BOOK REVIEW

Mahesh K. Nalla,[1] *Ph.D.*

Review of: *Investigating Computer-Related Crime*

REFERENCE: Stephenson P. Investigating computer-related crime. CRC Press, Boca Raton, FL, 2000, pp. 1534.

In *Investigating Computer-Related Crime* Stephenson examines the nature and extent of cyber crime and its impact on business community. He identifies various investigative and computer forensic techniques, describes techniques for gathering and preserving evidence, and finally suggest ways to prepare to deal with the problem. While computer crime is a broader concept, Stephenson focuses on "cyber crime" to limit his investigation of crimes that occur in the context of "networked issues, especially including global networks such as the internet" (p. 3).

This book is divided into four sections, which are further divided into 19 chapters. Section 1 covers chapters that describe the nature of cyber crime, the impact of cyber crime on industry, various forms of viruses, worms, surgical strikes, and shotgun blasts. In Section 2, Stephenson deals with investigation of cyber crime. More specifically, he provides a framework for conducting a computer crime incident. He takes the reader through various steps of investigation including eliminating the obvious, reconstructing the crime, and performing a traceback to the suspected source computer. In this section Stephenson also describes the human aspects of computer crime, collection, and preservation of evidence, interview and interrogation of witnesses. Further, he devoted additional chapters on how to handle the crime in progress, when to involve authorities, and when to quit an investigation. Section 3, a relatively shorter section but provides a framework for corporations to develop proactive measures such as cyber SWAT teams. The author also dwells into ethical issues surrounding internal enforcement strategies with a chapter on privacy and computer crime. Section 4 is devoted to forensic utilities with chapters on preserving evidence, collecting evidence, searching for hidden information, and handling floppy disks. Finally, the two appendices on the Introduction to Denial of Service Attacks and Technical Report 540-96 provides valuable checklist for practitioners to help prepare for safeguarding proprietary information from cyber crime.

Overall, this book is a well-written book, particularly for introductory classes in computer crime for security management/social science students, security practitioners, and law enforcement officers. Among the numerous resources in recent years on the subject, I find this book very informative, resourceful, and easy to read.

[1] Professor, School of Criminal Justice, Michigan State University, Lansing, MI.