University Sains Malaysia, Malaysia & Daffodil International University, Bangladesh

T. Ramayah
University Sains Malaysia, Malaysia & International Business School, Universiti Teknologi Malaysia, Malaysia

Md. Mahedi Hasan Nayeem
Daffodil International University, Bangladesh

S. M. Muzahidul Islam
Daffodil International University, Bangladesh

Pei Leng Gan
University Sains Malaysia, Malaysia

ABSTRACT

This study examined the impact of security champion and security training on protection behaviour in the context of IT service oriented SMEs in Bangladesh. Drawing upon protection motivation theory, this study examined the influence of security training on threat appraisal and influence of security training on coping appraisal which leads to protection behaviour via protection motivation. Data was collected from six different IT service oriented organizations with a sample size of 147 by survey questionnaire. Data was analysed using partial least squares (PLS) technique and result shows that perceived value of data, security training and threat appraisal are strong predictors of threat appraisal, protection motivation and protection behaviour. Theoretical contribution and practical implications of this research are also discussed.

DOI: 10.4018/978-1-7998-2466-4.ch021

INTRODUCTION

The advancement of the information and telecommunication technology (ICT) in Bangladesh in recent years has improved the infrastructure of information sharing through the Internet. According to the Bangladesh Telecommunication Regulatory Commission (BTRC), the total number of Internet subscribers has reached 61.288 million in Bangladesh. Among the 61 million, mobile internet has the biggest subscribers with 58.045 users, followed by 0.131 million Wimax users and 3.112 million users from Internet service providers. Aligned with cyber infrastructure growth, the possibilities of computer users being vulnerable to various security threats via Internet are higher too (Anderson & Agarwal 2010). Despite being ranked 11th globally in cyber security preparedness (Bhuiyan et al. 2016), recently at a seminar in Bangladesh, experts and researchers observed that cybercrimes increased at an alarming rate along with the rapid rise of Internet users at both individual and institutional levels (Nashique, 2015). The recent case of cyber-attack on Bangladesh's central bank that let hackers steal over $80 million from the Federal Reserve bank account was reportedly caused by the Malware installed on the Bank's computer systems. Development of ICT changed the how organizations operate, data and information which were once stored and kept in cabinets and files and today they are paperless. Similar to other organizations in developing countries, the modern organizations in Bangladesh depend on information systems (IS) for their survival. The systems used in the organizations contained priceless organizational data and resources (Cavusoglu et al., 2004; Ifinedo, 2009, 2012). In order to safeguard the critical IS assets held in such systems from misuse, abuse and destruction; organizations often utilize a variety of tools and measures such as installing firewalls, updating anti-virus software, backing up their systems, maintaining and restricting access controls, using encryption keys, using surge protectors, and using comprehensive monitoring systems (Workman et al., 2008; Lee & Larsen, 2009, Ilfendo, 2011). Individual level digital crimes include cyber stalking, cyber harassment, morphing and obscene publication, email/profile hacking, spoofing, cyber pornography including revenge porn, internet voyeurism, cyber defamation, cyber bullying, email harassment, cyber blackmailing, threatening, emotional cheating by impersonation, intimate partner violence through internet and abetment of such offences. It was also acknowledged by the Central Bank that "Bangladesh remains vulnerable to cyber-attacks because traditional cyber defences such as anti-virus software and firewalls are ineffective against new threat vectors such as zero-day malware and Advanced Persistent Threats (APT)" (Zamir, 2016). This has led the Information and Communication Technology (ICT) Ministry of Bangladesh to take the importance of activities related to building awareness to prevent such cybercrimes (Zamir, 2016). Despite having technological measures such as antivirus software, regulations and security policy are also widely used as methods to reduce the chance of cyber-attacks. In a study conducted by Warkentin and Willison (2009) indicated that many users do not follow the policy to protect organizations or themselves from cybercrime. The major reason behind this is insufficient crime protection behaviour from the users (Anderson & Agarwal 2010).

The goal of this paper is to understand the phenomenon of protection motivation, its antecedents and protection behaviour of individual computer users of government banks. Recently Srisawang et al. (2015) and Ifinedo (2012) investigated the factors rooted in protection motivation theory and theory of planned behaviour to explain computer users' protection behaviour. Our study aims to extend the knowledge of this particular behaviour by identifying several other factors like communication between IT department and other users, security champion and IT security training (Soto-Acosta et al. 2013; Travica, 2007). In doing so, the research questions of our study are: