Chapter 19
Toward a Model for Ethical Cybersecurity Leadership

Marisa Cleveland
Northeastern University, Boston, USA

Tonia Spangler
Florida SouthWestern State College, Fort Myers, USA

ABSTRACT

With no clear model for ethical cybersecurity leadership, the field of cybersecurity is largely unregulated. The advances in technology and the Internet of Things come at a price—security. Since there is a lack of regulation, no clear guidelines exist. Furthermore, there is a gap in the literature to identify a set of global ethical standards for cybersecurity leaders. This article proposes an international model of ethical standards with three ethical propositions to ensure the users of technology in today's global industry remain confident in the corporations entrusted with the users' information.

INTRODUCTION

Ethics within the field of cybersecurity must be examined from an international angle, given today's digital marketplace and global economy. Cybersecurity leaders have access to confidential information about individuals and companies, but unlike the medical profession, no standard of ethics exists for IT professionals (Schinder, 2005). The advanced technology came at a price – security. Since personal computers emerged in the 1980s, along with the Internet of Things, viruses and malware also surfaced. Data breaches continue to increase in frequency and magnitude, with Yahoo!, MySpace, Under Armour, and Equifax listed as the largest reported breaches affecting 3 billion, 360 million, 150 million, and 145 million accordingly (Weise, 2017). Most people believe in their right to privacy, but as governments continue to use technology for surveillance and as corporations fail to proactively search for more secure practices, the actions that occur within the cybersecurity field need to include an examination of the ethical implications of ignoring the risks (Cleveland & Cleveland, 2018a).

DOI: 10.4018/978-1-7998-2466-4.ch019

While vulnerabilities will never completely disappear, good leaders should address cybersecurity with a cross-functional, multidisciplinary approach. Leaders of cybersecurity teams should institute ethically sound best practices. According to Newmeyer (2012), "In 2007, several Cabinet Departments including Defense, Homeland Security, and Commerce were hacked and terabytes of information were exfiltrated by unknown agents." With no clear model for ethical cybersecurity leadership, and without a centralization of cybersecurity policy initiatives, the field of cybersecurity is largely unregulated. The Information Systems Security Association (ISSA) established a Code of Ethics, but to date, there is not one centralized and recognized legal regulating agency.

Since there is a lack of regulation, the problem is that there are no clear guidelines. Also, there is a gap in the literature to identify a set of ethical standards for cybersecurity leaders. With conflicting opinions on how to best handle cyber breaches in today's multicultural, digital environment, how should cybersecurity leaders best address ethical cybersecurity considerations through the lens of an international standard?

This paper provides an initial examination of the importance of ethics for cybersecurity leaders and the ethical considerations within the field of cybersecurity by proposing a basic ethics model that, when applied to cybersecurity leadership, will safeguard cybersecurity social justice. By doing so, this paper will add to the conversation of how ethical standards could be considered when dealing with cybersecurity professionals to ensure the users of technology in today's global industry remain confident in the corporations entrusted with the users' information.

IMPORTANCE OF ETHICS FOR CYBERSECURITY LEADERS

Cybersecurity leaders create the standard for ethical behavior across entire organizations, industries, and continents. Since the 1990s, trust in businesses and the integrity of business people has declined (Barker & Comer, 2012). Ethical leadership and ethical decision making are important components of business instruction and recognized as such by The Association to Advance Collegiate Schools of Business International (AACSB) (Baker & Comer, 2012). According to Gerde and Foster (2008) and Tomlinson (2009), students are taught how to identify ethical issues and how to make ethical decisions, but Dean and Beggs (2006) posit that teaching business ethics has a "negligible effect of their students' behavior" (Baker & Comer, 2012).

Beyond business ethics, information security professionals are expected to uphold a standard of practice that promotes trust from the users and assurance that the information they maintain will be used for the comprehended intended purpose. According to Bandura's Social Learning Theory, people learn from one another (Bandura, 1977), and in Kotter and Cohen (2002), one of the authors notes that after examining close to 100 cases, one finding was that most people "did not handle large-scale change well… mostly because they had little exposure to highly successful transformations."

If integrity and work ethic are traits of effective leaders (Schafer, 2010), and "mentoring is a form of leadership" (Burke, 2017), then cybersecurity leaders have the responsibility to not only model ethical behavior, but also mentor the cybersecurity professionals entering the information security industry. Bhattacharya (2011) concluded in a research study that vulnerabilities increase when leadership lacks concern toward information security problems.