One of the perks of being a columnist is that publishers send you free books in the hope that you will review them. One of these over-the-transom contributions to my library is an interesting collection of scholarly articles on white-collar crime that will be helpful to network and security managers looking for interesting case studies and ideas for their security-awareness courses [1].

The editors begin with an interesting preface that points out (among other things) that white-collar crime has been associated with political corruption and organized crime as well as individual larceny. They continue their interesting commentary in the introductions to each of the three parts of the book:

I. Defining White-Collar Crime
II. Forms of White-Collar Crime
III. The Criminal Justice System and White-Collar Crime.

Gilbert Geis introduces the thorny question of precisely what qualifies as white-collar crime.[2] The term was established by the famed criminologist Edwin H. Sutherland, who used it “in 1939 during his presidential address to the American sociological society in Philadelphia.” Early users of the term applied it to occupational crimes committed by people of high social status. In areas other than the United States, however, most people referred to “economic crimes” or to “abuse of power.” In the 1970s, sociologists and criminologists revived debates over the specific meaning of the term. Some argued for a very broad definition that included all kinds of economic crimes including frauds perpetrated on gullible victims (confidence games); a defining characteristic in this view was the lack of overt physical violence in the methods used. Others suggested that one should distinguish between individual white-collar crimes and corporate crime such as price-fixing or concealment of negative scientific results in regulatory processes.

Maria S. Boss and Barbara Crutchfield George review some of the US laws and jurisprudence governing white-collar crime.[3] Their section on the work environment is particularly applicable to network and security managers; I like their comment, “If whistleblowers are protected within the organization and or rewarded for their conduct (i.e., encouraged by the employer), a white-collar worker contemplating a crime will be less likely to commit the crime for fear of disclosure by fellow workers. It is in the employer’s best interest to protect whistleblowers, thereby exerting positive control over the workplace.”

Elizabeth Moore and Michael Mills discuss the victims of white-collar crime and point out that little has been done by legislators to help compensate them for their losses.[4]

Garry Potter and Larry Gaines point out how the corporate climate can influence criminality.[5] Excessive emphasis on profit at the expense of ethics and elements of what I identify as groupthink such as extraordinary fear of failure and extreme emphasis on loyalty can push people into illegality. Lying about motivations and behavior (what the authors describe as creating “front activities”) can create a habit of dishonesty that fosters white-collar crime. Some businesses fall so far from normal standards that they effectively _become_ organized crime. The authors review the intimate involvement of business and organized crime in the 20th century and provide many interesting case studies including the savings and loan scandals and the Iran Contra affair.

Part II has chapters analyzing specific types of white-collar crime including

- embezzlement
- savings and loan fraud
- insider trading
- telemarketing fraud
- computer-related crime
- physician violence new crime healthcare fraud
- occupational health crimes
- the waste oil industry
- government sabotage of OSHA
- contractor fraud in NASA.

David Carter and Andra J. Bannister are the authors of the chapter on computer-related crime.[6] Having written similar overviews myself, I was impressed with the authors’ thoroughness and clarity.[7] I think their chapter provides an excellent introduction to the field of computer crime, especially for people with a limited background in computing (such as, perhaps, some of your own upper managers, Dear Readers). Conversely, their work can also serve to interest and motivate technical personnel with a limited exposure to the kinds of crime that involve computers.

Part III of the book will interest not only criminologists but also anyone interested in the long-term effects of laws and law enforcement on this kind of crime.

In summary, this text will be a valuable addition to the libraries of security professionals interested in the human side of computer crime, to corporate and college librarians as a resource for faculty and students, and especially to anyone teaching a course in economic crime.

My only regret is that the cover is not mauve; I would _so_ have liked to entitle this column, “The Collar Purple.”

* * *

References


* * *

A Master’s degree in the management of information assurance in 18 months of online study from Norwich University – see <http://www3.norwich.edu/msia> for details.

M. E. Kabay, PhD, CISSP is Associate Professor in the Division of Business and Management at Norwich University in Northfield, VT. Mich can be reached by e-mail at <mailto:mkabay@norwich.edu>; Web site at <http://www.mekabay.com/index.htm>.

Copyright © 2004 M. E. Kabay. All rights reserved.

Permission is hereby granted to _Network World_ to distribute this article at will, to post it without limit on any Web site, and to republish it in any way they see fit.