Chapter 105
Law and Technology at Crossroads in Cyberspace: Where Do We Go From Here?

Anteneh Ayanso
Brock University, Canada

Tejaswini Herath
Brock University, Canada

ABSTRACT

Historical incidents have taught organizations several key lessons on computer crimes. The complexity of the current technology environment dictates that no one mechanism can effectively address computer crimes. Investing in the most sophisticated counter-technologies alone is not enough to fight cyber threats. Thus it has become increasingly important for organizations and governments to establish control frameworks that incorporate proactive measures in the technological, legislative, and administrative dimensions. While it is government's role to keep up with the legislative rules, organizations need to have the right security policies and guidelines in place as well as develop awareness in the legal front to combat computer crimes. With the review of the academic literature, industry reports, and the media, this chapter identifies various kinds of computer crimes and discusses the counter strategies to tackle such crimes in the legal, technological, and organizational dimensions.

INTRODUCTION

Computer crime has evolved to be a serious problem that deserves attention. The Internet enabled environment facilitates many flexible work opportunities for employees allowing them to work away from their desks. Telecommuting, working from home, remote computing while travelling is becoming common occurrence in many organizations. Thus organizations are subjected to a wide range of computer crimes through their personnel that are directed towards organizations as well as public mass in general. Employees as well as managers need to be aware of these issues and have a clear understanding of the various types of cyber threats in the current environment and how they could be controlled.

DOI: 10.4018/978-1-4666-5942-1.ch105

Computer crime varies significantly from one context to another depending on what scope (individual, organization, or society) it focuses on or even which country it refers to. Today, the Internet influences every activity of our life. As the number of transactional, communicative and distributional aspects of our lives goes online, higher is our vulnerability to cybercrime. The kind of crimes that are committed in the cyberspace are several and diverse, capable of causing serious damages to both person and property ranging from reputational harm, privacy violations, cyber stalking to intellectual property violations, economic fraud and security breaches, to name only a few. Worst still, detecting the cyber criminal in the online environment is subject to technological sophistication and knowledge which not all law enforcement agencies have the capacity to do. With the multitude of advantages that the Internet brings with it, this represents the darker side of this marvelous technology.

The evolution of the Internet to the current state of social media further complicates the ethical and legal conundrums that arise in various settings. The issue with WikiLeaks exemplifies how far the Internet can expose the world and the complexity of the social, ethical and legal debates that arise. For example, how do we maintain a balance between the right to information and the right to privacy? How much does copyright as an intellectual property right have a meaning in the current social media environment? Where does one draw the line between free speech and online defamation given that Internet allows one to reach a mass audience with little or no cost and almost anonymously? Thus, technology and law have a very complex relationship. Law attempts to closely observe the ways and means by which technology can be used to achieve unethical ends and outlaws the same by codifying such practice. However, technology moves at too fast a pace that the legal statutes cannot always catch up to it in time. New genre of crimes is being discovered on the Internet and accordingly we have to update our statutes and develop alternative mechanisms to overcome these threats. The list of cybercrimes is also in a nascent stage and continues to evolve as the bridge between our physical world and cyber world shrinks at an increasingly rapid pace. Thus, the challenge for managers today is to monitor progress and update the measures in all angles – technological, organizational, and legal. This chapter attempts to contribute towards this direction and provides an overview of computer crimes, examines the possible impacts of computer crimes at various contexts, and discusses alternative control mechanisms.

COMPUTER CRIME: AN OVERVIEW

The term computer crime has been given several labels, such as cybercrime, e-crime, hi-tech crime, electronic crime, etc. Today there are a variety of computer crimes at different scopes and contexts, and there is a lack of standardized classifications or definitions for many of the activities that could be considered illegal. Computer crime brings tremendous harm to both the public and organizations. For individuals, computer crimes can attack privacy, identity, and personal property. For the public and government, computer crimes can destroy infrastructure and administrative systems and can threaten national security.

Definition

Given the complexity and diversity of computer crimes in the current environment, no definition can comprehensively describe it (Gordon & Ford, 2006; Goodman, 2010). Gordon and Ford (2006) define computer crime as "any crime that is facilitated or committed using a computer, network, or hardware device."

According to the U.S. Department of Justice (DOJ), computer crime is defined as "any violations of criminal law that involve knowledge of computer technology for their perpetration, investigation, or prosecution" (Volonino & Robinson, 2004, p. 155).