Chapter 6
Cyber Security Competency Model Based on Learning Theories and Learning Continuum Hierarchy

Winfred Yaokumah
Pentecost University College, Ghana

ABSTRACT

There is an urgent need for transformative changes in cyber security awareness and training programs to produce individuals and the workforce that can deal with business risks emanating from the prevailing and emerging cyber-attacks. This chapter proposes a cyber security competency model that integrates learning theories (cognitive, affective, and psychomotor), learning continuum hierarchy (awareness and training), and cyber security domain knowledge. Employing literature search of scholarly and practitioner works, together with cyber security standards from governmental and non-governmental organizations, the chapter integrates cyber security domain knowledge, learning theories, and learning continuum hierarchy to design a model of cyber security competencies suitable for use in educating individuals and the general workforce. This theoretical-based approach to designing cyber security awareness and training programs will produce skillful individuals and workforce that can mitigate cyber-attacks in the global business environment.

INTRODUCTION

Cyber security is a global concern owing to the increasing reliance on the Internet (Dahbur, Bashabsheh, & Bashabsheh, 2017). It is one of the most serious economic and national security challenges faced by governments (Moskal, 2015), developed and developing nations (Stoddart, 2016), and public and the private businesses (Gunzel, 2017). National and international businesses are at risk as the Internet facilitates both business transactions and cyber-attacks across geographical boundaries. Cyber threats come from numerous sources, including hostile governments, terrorist groups, disgruntled employees, and malicious intruders (Nunez, 2017). The attacks can range from stealing of employees' personal infor-

DOI: 10.4018/978-1-5225-5927-6.ch006

mation (Office of Personnel Management, 2015) to attacks on critical infrastructure such as derailment of passenger trains, contamination of water supplies, and shutting down of power grid (Palmer, 2014).

Dealing with cybercrime becomes necessary because of the high cost of cybercrime on the societies, governments, and individuals (Wiederhold, 2014). For instance, the loss of revenue due to cyber attacks is estimated at US$240,000 per day among business organizations and can be more than US$100,000 per hour for retailers (Hui, Kim, & Wang, 2017; Neustar 2012). The Center for Strategic and International Studies estimates that an average annual cost of cybercrime to the global economy is $400 billion (McAfee, 2014); whereas Eubanks (2017) predicts that an average approximate cost of cybercrime will reach US$6 trillion by 2021.

Cyber threats pose danger to national security, financial security, and undermine individuals' privacy. Cyber security has become a top national priority (Proclamation 9508, 2016). It is an important institutional and community responsibility that requires an effective partnership between institutions and the entire community (Oblinger, 2015), including individuals and the general workforce. Thus, to effectively deal with cyber attacks, action is needed at national and global levels requiring individuals, society, and private businesses to better understand and to deal with cyber threats (Stoddart, 2016). The workforce and individuals need competencies and skills, including behavioural, management, and technical expertise to handle cyber attacks in the dynamic cyber threats environment (Singapore Increases Cyber security Training for Youths, 2014).

However, there seems to be a problem of inadequate knowledge and skill among individuals and the general workforce as to how to appropriately maintain cyber safety and respond to cyber attacks. Individuals and the current workforce apparently lack how to effectively apply cyber security measures. According to Russell (2017), public awareness of cyber threats is growing. However, evidence suggests that there are rapid increases in cyber related crimes in the recent years. For example, Global Economic Crime Survey records a high rise of cybercrime from 4th to 2nd position on the global economic crimes list (Global Economic Crime Survey, 2016).

Therefore, there is an urgent need for transformative changes in the current cyber security education to produce individuals and workforce to deal with business risks emanating from the prevailing and emerging cyber attacks. These changes are necessary because of the multifaceted nature of cyber security, the scope of cyber attacks and activities, and the targets of cyber attacks (businesses, government, individual users, and ICT service providers).

Cyber security awareness and training underpinned by relevant learning theories are needed for individuals in the society and the workforce to produce people that are capable of mitigating the current and future cyber attacks (Moskal, 2015). Thus, there will be improvement in cyber security if the individuals and the workforce are aware and properly trained to apply necessary safeguards to deal with issues related to digital privacy and security (Rohrer & Hom, 2017).

The purpose of this chapter is to propose a Cyber Security Competency Model for the current workforce and individuals aimed at developing cyber security knowledge and skills needed to address current global cyber security labor shortage (ITU, 2017). The study includes adding learning theories to cyber security body of knowledge and the learning continuum hierarchy (awareness and training) to support cyber security instructional design and development activities. Efforts at strengthening cyber defences warrant a solid theoretical research foundation (Ortiz & Reinerman-Jones, 2015). However, too often, theory and practice are separated from one another in training programs (ACM, 2014). A cyber security domain knowledge that is underpinned by learning theories (Bloom, 1956; Krathwohl, Bloom, & Masia, 1973; Simpson, 1972), mapped to learning continuum hierarchy will have greater impact. The proposed