

Book Review

Electronic Crime

Peter Grabosky

Upper Saddle River, NJ, Pearson Prentice-Hall, 2007, 123pp., \$13.33

ISBN: 0131534610

Security Journal (2008) 21, 137–138. doi:10.1057/palgrave.sj.8350080

It is truly fitting that Prentice-Hall would select Peter Grabosky to write a book on computer crime for its Masters Series in Criminology. Grabosky has emerged as one of the leading academicians in the area of computer crime. Through his numerous publications on the subject, he has provided insight into the types of computer-related crime, methodologies used by criminals who commit computer crime, and solutions to prevent future offending. His work moves well beyond the investigative domain of the law enforcement community to recognize the roles of prosecutorial and corrections agencies in addressing computer crime.

Electronic Crime fills a void in the scholarly literature by offering a single introductory resource that addresses both the nature of and the criminal justice system's response to computer crime. Chapter One begins with a brief discussion of how computing and related networking technologies have changed our lives. Grabosky links this discussion to computer crime by calling attention to the capabilities computer technology afford society and how computers serve those with lawful and unlawful intentions. Chapter Two provides a brief history of computer crime. Here, Grabosky emphasizes new opportunities for crime based upon developments in computer technology. The differences between a hacker and a cracker are also explored, as is the evolution of computer crime legislation.

Chapter Three examines the relationship between computer technology and crime and lays out a typology of computer crime. Grabosky categorizes computer crime by differentiating between conventional crimes that are committed with computer technology (e.g. extortion, stalking, and the production, dissemination of child pornography) and new crimes that are committed with computer technology (e.g. website defacement, denial-of-service attacks, ATM fraud, dissemination of malicious code). Chapter Three also contains a glossary of technical terms that are commonly used in the computer crime literature.

Chapter Four lays out a theoretical framework to explain computer crime. Here, Grabosky uses routine activity theory as the basis for explaining why cybercrime occurs. He attributes the supply of both motivated offenders and suitable targets for victimization to an increasing Internet user population and familiarization with computer technology. Capable guardianship in cyberspace, as it pertains to routine activity theory, is discussed from the human (e.g. parents, employers, and system administrators) and technological (e.g. encryption, anti-virus, and intrusion detection programs) perspectives.

Chapter Five reviews past victimization research in an attempt to get at the prevalence and impact of computer crime. Grabosky calls attention to some of the methodological difficulties in estimating the prevalence of cybercrime and associated damages, including

an unwillingness of victims to report many types of cybercrime. Chapter Six examines recent trends in cyber crime in terms of criminal methodologies and offender characteristics. An increase in the sophistication of attack methodologies, the potential for financial reward, the involvement of juveniles, and the availability of encryption are, according to Grabosky, all challenges the criminal justice system are likely to face in its efforts to address computer crime.

Chapter Seven focuses on the criminal justice process as it pertains to computer crime. Grabosky, as do many others who have written on the topic, discusses computer crime investigations in terms of the search and seizure processes and issues surrounding the collection, preservation, analysis, and presentation of digital evidence. What differentiates *Electronic Crime* from many other publications that address the criminal justice system's response to computer crime is the discussion surrounding the prosecutorial and sentencing processes.

Chapter Eight puts forth crime prevention strategies to address computer crime. Preventive solutions are discussed in terms of the motivation, opportunity, and guardianship components of routine activity theory. The roles of private enforcement entities, cyber vigilantes, and criminal legislation in combating computer crime are also discussed. *Electronic Crime* concludes with an appendix of online resources pertaining to computer crime and a list of the works cited in the book. The appendix and reference list will prove extremely helpful to students and researchers looking for additional materials on computer crime.

In keeping with the theme of Prentice-Hall's Masters Series in Criminology, *Electronic Crime* is bound to peak the interest of readers who are exploring computer crime for the first time. College instructors looking to introduce students to the academic study of computer crime will be served well by using *Electronic Crime* in the classroom. Its length and subject matter make *Electronic Crime* the perfect companion-piece to introductory textbooks on criminology, criminal justice, and security. Grabosky does an excellent job of explaining the technical side of computer crime in a manner that is easily understood by the lay reader. Students without a formal background in computer science will, thus, not be at a disadvantage when reading this book.

Grabosky's inclusion of a theoretical framework to explain computer crime is a rarity when it comes to books on this subject. All too often, authors writing on computer crime rely solely upon war-stories from field investigations to win readers over. *Electronic Crime* does include many contextually rich stories describing real cases of computer crime. Grabosky, however, uses these stories in a systematic manner to advance our understanding of computer crime as an academic field of study rather than to merely provide yet another example of crime in the Information Age. *Electronic Crime* synthesizes theory and practice to offer readers a framework from which to categorize the types of computer crime, explain the behavior of offenders, and understand the challenges faced by the criminal justice system in dealing with this type of crime.

Rob D'Ovidio
Criminal Justice Program,
Department of Culture & Communication,
Drexel University, Philadelphia, VA, USA.