Book Review of Understanding and Managing Cybercrime[1]

Robert M. Slade[2]
Data communications and security specialist, Canada

Understanding and Managing Cybercrime, (2006) Samuel C. McQuade, Allyn and Bacon (Pearson), 512 pp, ISBN-10: 020543973X, ISBN-13: 978-0205439737.

The preface states that this book should be considered an introductory text to the field of cybercrime (although it does not define what that topic is until chapter one of the book). The guide is addressed to two audiences of students, those in the field of information technology administration and management, and those in the field of criminology. McQuade suggests that the work can be used as a primer in basic courses expounding on information systems security, and may also be used as a supporting volume for curricula in sociology, law, public administration, public policy, or ethics courses that deal with information system crime and abuse. In the Foreword, Charles Wellford notes the increase in significance of crimes related to, or perpetrated via the use of, computers. Whereas crime statistics of traditional types have been falling in recent years, cybercrime has exploded in an environment where traditional law enforcement has been largely unprepared.

Part one introduces the field, and outlines the growth, of cybercrime. Chapter one starts out with a valuable addition to the discussion of the sociology of cybercrime: the concept of "relative" normality and deviance of behaviour in a new and rapidly changing field. The author then moves on to note the range of terms and activities covered under the cybercrime reference, and to note the importance of defining those terms not only in regard to research, but particularly in relation to law and prosecution. The questions provided at the end of the chapter are not simply reading checks, but thoughtful items to prompt discussion of critical concepts. The protection of information and other assets is covered in chapter two, starting with the nature of information itself, moving through the standard concepts of information security, and ending up with critical infrastructure protection (which may be a bit of overkill). Chapter three reviews the various types of cyber attacks and crimes. I was intrigued to note the inclusion of a section on academic computer abuses (generally a neglected topic), and pleased with the realistic assessment of cyberterrorism, but the structure and taxonomy of attacks could use some work. In addition, the material on malware is quite weak: the definitions for differing types are

[1] © Robert M. Slade. Reprinted with permission from Robert M. Slade. Earlier published in The Risks Digest: Forum on Risks to the Public in Computers and Related Systems, Volume 24: Issue 50 Friday 15 December 2006. Available at http://catless.ncl.ac.uk/Risks/24.50.html

[2] Data communications and security specialist, North Vancouver, British Columbia, Canada. Email: rslade@computercrime.org

better than many in general security works, but many of the surrounding explanations are false or misleading. For example, McQuade partially uses the Cohenesque definition that viruses must infect existing programs (which is no longer true of recent versions), and implies that a user is required for viral reproduction and spread (viruses generally require some user action for invocation, but spread is usually automated). Additionally, he makes the rather questionable assertion that the skills necessary for creating malware are the same as those required to defend national security. The psychology of cybercriminals and abusers is reviewed in chapter four, which also provides a very detailed classification for social engineering, and Donn Parker's SKRAM (skill, knowledge, resources, access, motivation) model for assessing attackers. McQuade notes the difficulty in getting agreement on a profile for computer abusers, but does not address the changing style of attacks and attackers over time.

It is interesting that chapter four is not contained within part two, which addresses social thought on cybercrime. Chapter five, in a sense, extends chapter four's discussion of categories of criminals by providing an overview of major criminologic theories: it would have been interesting to see the classification schema analyzed in light of the hypotheses, but simply having the philosophies outlined here is a major contribution to the information security literature. In assessing the impact of cybercrime, in chapter six, McQuade notes that there is both economic and social damage to be determined. However, this merely exacerbates an existing problem: the author also points out the lack of reliable information, even in regard to economic losses alone. It is difficult to know what to make of chapter seven. Titularly it promises emerging and controversial topics in cybercrime. However, the discussion of the necessity for attack skills in regard to defence (promised in chapter three) never appears. The topics that are presented would seem to extend either the first section of chapter one (noting that computers are changing various activities in society), or chapter three (listing different types of attacks).

Part three moves to the management of cybercrime: prevention and protection. Although chapter eight deals with legal philosophies and types of laws, most of the material is only relevant to the United States. The limitation on investigators, which is the primary content of chapter nine, is again mostly restricted to the United States. There is material on investigation and computer forensics (although network and software forensics do not appear to be covered), but it is fairly brief. Chapter ten's review of information security is oddly disjointed: parts are academic in tone, parts read like a "secure your home computer" pamphlet, and parts promote risk assessment models best suited to major corporations. Future activities (mostly at the federal government level) that might help reduce cybercrime is one part of chapter eleven, the other is a discussion of computer ethics.

The book is readable and entertaining in sections. Most of the information is reasonable. However, suggesting this as a sole text for an information security course would be unwise: it is weak in a number of technical areas. As an adjunct text it would be excellent: the law enforcement perspective is all too often neglected in security literature.