Chapter 5
Developing the Social, Political, Economic, and Criminological Awareness of Cybersecurity Experts:
A Proposal and Discussion of Non-Technical Topics for Inclusion in Cybersecurity Education

Marcus Leaning
University of Winchester, UK

Udo Richard Averweg
eThekwini Municipality, South Africa

ABSTRACT

The global shortage in skilled labor for cybersecurity and the risk it presents to international business can only be solved by a significant increase in the number of skilled personnel. However, as the nature of risks proliferate and bifurcate the training of such, personnel must incorporate a broader understanding of contemporary and future risks. That is, while technical training is highly important, it is contended that future cybersecurity experts need to be aware of social, political, economic, and criminological issues. Towards this end, this chapter considers a number of exemplary issues that are considered worthy of inclusion in the development of future cybersecurity workers. Accordingly, an overview is given of the issues of the "dark side of the net" that cause problems for global cybersecurity and international business risk. The issues are discussed so that from these a skill set can be articulated which will attend to (and mitigate against) potential threats.

DOI: 10.4018/978-1-5225-5927-6.ch005

INTRODUCTION

The global shortage of skilled Information technology (IT) security staff presents a significant problem to business. Without qualified and skilled staff, ever increasing cybersecurity threats will make businesses untenable (Evans & Reeder, 2010). However, as explored in this collection there is currently a significant shortage of such qualified and skilled staff. This chapter is concerned with the education and training of such staff. However, despite a number of attempts (Hansche, 2006; Paulsen, McDuffie, Newhouse & Toth, 2012; Vinnakota, 2013; Kim, 2014; Beuran, Chinen, Tan, & Shinoda, 2016) definitions of what constitutes a trained IT security specialist are fairly fluid.

As Martin (2015) notes, there is not as yet a widely accepted structure or framework of skills. Indeed, there is a discrepancy between what different national governments and providers of education see as key areas of such an education (Henry, 2017). For the most part, staff and students willing to gain entry to the lucrative IT security workforce can choose from a very wide and heterogeneous educational market. Courses on offer tend to center upon two main approaches: first are courses that offer training at various levels in specific technological practices to detect and protect organizations from cyber-attacks.

Such training programs range from short upskilling in specific technologies through to full bachelors and masters level degrees in universities. Many of these courses, particularly at the sub-degree level, are accredited by brand leaders in the cybersecurity industry. Second are business and management courses which incorporate a component of cybersecurity. Such programs tend to seek to accord cybersecurity a significant role in management practices and advance the idea that individuals at all levels of an organization have a vital role to play in ensuring there is a robust defense to those wishing to attack it.

In this chapter, the authors contend that cybersecurity training has to-date neglected a significant aspect in its scope. Drawing upon ideas from cultural criminology it is asserted that those charged with defending against cyber threats should be cognoscente of a range of non-technical issues which relate to the reasons for attack. Also included are the wider social and cultural aspects of attacks such as the culture of those attacking understanding the political, economic and psychological motivations of attackers, the economics of the attacker's culture and the cultural norms of the attackers. Cultural criminologists have asserted that through such awareness those involved in defending an organization from external threats can better predict and mitigate future threats (Ferrell & Sanders, 1995; Jaishankar, 2011).

To address such issues, the authors assert that cybersecurity should incorporate a range of topics and issues currently outside of the accepted scope of training. Determining the scope of such topics and issues is problematic and the list of such areas will need to be continually revised as new aspects emerge and new social issues arise. Indeed, ensuring that cybersecurity personnel are as aware of contemporary social issues in security is as difficult as ensuring the technical skills are up-to-date. Mindful of this, the authors here identify four key areas in this chapter that will serve the contemporary and immediate future needs of cybersecurity personnel.

The objective of this chapter is to advance an outline of four areas the authors feel cybersecurity personnel need to consider: (1) the rationale for spam emails; (2) the reasons people hack; (3) the new economy of crypto currencies; and (4) the places of communication used by cyber criminals.