Chapter 82
The Cyberethics, Cybersafety, and Cybersecurity at Schools

Irene L. Chen
University of Houston Downtown, Houston, USA

Libi Shen
University of Phoenix, Los Angeles, USA

ABSTRACT

The 2006 Megan Meier case, where a teenage girl who was bullied on the Internet through e-mail and Myspace which was said to ultimately lead to her suicide, shed light on the cyber bullying issue in schools. This article uses a case study approach to describe how a number of school institutes were grappling with the loss of confidential information and protecting students on the WWW, each through a unique set of circumstances. It will reveal potential reactions of the institutions and possible ways to deal with the cyber threats. With experiences, school districts take measures to offer value education by improving students' knowledge and awareness of Cyberethics, Cybersafety, and Cybersecurity (C3) concepts to provide them with the means to protect themselves, and to enhance the safety and security of national infrastructure.

INTRODUCTION

Cybersecurity has been a critical issue for schools in recent years. According to *Data Breach Reports* (2014), there were 783 data breaches with 85,611,528 records exposed in the categories of banking/credit/financial, business, education, government/military, and medical/healthcare. Among them, 57 (7.3%) breaches are educational with 1,247,812 records exposed (Data Breach Reports, 2014). In 2015, there were 690 data breaches with 176,183,204 records exposed in the categories of banking/ credit/financial, business, education, government/ military, and medical/healthcare (Data Breach Reports, 2015). Among them, 53 (7.7%) breaches were educational with 759,600 records exposed (Data Breach Reports, 2015). Both universities and public schools were involved.

DOI: 10.4018/978-1-7998-2466-4.ch082

Data breach problem is serious and worldwide. Khandelwal (2016) stated that 50 million Turkish citizens' personal data were leaked online. The leaked database contained 49,611,709 records with the following information: first and last names, national ID numbers, gender, city of birth, data of birth, full address, ID registration city, and user's mother's/father's first names. This data breach included personal detailed information of Turkish president Recep Tayyip Erdogan, his predecessor Abdullah Gul, and Prime Minister Ahmet Davutoglu.

Additionally, approximately 62% IT managers cited security threats from malware as the chief reason not to use unlicensed or mis-licensed applications. Based on the Business Software Alliance, unlicensed software use continued to be a major problem in 2013 in which 43% of the software installed on personal computers around the world was not properly licensed. The commercial value of the unlicensed installations was $62.7 billion (BSA, 2014). It is of great importance to examine cyberethics, cybersafety, and cybersecurity (C3) at schools to avoid more threats and damages.

CYBERETHICS, CYBERSAFETY, AND CYBERSECURITY

Pruitt-Mentle (2000) is credited for coining the concepts of C3 Matrix: cybersafety, cybersecurity, and cyberethics. She was one of the pioneers who promoted the integration of C3 across K-12 curriculum through organizations such as iKeepSafe. According to C3Matrix, cybersafety is "the ability to act in a safe and responsible manner on the Internet and other connected environments"; cybersecurity "covers physical protection (both hardware and software) of personal information and technology resources from unauthorized access gained via technological means"; cyberethics is "the discipline of using appropriate and ethical behaviors and acknowledging moral duties and obligations pertaining to online environments and digital media" (C3Matrix, 2015, p. 2). The three concepts of cybersafety, cybersecurity, and cyberethics are tightly integrated and ever changing.

Cyberethics is "the philosophical study of ethics pertaining to computer networks encompassing users' behavior, what networked computers are programmed to do, and how this affects the individuals and the society" (Mosalanejad, Dehghani, & Abdolahifard, 2014, p. 205). DeWitt-Heffner (2001) has raised three issues regarding to ethical dilemmas in cyberspace: intellectual property, privacy/security and free speech/hate speech. She emphasized that "both students and teachers question when it is appropriate to transfer our understanding of ethical behavior form the classroom to the online environment" regardless of the particular issue under discussion (DeWitt-Heffner, 2001, p. 101). Further, DeWitt-Heffner (2001) identified four major themes for ethical decision-making: (1) "the cyberethics authority recognized by students is much younger than the offline ethical authority" (p. 102); (2) "students of different ages use different mental frameworks to decide online behavior" (p. 103); (3) "when considering appropriate and inappropriate behavior online, some issues are clear for both teachers and students, however many others are not" (p.103); and (4) "educators can encourage ethical behavior by recognizing the type of situations that make unethical behavior attractive and challenging students to channel their technological expertise in positive directions" (p.104).

Pusey and Sadera (2012, p. 82) indicated that "cyberethics are the moral choices individuals make when using Internet-capable technologies and digital media" which include copyright, online etiquette, hacking, and online addictions. They conducted a survey to explore 318 preservice teachers' knowledge and ability to teach C3 topics/contents, and found that teachers were not prepared to model or teach these concepts (Pusey & Sadera, 2012). In other words, although those teachers are digital natives, they