Chapter 20
A Comparative Study in Israel and Slovenia Regarding the Awareness, Knowledge, and Behavior Regarding Cyber Security

Galit Klein
Ariel University, Israel

Moti Zwilling
Ariel University, Israel

Dušan Lesjak
International School for Social and Business Studies, Slovenia

ABSTRACT

With the COVID-19 pandemic, many organizations and institutions moved to e-learning and to e-working from home. With the increase in internet usage, the rate of cyber-attacks have also increased, and this was followed by the request for more cyber security behaviors from employees and students. In the current study, the authors explore the connection between cyber security awareness, cyber knowledge, and cyber security behavior. The authors measured the behaviors among students in two similar countries: Israel and Slovenia. Results show that students felt they had adequate awareness on cyber threat but apply only a few protective measures to protect their devices, usually relatively common and simple ones. The study findings also show that awareness to cyber threats mediate the connection between knowledge and protection behaviors, but only in the case that the knowledge is specific with regard to IT protection courses. Results, implications, and recommendations for effective cyber security training programs for organizations and academic institutions are presented and discussed.

DOI: 10.4018/978-1-6684-3698-1.ch020

INTRODUCTION

As the usage of internet increases, cyber security became one of the main concern for private individuals, companies and governments. Cyber threats include various malwares and cybercrime activities, such as the usage of trojan horses, worms, ransomware and spyware malware to perform attacks, collect information, bypass an unauthorised access to data assets and other kinds of hateful behaviours (Srinivas, Kumar Das & Kumar, 2019). These malicious attacks harming and causing disruption to business operations, financial loss but also reduce the trust between computer users and their companies services. In order to response to this problem government legislated several regulation that are aim to protect private and public sectors from crime behaviours, such as the 1996 Health Insurance Portability and Accountability Act (HIPAA) or the Federal Information Security Management Act (FISMA) (Srinivas et al., 2019).

Legislating regulation is just one solution, among others, that increases awareness to cyber hazards among others, including education and training programs. While education process and interactions is not considered as a new idea and has been introduced for several years (Dunn, 2012)[1] the new pandemic accelerated this process. Today, more than ever, children, students, teachers and lecturers are learning through the internets. According to Dunn (2012) the ability to access into unlimited amounts of data, cause them to expand their learning and knowledge horizons, but also to add to their dynamic educational experiences (Dunn, 2012). With that, moving to e-learning environment and relying on cyber technologies which are improved rapidly (from a technological perspective) had yield an increasingly difficult challenges to protect the users from malicious activities and cyber-attacks. As the potential for cyber-attacks became lucid, researches (e.g. Al-Janabi, S., & Al-Shourbaji, 2016; McDaniel, 2013) argue that educational institution should apply cyber awareness programs for cyber protection and cyber security methods. Awareness programs should provide cyber awareness program, cyber knowledge and cyber security active training for users and employees. The programs should be instrumental in developing and spreading security awareness among cyber users, employing proper physical access controls, obeying the security policies and rules as laid down by the institution and the firm in order to achieve the best security outcomes (McDaniel, 2013).

Several cyber security awareness training programs had been presented in the literature affiliated with the awareness program itself (Shaw et al., 2009). Other studies (Lehto, 2015) emphasized the need to understand the factors that motivate or suppress cyber hazard awareness among users. In the current study we will address another angel, and try to reveal *if there is a connection between cyber knowledge, cyber awareness and cyber security behaviours*. To measure these connections we conducted a comparison study in which we compare collected data by Israeli and Slovenian students from the department of Economics & Business Administration, in both countries. The data was defined by the following variables: cyber knowledge, cyber behaviour and the cyber security awareness. Implications and results are farther discussed.

LITERATURE REVIEW

Cyber Security Risks and Solutions

Since the end of the 20th century cyber online transactions has become integral part of our life. As cyber usage becomes more and more prominent, amongst individuals with different levels of knowledge of