Chapter 17
A Technoethical Study of Ethical Hacking Communication and Management Within a Canadian University

Baha Abu-Shaqra
University of Ottawa, Canada

Rocci Luppicini
Universisty of Ottawa, Canada

ABSTRACT

Ethical hacking is an important information security risk management strategy within higher education applied against the growing threat of hacking attacks. Confusion regarding the meaning and ethics of ethical hacking within broader society and which resonates within organizations undermines information security. Confusion within organizations increases unpredictably (equivocality) in the information environment, which raises risk level. Taking a qualitative exploratory case study approach, this chapter pairs technoethical inquiry theory with Karl Weick's sensemaking model to explore the meanings, ethics, uses and practices, and value of ethical hacking in a Canadian university and applies technoethical inquiry decision-making grid (TEI-DMG) as an ethical decision-making model. Findings point to the need to expand the communicative and sociocultural considerations involved in decision making about ethical hacking organizational practices, and to security awareness training to leverage sensemaking opportunities and reduce equivocality in the information environment.

INTRODUCTION

Universities and other higher education institutions represent a tempting target for hackers and are under an increasing risk of hacking attacks. Educational institutions maintain databases of personal information about faculty, staff, and students. Such databases represent a tempting target for cybercriminals who sell stolen personal information on the black market to other criminals for profit (Burrell, n.d.). Cybercrimi-

DOI: 10.4018/978-1-5225-5094-5.ch017

nals may be looking to steal university research. Ethical hacking is an important information security risk management strategy higher education institutions and businesses use against the growing threat of hacking attacks. Implementation challenges within an organization intersect several perspectives within the broader societal/industry context--social/sociocultural, ethical, and technical/technological perspectives. There is confusion (among other challenges) surrounding ethical hacking meaning and ethics within society and which resonates within societal organizations with costs to society. Confusion within organizations increases unpredictably (equivocality) in the information environment which negatively affects information security—it raises hacking risk. Confusion among the general public can manifest in a stigma that can hurt businesses. Confusion undermines innovation and effective policy development.

A social/sociocultural perspective is concerned with a broad question, what is ethical hacking? A key cause of confusion regarding ethical hacking meaning and ethics within society results from a difference in language use (application of the term ethical hacking) between and among engineers and technologists, and non-technologists. This difference can manifest in two ways. First, hacking as a contronym resulting from a tension between two contradictory stakeholder perspectives--hacking as having a positive connotation among engineers and technologists in contrast to the more popular understanding of hacking as being a malicious activity. Second, the terms white, grey, and black hackers and hacking can refer to a type of information security testing or to sociocultural codes. An ethical perspective focuses on fair and efficient (effective) technology implementation--including, whether it should be used or not, and how to implement it effectively so that organizations are protected and the public is served. A technical/technological perspective includes account for broad industry trends, and addresses aspects of hacking technology proliferation and the changing technological landscape of cybersecurity, as well as broader concerns related to problems within the information security management field, such as the metrics problem, the lack of broad industry information security standards, and software interoperability challenges. Importantly, organizational challenges resonating form broader societal practices—notably, confusion regarding ethical hacking meaning and ethics among various stakeholder groups extends into organizations which undermines organizational information security.

Most information security management books on ethical hacking focused on its technical application in information security risk assessment practices. The broader societal context of ethical hacking implementation was less considered. Non-technical challenges involved in the implementation of ethical hacking within higher education organizations intersect several perspectives. The study focused on effective ethical hacking implementation in an higher education organization understood within the broader societal/industry context—within the ethical, social/sociocultural, and technical/technological context. The study explored the research question, What are the meanings, ethics, uses and practices, and value of ethical hacking in a Canadian university? by applying technoethical inquiry theory (Luppicini, 2008A, 2008B, 2010) and Karl Weick's (1969, 1979, 1995) sensemaking model to a case study. This paper addressed a gap within the information security management literature on ethical hacking. The important contribution to knowledge of this study lies in filling in a gap in the literature on information security management that results from the scarcity of research on the communicative and sociocultural considerations involved in the implementation of ethical hacking within organizations, focusing on non-technical aspects, while the dominant scholarship is application and certification oriented focusing on technical and legal aspects.

Technoethical inquiry theory (TEI) is a pragmatic systems theory that highlights knowledge gathering from multiple perspectives, including ethical, technological, political, legal, historical, communicative, and sociocultural (Luppicini, 2010). The goal of TEI is to uncover information related to the efficiency

Related Content