Preface

The successful protection against cyber crime is critical to an organization’s success and productivity. Current cyber crime destroys the everyday functionality of organizations and livelihood of individuals, but the technological advancements against cyber crime have revolutionized information science, robotics, forecasting and modeling, and a wide variety of technologies. From artificial intelligence and adaptive technology to data warehousing and mining, this ever-advancing research protecting against cyber crime is critical to the success of modern businesses, academic communities, and consumers.

The constantly changing landscape of cyber crime makes it challenging for experts and practitioners to stay informed of the field’s most up-to-date research. That is why Information Science Reference is pleased to offer this four-volume reference collection that will empower students, researchers, and academicians with a strong understanding of critical issues within cyber crime by providing both broad and detailed perspectives on cutting-edge theories and developments. This reference is designed to act as a single reference source on conceptual, methodological, technical, and managerial issues, as well as provide insight into emerging trends and future opportunities within the discipline.

Cyber Crime: Concepts, Methodologies, Tools and Applications is organized into eight distinct sections that provide comprehensive coverage of important topics. The sections are: (1) Fundamental Concepts and Theories, (2) Development and Design Methodologies, (3) Tools and Technologies, (4) Utilization and Application, (5) Organizational and Social Implications, (6) Managerial Impact, (7) Critical Issues, and (8) Emerging Trends. The following paragraphs provide a summary of what to expect from this invaluable reference tool.

Section I, Fundamental Concepts and Theories, serves as a foundation for this extensive reference tool by addressing crucial theories essential to the understanding of cyber crime. Introducing the book is “Internet Crime” by Tejaswini Herath. Further introductory chapters laying the groundwork for the rest of the book include “How Safe Is Your Identity?” by Bobbe Baggio and Yoany Beldarrain and “Deciphering the Hacker Underground” by Michael Bachmann. In all, the section covers topics from personal security to codebreaking, hacking, and the digital technologies for safeguarding information and data. It serves as a great tool for students and practitioners looking to get an understanding of the current basics within the field of cyber crime.

Section II, Development and Design Methodologies, presents in-depth coverage of the conceptual design and architecture of cyber crime, focusing on aspects including phishing, surveillance, privacy, and security to name a few. Chapters are presented in the forms of case studies, architectures, and frameworks for putting together techniques to deter and protect against cyber crime. The section opens with “A Simulation Model of IS Security” by Norman Pendegraft and Mark Rounds. Chapters vary in terms of technical and topical scope, with chapter authors from around the globe, such as “A Framework for Privacy Assurance and Ubiquitous Knowledge Discovery in Health 2.0 Data Mashups” by Jun Hu.
and Liam Peyton (University of Ottawa, Canada) and “A Partial Optimization Approach for Privacy Preserving Frequent Itemset Mining” by Shibnath Mukherjee (Yahoo! Research and Development, India), Aryya Gangopadhyay, and Zhiyuan Chen (University of Maryland Baltimore County, USA). The section concludes with “An Analysis of Privacy and Security in the Zachman and Federal Enterprise Architecture Frameworks” by Richard V. McCarthy.

Section III, Tools and Technologies, presents extensive coverage of the various tools and technologies used in the development and implementation of cyber crime. The first chapter, “Current Network Security Technology” by Göran Pulkkis, Kaj Grahn, and Peik Åström surveys the field and gives the latest technological breakthroughs and developments. Where the first two sections laid out planning and fundamentals of cyber crime and its prevention, section 3 includes chapters that detail the technical aspects of the current technological state of the art. Topics include hacking neutralization, biometric controls, image watermarking, and privacy regulation, and include cases and research from universities and the private sector around the world. Section 3 concludes with “Essential Mobile-Commerce Technology” by Wen-Chen Hu, a nice transition into the broad category of applications detailed in the next section.

Section IV, Utilization and Application, describes how cyber crime has been utilized and offers insight on and important lessons for its prevention and discouragement. Section four includes the widest range and largest number of chapters because it describes case studies, research, methodologies, frameworks, architectures, theory, analysis, and guides for implementation. Topics range from crimes against women, child pornography, and privacy protection to digital surveillance, telecommunication interception, and federal data mining. The section opens with two chapters about cross-cultural perceptions of security and privacy with “A Comparison of Cyber-Crime Definitions in India and the United States” by Manish Agrawal and Himanshu Maheshwari, and “Cross Cultural Perceptions on Privacy in the United States, Vietnam, Indonesia, and Taiwan” by Andy Chiou. Section 4 continues with four chapters about cyber crimes against women around the world, and then a broad survey of topics populate the remainder of the section. The section concludes with “A Performance Study of Secure Data Mining on the Cell Processor” by Hong Wang, Hiroyuki Takizawa, and Hiroaki Kobayashi.

Section V, Organizational and Social Implications, includes chapters discussing the organizational and social impact of cyber crime. Introducing the section is “ICT Security Policy: Challenges and Potential Remedies” by Lawan A. Mohammed. As section 5 continues, chapter topics will discuss how cyber crime affects organizations, people, communications, and interactions. It looks at behavior and decision making, and how people commit and are affected by cyber crime. The section continues with such chapters as “Female and Male Hacker Conferences Attendees” by Bernadette H. Schell and June Melnychuk, and concludes with “Effects of Individual Trust in Broadcast Media and the Internet on Privacy-Risking Uses of E-Health” by E. Vance Wilson, David D. Dobrzykowski, and Joseph A. Cazier.

Section VI, Managerial Impact, presents focused coverage of cyber crime as it relates to effective uses of resource allocation, forecasting, modeling, and much more. When a business’ security or privacy is threatened by cyber crime, it is the duty of the management to understand what they should be doing to protect their employees and the information in their company. The section opens with “Managing IS Security and Privacy” by Vasilios Katos. Managers and academics alike will find troubleshooting technologies and tools for addressing their information security needs. Other selected chapters within the section include “An Analysis of Online Privacy Policies of Fortune 100 Companies” by Suhong Li and “Building and Management of Trust in Networked Information Systems.” Section 6 concludes with “A Case for Consumer Virtual Property” by Matt Hettche, a look into the theory of virtual property and
how managers can use CRM methods and implement cyber security techniques to mainstream their processes and safeguard their products and information.

Section VII, Critical Issues, presents coverage of academic and research perspectives on cyber crime tools and applications. The section begins with an expository chapter, “The Sense of Security and Trust” by Yuko Murayama, Carl Hauser, Natsuko Hikage, and Basabi Chakraborty. This chapter opens the section by laying down the fundamentals of what it means to be safe and secure, and how individuals and societies function with the role of trust. Section 7 is full of chapters like this, detailing theory and analysis more so than technologies or management strategy. Critical issues include privacy paradox, etiology, and criminal motives, to name a few. Other highlights in section 7 include “A Profile of the Demographics, Psychological Predispositions, and Social/Behavioral Patterns of Computer Hacker Insiders and Outsiders” by Bernadette H. Schell and Thomas J. Holt, and “What About the Balance Between Law Enforcement and Data Protection?” by Maria Manuela Cruz-Cunha and Irene Maria Portela. Section 7 concludes with “Which Rights for Which Subjects? Genetic Confidentiality and Privacy in the Post-Genomic Era” by Antoinette Rouvroy, a fascinating look at the scientific privacy of one’s own genetic information, a fundamental, yet somewhat futuristic foray into the security issues of today and tomorrow.

Section VIII, Emerging Trends, highlights areas for future research within the field of cyber crime, opening with “Future Trends in Digital Security” by Daniel Viney. Section 8 offers the cutting edge within the field, and suggestions for the future research directions in the privacy and security protection against cyber crime. The final two chapters of the book include the latest research in technology and implementation of cyber crime prevention: “Cryptography-Based Authentication for Protecting Cyber Systems” by Xunhua Wang and Hua Lin, and “Aspect-Oriented Programming and Aspect.NET as Security and Privacy Tool for Web and 3D Web Programming” by Vladimir O. Safonov.

Although the primary organization of the contents in this multi-volume work is based on its eight sections, offering a progression of coverage of the important concepts, methodologies, technologies, applications, social issues, and emerging trends, the reader can also identify specific contents by utilizing the extensive indexing system listed at the end of each volume. Furthermore to ensure that the scholar, researcher, and educator have access to the entire contents of this multi volume set as well as additional coverage that could not be included in the print version of this publication, the publisher will provide unlimited multi-user electronic access to the online aggregated database of this collection for the life of the edition, free of charge when a library purchases a print copy. This aggregated database provides far more contents than what can be included in the print version in addition to continual updates. This unlimited access, coupled with the continuous updates to the database ensures that the most current research is accessible to knowledge seekers.

As a comprehensive collection of research on the latest findings related to using technology to providing various services, Cyber Crime: Concepts, Methodologies, Tools and Applications, provides researchers, administrators and all audiences with a complete understanding of the development of applications and concepts in cyber crime. Given the vast number of issues concerning usage, failure, success, policies, strategies, and applications of cyber crime in organizations, Cyber Crime: Concepts, Methodologies, Tools and Applications addresses the demand for a resource that encompasses the most pertinent research in privacy and security technologies being employed to globally counteract the impact of cyber crime.