Preface

This book takes a novel approach to the presentation and understanding of a controversial topic in modern-day society: hacking. The term hacker was originally used to denote positively-motivated individuals wanting to stretch the capabilities of computers and networks. In contrast, the term cracker was a later version of the term, used to denote negatively-motivated individuals wanting to take advantage of computers and networks’ vulnerabilities to cause harm to property or persons, or to personally gain financially. Most of what the public knows about hackers comes from the media—who tend to emphasize the cracker side in many journalistic pieces. In the academic domain, content experts from computer science, criminology, or psychology are often called in to assess individuals caught and convicted of computer-related crimes—and their findings are sometimes published as case studies.

In an age when computer crime is growing at a exponential rate and on a global scale, industry and government leaders are crying out for answers from the academic and IT Security fields to keep cyber crime in check—and to, one day, be ahead of the “cyber criminal curve” rather than have to react to it. After all, the safety and security of nations’ critical infrastructures and their citizens are at risk, as are companies’ reputations and profitable futures. According to 2009 Computer Security Institute report, the average loss due to IT security incidents per company exceeds the $230,000 mark for the U.S., alone. Given the 2009 financial crisis worldwide, a looming fear among IT Security experts is that desperate times feed desperate crimes, including those in the virtual world—driving the cost factor for network breaches upward.

To answer this call for assistance, we approached content experts in Criminal Justice, Business, and Information Technology Security from around the world, asking them to share their current research undertakings and findings with us and our readers so that, together, we can begin to find interdisciplinary solutions to the complex domain of cyber crime and network breaches. In our invitation to potential authors, we said, “Your pieces, we hope, will focus on the analysis of various forms of attacks or technological solutions to identify and mitigate these problems, with a view to assisting industry and government agencies in mitigating present-day and future exploits.” Following a blind review of chapters submitted, we compiled the best and most exciting submissions in this book, entitled, Corporate Hacking and Technology-Driven Crime: Social Dynamics and Implications.

The chapters in this book are meant to address various aspects of corporate hacking and technology-driven crime, including the ability to:

Define and understand computer-based threats using empirical examinations of hacker activity and theoretical evaluations of their motives and beliefs.

Provide a thorough review of existing social science research on the hacker community and identify new avenues of scholarship in this area.
Identify and examine attack dynamics in network environments and on-line using various data sets. Explore technological solutions that can be used to proactively or reactively respond to diverse threats in networked environments. Outline a future research agenda for the interdisciplinary academic community to better understand and examine hackers and hacking over time.

There are 12 great chapters in this book, grouped into the following five sections: (1) Background, (2) Frameworks, (3) Empirical Assessments, (4) Corporate and Government Hacking and Network Intrusions, and (5) Policies, Techniques, and Laws for Protection.

Section 1 provides background information and an overview of hacking—and what experts say is the breadth of the problem. In Chapter 1, Robert Morris explores malicious hacking from a criminological perspective, while focusing on the justifications, or neutralizations, that cyber criminals may use when engaging in computer cracking—an act that is illegal in the United States and other jurisdictions worldwide. In Chapter 2, Orly Turgeman-Goldschmidt notes that scholars often view hacking as one category of computer crime, and computer crime as white-collar crime. He affirms that no study, to date, has examined the extent to which hackers exhibit the same characteristics as white-collar offenders. This chapter attempts to fill this void by looking at empirical data drawn from over 50 face-to-face interviews with Israeli hackers, in light of the literature in the field of white-collar offenders and concentrating on their accounts and socio-demographic characteristics. While white-collar offenders usually act for economic gain, notes the author, hackers act for fun, curiosity, and opportunities to demonstrate their computer virtuosity. But is this assertion validated by the data analyzed by this researcher?

In Chapter 3, Adam Bossler and George Burrus note that though in recent years, a number of studies have been completed on hackers’ personality and communication traits by experts in the fields of psychology and criminology, a number of questions regarding this population remain. One such query is, Does Gottfredson and Hirschi’s concept of low self-control predict the unauthorized access of computer systems? Do computer hackers have low levels of self-control, as has been found for other criminals in mainstream society? Their chapter focuses on proffering some answers to these questions.

In Chapter 4, David Wall notes that over the past two decades, network technologies have shaped just about every aspect of our lives, not least the way that we are now victimized. From the criminal’s point of view, networked technologies are a gift, for new technologies act as a force multiplier of grand proportions, providing individual criminals with personal access to an entirely new field of “distanciated” victims across a global span. This chapter looks at different ways that offenders can use networked computers to assist them in performing deceptions upon individual or corporate victims to obtain an informational or pecuniary advantage.

Section 2 consists of one chapter offering frameworks and models to study inhabitants of the Computer Underground. In Chapter 5, Johnny Nhan and Alesandra Garbagnatti look at policing of movie and music piracy in a U.S. context, applying the utility of a nodal governance model. This chapter explores structural and cultural conflicts among security actors that make fighting piracy extremely difficult. In addition, this chapter considers the role of law enforcement, government, and industries—as well as the general public—in creating long-term security models that will work.

Section 3 includes research studies from around the globe that report empirical findings on who hacks and cracks—why and how. In Chapter 6, Michael Bachmann notes that the increasing dependence of modern societies, industries, and individuals on information technology and computer networks renders them ever more vulnerable to attacks. While the societal threat posed by malicious hackers and other types of cyber criminals has been growing significantly in the past decade, mainstream criminology
has only begun to realize the significance of this threat. In this chapter, the author attempts to provide answers to questions like: Who exactly are these network attackers? Why do they engage in malicious hacking activities?

In Chapter 7, Thomas J. Holt looks at a particular segment of the dark side of the Computer Underground: Carders. Carders engage in carding activities—the illegal acquisition, sale, and exchange of sensitive information—which, the author notes, are a threat that has emerged in recent years. In this chapter, the author explores the argot, or language, used by carders through a qualitative analysis of 300 threads from six web forums run by and for data thieves. The terms used to convey knowledge about the information and services sold are explored.

In Chapter 8, Bernadette H. Schell and June Melnychuk look at the psychological, behavioral, and motivational traits of female and male hacker conference attendees, expanding the findings of the first author’s 2002 study on hackers’ predispositions, as detailed in the book *The Hacking of America*. This chapter looks at whether hackers are as strange behaviorally and psychologically as the media and the public believe them to be, focusing, in particular, on hackers’ autism-spectrum traits. It also focuses on hacker conference attendees’ self-reports about whether they believe their somewhat odd thinking and behaving patterns (as the world stereotypically perceives them) help them to be successful in their chosen field of endeavor.

Section 4 focuses on macro-system issues regarding corporate and government hacking and network intrusions. In Chapter 9, Dorothy E. Denning examines the emergence of social networks of non-state warriors launching cyber attacks for social and political reasons. The chapter examines the origin and nature of these networks; their objectives, targets, tactics, and use of online forums. In addition, the author looks at their relationship, if any, to their governments. General concepts are illustrated with case studies drawn from operations by Strano Net, the Electronic Disturbance Theater, the Electrohippies, and other networks of cyber activists. The chapter also examines the concepts of electronic jihad and patriotic hacking.

In Chapter 10, Robert Radzinoski looks at present-day fears regarding the safety and integrity of the U.S. national power grid, as questions have been raised by both political and executive-level management as to the risks associated with critical infrastructures, given their vulnerabilities and the possibility that hackers will exploit them. This chapter highlights the importance of preventing hack attacks against SCADA systems, or Industrial Control Systems (abbreviated as ICS), as a means of protecting nations’ critical infrastructures.

Section 5 deals with policies, techniques, and laws for protecting networks from insider and outsider attacks. In Chapter 11, Max Kilger notes that the future paths that cybercrime and cyber terrorism will take are influenced, in large part, by social factors at work, in concert with rapid advances in technology. Detailing the motivations of malicious actors in the digital world—coupled with an enhanced knowledge of the social structure of the hacker community, the author affirms, will give social scientists and computer scientists a better understanding of why these phenomena exist. This chapter builds on the previous book chapters by beginning with a brief review of malicious and non-malicious actors, proceeding to a comparative analysis of the shifts in the components of the social structure of the hacker subculture over the last decade, and concluding with an examination of two future cybercrime and national-security-related scenarios likely to emerge in the near future.

In Chapter 12, Walid Hejazi, Alan Lefort, Rafael Etges, and Ben Sapiro—a study team comprised of Canadian IT Security experts and a Business academic—examined Canadian IT Security Best Practices, with an aim to answering the question, Compared to the United States, how well is the Canadian industry
doing in thwarting network intrusions? This chapter describes their 2009 study findings, focusing on how 500 Canadian organizations with over 100 employees are faring in effectively coping with network breaches. The study team concludes that in 2009, as in 2008, Canadian organizations maintained that they have an ongoing commitment to IT Security Best Practices; however, with the global 2009 financial crisis, the threat appears to be amplified, both from outside the organization and from within. Study implications regarding the USA PATRIOT Act are discussed at the end of this chapter.

In closing, while we cannot posit that we have found all of the answers for helping to keep industrial and government networks safe, we believe that this book fills a major gap by providing social science, IT Security, and Business perspectives on present and future threats in this regard and on proposed safeguards for doing a better job of staying ahead of the cyber criminal curve.

*Thomas J. Holt*

*Michigan State University, USA*

*Bernadette H. Schell*

*Laurentian University, USA*