Chapter 82
Cyber Security Education in the Fourth Industrial Revolution: The Case of South Africa

Paul Kariuki
University of KwaZulu Natal, South Africa

ABSTRACT

It is critical that cyber education curriculum considers the growing cyber technologies and which aspects of these technologies need to be aligned with the fourth industrial revolution. This chapter seeks to present a comprehensive analysis of the current level of cyber security education in South Africa. It will also track the current trends of cyber security education in the country as well as examining any challenges being experienced including any knowledge gaps. In the end, the chapter proposes recommendations for consideration in strengthening cybersecurity education in the country in to achieve advanced cyber security responses, capable of mitigating any cyber security threats. Offering quality cyber security education is important in preparing the next generation cyber security practitioners, who are highly competent and capable of developing innovative solutions in response to the growing global demand of cyber technologies. The chapter ends by proposing specific strategies that can guide towards this ideal in the context of the fourth industrial revolution.

INTRODUCTION

Individual and national security has been a priority since time immemorial. Evidence shows that information technology has played a positive and negative role in this regard. While the development of technology linked to the internet and other means of communication has ushered in a new way of life and transformed all economic sectors, it also provides a space for cyber and related crimes.

Growing use of the internet and related communication tools has raised the need to respond effectively to pervasive threats within state governance institutions, the transformation of goods, and security of borders and critical infrastructure. Research and policies are required to ensure that cyber-crime does not adversely affect citizens' development and well-being. There is growing demand for cyber security experts

DOI: 10.4018/978-1-5225-8897-9.ch082

to provide education on the unforeseen events that unfold due to information technology facilities around the world. Expert skills (Morgan, 2016) are required to ensure that devices are secure, prevent intruders from taking control of intellectual property, and alleviate and neutralise hacking, malware, viruses, etc.

However, globally, there is a dearth of experts in this field (Evans & Reeder, 2010). This calls for cyber security education curricula to be strengthened. While state institutions and businesses have made much progress in counter-balancing the threats and real effects of terrorists and cyber criminals, many challenges remain.

This chapter consists of four sections. The first examines trends and challenges relating to the cyber security curriculum. Section two highlights mitigation strategies that could be adopted to fight cyber-crime as well as their consequences for society. Section three addresses the policy implications for the government, educational institutions and cyber security professionals. Finally, section four focuses on the common responsibility of improving cyber education technologies in the fourth industrial revolution. The chapter ends with a conclusion.

THE CYBER SECURITY CURRICULUM IN SOUTH AFRICA: CURRENT TRENDS AND CHALLENGES

Cyber security education has gained traction in recent decades in South Africa. According to Dlamini (2012:5), it has been geared towards rebuilding the skills of practicing cyber security experts whilst at the same time increasing general awareness of such issues. Table 1 lists recent cyber security awareness initiatives in the country.

Thus, cyber security education in South Africa is geared towards raising awareness at all levels of society, focusing on diverse aspects.

Cyber security has been recognised as a national security issue in South Africa and the policy framework dates back to 2009. Grobler, van Vuuren, and Leenen (2012, p. 2) note that the 2011 draft policy framework set the stage for the launch of a Computer Security Incident Response Team (CSRIT) and the sector Computer Security Emergency Response Team (CSERT) by the end of 2012. The government has acknowledged the importance of cyber security and has invested in cyber security programmes and education (Conklin, Cline, & Roosa, 2014).

The literature notes the need for accreditation of institutions that offer cyber security education. This occurs in the United States (US), it is employed to ensure consistent quality. However, the most important aspect of accreditation is regulating the types of programmes offered to students. The common standard in the US is the IS 2010 Curriculum standard programme (Topi et al., 2010).

The IS 2010 curriculum covers different undergraduate programmes and offers the following seven modules: (1) IS 2010: Foundations of Information Systems; (2) IS 2010: Data and Information Management; (3) IS 2010 Enterprise Architecture; (4) IS 2010 IS Project Management; (5) IS 2010: IT Infrastructure; (6) IS 2010: Systems Analysis and Design; and (7) IS 2010 IS: Strategy, Management, and Acquisition (Conklin et al., 2014). In terms of supervision, the modules should be e-instinctive, student-friendly and methodically organised to facilitate knowledge acquisition.

Research suggests that students should be initiated on the use of codes in Information Technology. Some universities have expanded teaching of the theory and practice of secure coding to cover subjects such as Programming Secure Systems (Johnstone, 2013, p. 287).