Cybercrime Top 10 Countries Where Attacks Originate Bba

Discover the security risks that accompany the widespread adoption of new medical devices and how to mitigate them In Do No Harm: Protecting Connected Medical Devices, Healthcare, and Data from Hackers and Adversarial Nation States, cybersecurity expert Matthew Webster delivers an insightful synthesis of the health benefits of the Internet of Medical Things (IoMT), the evolution of security risks that have accompanied the growth of those devices, and practical steps we can take to protect ourselves, our data, and our hospitals from harm. You'll learn how the high barriers to entry for innovation in the field of healthcare are impeding necessary change and how innovation accessibility must be balanced against regulatory compliance and privacy to ensure safety. In this important book, the author describes: The increasing expansion of medical devices and the dark side of the high demand for medical devices The medical device regulatory landscape and the dilemmas hospitals find themselves in with respect medical devices Practical steps that individuals and businesses can take to encourage the adoption of safe and helpful medical devices or mitigate the risk of having insecure medical devices How to help individuals determine the difference between protected health information and the information from health devices--and protecting your data How to protect your health information from cell phones and applications that may push the boundaries of personal privacy Why cybercriminals can act with relative impunity against hospitals and other organizations Perfect for healthcare professionals, system administrators, and medical device researchers and developers, Do No Harm is an indispensable resource for anyone interested in the intersection of patient privacy, cybersecurity, and the world of Internet of Medical Things.

This edited book examines the contemporary regional security concerns in the Asia-Pacific recognizing the ‘Butterfly effect’, the concept that small causes can have large effects: ‘the flap of a butterfly’s wings can cause a typhoon halfway around the world’. For many Asia-Pacific states, domestic security challenges are at least as important as external security considerations. Recent events (both natural disasters and man-made disasters) have pointed to the inherent physical, economic, social and political vulnerabilities that exist in the region. Both black swan events and persistent threats to security characterize the challenges within the Asia-Pacific region. Transnational security challenges such as global climate change, environmental degradation, pandemics, energy security, supply chain security, resource scarcity, terrorism and organized crime are shaping the security landscape regionally and globally. The significance of emerging transnational security challenges in the Asia-Pacific Region impact globally and conversely, security developments in those other regions affect the Asia-Pacific region.

Over the years, a plethora of reports has emerged that assess the causes, dynamics, and effects of cyber threats. This proliferation of reports is an important sign of the increasing prominence of cyber attacks for organizations, both public and private, and citizens all over the world. In addition, cyber attacks are drawing more and more attention in the media. Such efforts can help to better awareness and understanding of cyber threats and pave the way to improved prevention, mitigation, and resilience. This report aims to help in this task by assessing what we know about cyber security threats based on a review of 70 studies published by public authorities, companies, and research organizations from about 15 countries over the last few years. It answers the following questions: what do we know about the number, origin, and impact of cyber attacks? What are the current and emerging cyber security trends? And how well are we prepared to face these threats?

As society continues to rely heavily on technological tools for facilitating business, e-commerce, banking, and communication, among other applications, there has been a significant rise in criminals seeking to exploit these tools for their nefarious gain. Countries all over the world are seeing substantial increases in identity theft and cyberattacks, as well as illicit transactions, including drug trafficking and human trafficking, being made through the dark web internet. Sex offenders and murderers explore unconventional methods of finding and contacting their victims through Facebook, Instagram, popular dating sites, etc., while pedophiles rely on these channels to obtain information and photographs of children, which are shared on hidden community sites. As criminals continue to harness technological advancements that are outpacing legal and ethical standards, law enforcement and government officials are faced with the challenge of devising new and alternative strategies to identify and apprehend criminals to preserve the safety of society. The Encyclopedia of Criminal Activities and the Deep Web is a three-volume set that includes comprehensive articles covering multidisciplinary research and expert insights provided by hundreds of leading researchers from 30 countries including the United States, the United Kingdom, Australia, New Zealand, Germany, Finland, South Korea, Malaysia, and more. This comprehensive encyclopedia provides the most diverse findings and new methodologies for monitoring and regulating the use of online tools as well as hidden areas of the internet, including the deep and dark web. Highlighting a wide range of topics such as cyberbullying, online hate speech, and hacktivism, this book will offer strategies for the prediction and prevention of online criminal activity and examine methods for safeguarding internet users and their data from being tracked or stalked. Due to the techniques and extensive knowledge discussed in this publication it is an invaluable addition for academic and corporate libraries as well as a critical resource for policy makers, law enforcement officials, forensic scientists, criminologists, sociologists, victim advocates, cybersecurity analysts, lawmakers, government officials, industry professionals, academicians, researchers, and students within this field of study.

India Rising unpacks the country’s approach to global governance by systematically considering three potential factors—ideas, interests, and institutions—that have an impact on India’s foreign policy making. The editors and contributors of this volume examine possible explanations for India’s varying compliance with global regimes and its contributions to the development and change of those regimes in areas such as nuclear non-proliferation, maritime security, counter-terrorism, cyber-governance, democracy promotion, climate change, and trade policy. The book also discusses how India is globally perceived in differing ways: as a hub of diplomatic interaction and as a difficult negotiator with a frequently inflexible stance. Looking at the prime ministerial years of Manmohan Singh and Narendra Modi’s first term, it examines India’s often ambivalent approach to global governance and foreign policy making in the backdrop of its image as a rising global power. It thus seeks to answer the primary question: What drives rising India’s conduct on the world stage?

Integrating theories from a wide range of disciplines, Nir Kshetri compares the patterns, characteristics and processes of cybercrime activities in major regions and economies in the Global South such as China, India, the former Second World economies, Latin America and the Caribbean, Sub-Saharan Africa and Middle East and North Africa.

An important outcome of the Fourth World Internet Conference, this book provides a comprehensive account of the status quo and trends in global Internet development. Covering network infrastructure, information technology, digital economy, e-governance, cyber security, and international cyberspace governance, it presents the Global Internet Development Index System to assess the Internet development of various major countries and emerging economies.

Written by experts on the frontlines, Investigating Internet Crimes provides seasoned and new investigators with the background and tools they need to investigate crime occurring in the online world. This invaluable guide provides step-by-step instructions for investigating Internet crimes, including locating, interpreting, understanding, collecting, and documenting online electronic evidence to benefit investigations. Cybercrime is the fastest growing area of crime as more criminals seek to exploit the speed, convenience and anonymity that the Internet provides to commit a diverse range of criminal activities. Today's online crime includes attacks against computer data and systems, identity theft, distribution of child pornography, penetration of online financial services, using social networks to commit crimes, and the deployment of viruses, botnets, and email scams such as phishing. Symantec's 2012 Norton Cybercrime Report stated that the world spent an estimated $110 billion to combat cybercrime, an average of nearly $200 per victim. Law enforcement agencies and corporate security officers around the world with the responsibility for enforcing, investigating and prosecuting cybercrime are overwhelmed, not only by the sheer number of crimes being committed but by a lack of adequate training material. This book provides that fundamental knowledge, including how to properly collect and document online evidence, trace IP addresses, and work undercover. Provides step-by-step instructions on how to investigate crimes online Covers how new software tools can assist in online investigations Discusses how to track down, interpret, and understand online electronic evidence to benefit investigations Details guidelines for collecting and documenting online evidence that can be presented in court

Detect and combat corporate fraud with new profiling techniques Profiling the Fraudster: Removing the Mask to Prevent and Detect Fraud takes a step-by-step approach beyond the Fraud Triangle to identify characteristics in potential fraudsters, employees and new hires that will sound alarm bells before they get their hands on your organization's assets. The typical organization loses a staggering 5% of its annual revenue to fraud. Traditional fraud investigations focus on the breakdown of internal controls but what happens when the human beings forming a key component of that chain of control are inherently dishonest? This book shows you how to recognize the characteristics and behavioral patterns of potential fraudsters who are entrusted with safeguarding corporate assets. The book includes: An in-depth look at fraud investigation techniques and how these can be enhanced by using the characteristics of fraudulent behavior, A detailed look at profiling potential perpetrators of fraud, A detailed breakdown of how to compile a fraud profile, A discussion of a wide range of organizational fraud, including abuse of power, embezzlement, computer fraud, expense abuse, and more, Tables, illustrations, and diagrams to enhance the narrative If you're a corporate fraud investigator, auditor, forensic accountant, law enforcement professional, or anyone challenged with safeguarding your organizations assets—Profiling the Fraudster shows you how to remove the mask and prevent and detect fraud.

In today’s litigious business world, cyber-related matters could land you in court. As a computer security professional, you are protecting your data, but are you protecting your company? While you know industry standards and regulations, you may not be a legal expert. Fortunately, in a few hours of reading, rather than months of classroom study, Tari Schreider’s Cybersecurity Law, Standards and Regulations (2nd Edition), lets you integrate legal issues into your security program. Tari Schreider, a board-certified information security practitioner with a criminal justice administration background, has written a much-needed book that bridges the gap between cybersecurity programs and cybersecurity law. He says, “My nearly 40 years in the fields of cybersecurity, risk management, and disaster recovery have taught me some immutable truths. One of these truths is that failure to consider the law when developing a cybersecurity program results in a protective façade or false sense of security.” In a friendly style, offering real-world business examples from his own experience supported by a wealth of court cases, Schreider covers the range of practical information you will need as you explore – and prepare to apply – cybersecurity law. His practical, easy-to-understand explanations help you to: Understand your legal duty to act reasonably and responsibly to protect assets and information. Identify which cybersecurity laws have the potential to impact your cybersecurity program. Upgrade cybersecurity policies to comply with state, federal, and regulatory statutes. Communicate effectively about cybersecurity law with corporate legal department and counsel. Understand the implications of emerging legislation for your cybersecurity program. Know how to avoid losing a cybersecurity court case on procedure – and develop strategies to handle a dispute out of court. Develop an international view of cybersecurity and data privacy – and international legal frameworks. Schreider takes you beyond security standards and regulatory controls to ensure that your current or future cybersecurity program complies with all laws and legal jurisdictions. Hundreds of citations and references allow you to dig deeper as you explore specific topics relevant to your organization or your studies. This book needs to be required reading before your next discussion with your corporate legal department. This new edition responds to the rapid changes in the cybersecurity industry, threat landscape and providers. It addresses the increasing risk of zero-day attacks, growth of state-sponsored adversaries and consolidation of cybersecurity products and services in addition to the substantial updates of standards, source links and cybersecurity products.

Social psychology is the scientific study of how the thoughts, feelings, and behaviors of individuals are influenced by the actual, imagined, and implied presence of others. In this definition, scientific refers to the empirical investigation using the scientific method, while the terms thoughts, feelings, and behaviors refer to the psychological variables that can be measured in humans. Moreover, the notion that the presence of others may be imagined or implied suggests that humans are malleable to social influences even when alone, such as when watching videos or quietly appreciating art. In such situations, people can be influenced to follow internalized cultural norms. Social psychology deals with social influence, social perception, and social interaction. The research in this field deals with what shapes our attitudes and how we develop prejudice. The Handbook of Research on Applied Social Psychology in Multiculturalism explores social psychology within the context of multiculturalism and the way society deals with cultural diversity at national and community levels. It will cover major topics of social psychology such as group behavior, social perception, leadership, non-verbal behavior, conformity, aggression, and prejudice. This book will deal with social psychology with a direct focus on how different cultures can coexist peacefully by preserving, respecting, and even encouraging cultural diversity, along with a focus on the psychology that is hindering these efforts. This book is essential for researchers in social psychology and the social sciences, activists, psychologists, practitioners, researchers, academicians, and students interested in how social psychology interacts with multiculturalism.

As more individuals own and operate Internet-enabled devices and more critical government and industrial systems rely on advanced technologies, the issue of cybercrime has become a crucial concern for both the general public and professionals alike. The Psychology of Cyber Crime: Concepts and Principles aims to be the leading reference examining the psychology of cybercrime. This book considers many aspects of cybercrime, including research on offenders, legal issues, the impact of cybercrime on victims, punishment, and preventative measures. It is designed as a source for researchers and practitioners in the disciplines of criminology, cyberpsychology, and forensic psychology, though it is also likely to be of significant interest to many students of information technology and other related disciplines.

The growth of technology allows us to imagine entirely new ways of committing, combating and thinking about criminality, criminals, police, courts, victims and citizens. Technology offers not only new tools for committing and fighting crime, but new ways to look for, unveil, label crimes and new ways to know, watch, prosecute and punish criminals. This book attempts to disentangle the realities, the myths, the politics, the theories and the practices of our new, technology-assisted, era of crime and policing. Technocrime, policing and surveillance explores new areas of technocrime and technopolicing, such as credit card fraud, the use of DNA and fingerprint databases, the work of media in creating new crimes and new criminals, as well as the "proper" way of doing policing, and the everyday work of police investigators and intelligence officers, as seen through their own eyes. These chapters offer new avenues for studying technology, crime and control, through innovative social science methodologies. This book builds on the work of Leman-Langlois' last book Technocrime, and brings together fresh perspectives from eminent scholars to consider how our relationship with technology and institutions of social control are being reframed, with particular emphasis on policing and surveillance. Technocrime, policing and surveillance will be of interest to those studying criminal justice, policing and the sociology of surveillance as well as practitioners involved with the legal aspects of law enforcement technologies, , domestic security government departments and consumer advocacy groups.

This Handbook addresses the key questions surrounding US–China relations: what are the historical and contemporary contexts that underpin this complex relationship? How has the strategic rivalry between the two evolved? What are the key flashpoints in their relationship? What are the key security issues between the two powers? The international contributors explore the historical, political, economic, military, and international and regional spheres of the US–China relationship. The topics they discuss include human rights, Chinese public perception of the United States, US–China strategic rivalry, China’s defence build-up and cyber war.

Threatening the safety of individuals, computers, and entire networks, cyber crime attacks vary in severity and type. Studying this continually evolving discipline involves not only understanding different types of attacks, which range from identity theft to cyberwarfare, but also identifying methods for their prevention. Cyber Crime: Concepts, Methodologies, Tools and Applications is a three-volume reference that explores all aspects of computer-based crime and threats, offering solutions and best practices from experts in software development, information security, and law. As cyber crime continues to change and new types of threats emerge, research focuses on developing a critical understanding of different types of attacks and how they can best be managed and eliminated.

Cybercrime and Business: Strategies for Global Corporate Security examines the three most prevalent cybercrimes afflicting today's corporate security professionals: piracy, espionage, and computer hacking. By demonstrating how each of these threats evolved separately and then converged to form an ultra-dangerous composite threat, the book discusses the impact the threats pose and how the very technologies that created the problem can help solve it. Cybercrime and Business then offers viable strategies for how different types of businesses—from large multinationals to small start-ups—can respond to these threats to both minimize their losses and gain a competitive advantage. The book concludes by identifying future technological threats and how the models presented in the book can be applied to handling them. Demonstrates how to effectively handle corporate cyber security issues using case studies from a wide range of companies around the globe Highlights the regulatory, economic, cultural, and demographic trends businesses encounter when facing security issues Profiles corporate security issues in major industrialized, developing, and emerging countries throughout North America, Europe, Asia, Latin America, Africa, and the Middle East

Explaining cybercrime in a highly networked world, this book provides a comprehensive yet accessible summary of the history, modern developments, and efforts to combat cybercrime in various forms at all levels of government—international, national, state, and local. • Provides accessible, comprehensive coverage of a complex topic that encompasses identity theft to copyright infringement written for non-technical readers • Pays due attention to important elements of cybercrime that have been largely ignored in the field, especially politics • Supplies examinations of both the domestic and international efforts to combat cybercrime • Serves an ideal text for first-year undergraduate students in criminal justice programs

Recent developments in cyber security, crime, and forensics have attracted researcher and practitioner interests from technological, organizational and policy-making perspectives. Technological advances address challenges in information sharing, surveillance and analysis, but organizational advances are needed to foster collaboration between federal, state and local agencies as well as the private sector. Cyber Security, Cyber Crime and Cyber Forensics: Applications and Perspectives provides broad coverage of technical and socio-economic perspectives for utilizing information and communication technologies and developing practical solutions in cyber security, cyber crime and cyber forensics.

Looking for a fun way to learn or teach cybersecurity? Whether for yourself or a young person in your life, this one-of-a-kind puzzle book will also transform the puzzle-solver into someone who understands the fundamentals of cybersecurity. You'll be better off than 99.99% of the rest of the population! And you'll be ready to take your knowledge and skills to the next level with whatever you choose to do next. YOU WILL LEARN through a wide variety of 25+ puzzles and activities Essential terms in cybersecurity Computer hardware overview Computer software overview Cybersecurity practices and principles An industry-recognized cybersecurity framework Top 10 countries that are sources of cybercrime attacks Top 10 countries that are victims of cybercrime attacks How to create (and solve) a cybersecurity algorithm (aka cipher) To encourage the pursuit of an education or career in cybersecurity, there are also puzzles specifically on: School subjects every cybersecurity professional needs to study Jobs in cybersecurity Relevant and practical skills for cybersecurity that are fostered through these puzzles include: fault detection network tracing threat avoidance memory recall encryption deciphering logical reasoning analytical thinking password integrity threat detection strategic thinking mental endurance concentration creativity geography What types of puzzles and activities are here for your enjoyment and mental exercise, you are wondering? Take a look at this long list! cryptograms word searches mazes crosswords words scrambles sudoku find the defect (spot the difference) coloring BONUS SECTION FOR GROUP PLAY: This book also features a set of paper-based two-player games. Hacker Hide And Seek (a fun version of the popular ocean warships game) 3-D Tic Tac Toe Dots and Boxes You can photocopy those pages to make as many copies as you like. The pages are full-size high-quality white paper (8.5x11"). Most puzzles are single-sided in order to minimize bleed-through or puncturing into other puzzles. WHY THIS BOOK IS SPECIAL Cybersecurity is important enough that everyone with a computer and internet connection should have a basic understanding of it. Why spend lots of money and time on boring online courses, text books, or lectures when you can learn much of that here? (You'll be surprised how informed you or your child will become compared to everyone else.) Best of all, this requires no batteries, no electricity, and no staring at a computer screen! Considering the number of hours this book will keep someone occupied while they learn about cybersecurity, you'll realize that this cybersecurity puzzle book for kids is one of the smartest investments you've ever made as a practical and effective educational resource. Answers are provided in the back. The information in this book comes from recognized and respected sources in cybersecurity such as the U.S. Cybersecurity and Infrastructure Security Agency (CISA), the U.S. National Institute of Standards and Technology (NIST), and several industry leaders. Puzzle Punk Books exists to create puzzle books that bring a (slightly) punk attitude into the world. This means we enjoy challenging the status quo and making people see the world in a new way, through puzzles. Click our name to see our passionately created list of other products. Thank you for your purchase.

This book starts with the basic premise that a service is comprised of the 3Ps-products, processes, and people. Moreover, these entities and their sub-entities interlink to support the services that end users require to run and support a business. This widens the scope of any availability design far beyond hardware and software. It also increases t

This book constitutes the refereed proceedings of the Pacific Asia Workshop on Intelligence and Security Informatics, PAISI 2007, held in Chengdu, China in April 2007. Coverage includes crime analysis, emergency response and surveillance, intrusion detection, network security, data and text mining, cybercrime and information access and security, intrusion detection, network security, terrorism informatics and crime analysis.

This book provides an overview of the most recent developments in Internet of Things (IoT) security and data protection. It presents the results of several international research projects addressing this topic from complementary angles. It starts by analyzing the main privacy and security threats on IoT, as well as the evolution of data protection norms, such as the European General Data Protection Regulation (GDPR), and their impact on IoT. Through a comprehensive and systematic approach, the contributors present new perspectives on IoT & Cloud Computing security requirements. They discuss the most recent approach to support trusted IoT, including new models of privacy risk assessment, labeling and certification, and contractual tools (such as Privacy PACT). Practical implementations, such as in the European Large Scale Pilots on IoT for Smart Cities (Synchronicity), are presented, explaining how they address security, privacy and data protection. Finally, innovative models to secure IoT systems are presented for the network and end-nodes security, including network threats analysis.

The true story of Max Butler, the master hacker who ran a billion dollar cyber crime network. The word spread through the hacking underground like some unstoppable new virus: an audacious crook had staged a hostile takeover of an online criminal network that siphoned billions of dollars from the US economy. The culprit was a brilliant programmer with a hippie ethic and a supervillain's double identity. Max 'Vision' Butler was a white-hat hacker and a celebrity throughout the programming world, even serving as a consultant to the FBI. But there was another side to Max. As the black-hat 'Iceman', he'd seen the fraudsters around him squabble, their ranks riddled with infiltrators, their methods inefficient, and in their dysfunction was the ultimate challenge: he would stage a coup and steal their ill-gotten gains from right under their noses. Through the story of Max Butler's remarkable rise, KINGPIN lays bare the workings of a silent crime wave affecting millions worldwide. It exposes vast online-fraud supermarkets stocked with credit card numbers, counterfeit cheques, hacked bank accounts and fake passports. Thanks to Kevin Poulsen's remarkable access to both cops and criminals, we step inside the quiet,desperate battle that law enforcement fights against these scammers. And learn that the boy next door may not be all he seems.

“Given the complexity of the issues, the study of social problems requires, indeed demands, specialized focus by experts.” -A. Javier Treviño Welcome to a new way of Investigating Social Problems. In this groundbreaking new text, general editor A. Javier Treviño, working with a panel of experts, thoroughly examines all aspects of social problems, providing a contemporary and authoritative introduction to the field. Each chapter is written by a specialist on that particular topic. This unique, contributed format ensures that the research and examples provided are the most current and relevant in the field. The chapters carefully follow a model framework to ensure consistency across the entire text and provide continuity for the reader. The text is framed around three major themes: intersectionality (the interplay of race, ethnicity, class, and gender), the global scope of many problems, and how researchers take an evidence-based approach to studying problems.

The Handbook of Asian Criminology aims to be a key reference for international scholars with an interest in the broad theme of international criminology in general, and the Asian region in particular. Contextualization is a key theme in this book. The role of context is often underemphasized in international criminology, so the Handbook of Asian Criminology’s premise that crime and the responses to it are best understood as deeply embedded in the cultural specificity of the environment which produces them will play a key role throughout the work. Attention will be given to country- and region specific attitudes towards crime and punishment.

A comprehensive examination of different forms of identity theft and its economic impact, including profiles of perpetrators and victims and coverage of current trends, security implications, prevention efforts, and legislative actions. * Includes a chronology of key decisions, cases, and government action in the development of identity theft policy * Offers a list of key terms that will help the reader to better understand the sometimes unique language of crimes

Learn the art of preventing digital extortion and securing confidential data About This Book Get acquainted with multiple cyber extortion attacks and techniques to mitigate them Learn how DDOS, Crypto Virus, and other cyber extortion techniques can infect your computers, smartphones, servers, and cloud A concise, fast-paced guide that develops your skills in protecting confidential data by leveraging widely used tools Who This Book Is For This book targets IT security managers, IT security engineers, security analysts, and professionals who are eager to avoid digital extortion for themselves or their organizations. They may have heard of such attacks but are not aware of their various types, techniques, and business impact. What You Will Learn Delve into the various types, stages, and economics of digital extortion Understand the science behind different attacks Understand the gravity of and mechanics behind ransomware and prevent and mitigate data breaches and financial losses Use effective tools to defend against ransomware Analyze attacks, the money flow, and cyber insurance processes Learn the art of preventing digital extortion and securing confidential data Get an idea of the future of extortion tactics and how technological advances will affect their development In Detail More and more cyber threats keep emerging every day, affecting organizations across the board, targeting the entire spectrum of the Internet. Digital--or cyber--extortion so far has come across as the most serious of such threats as it seeks to profit from criminal activity, akin to blackmail. Such extortion has been rising exponentially in the digital age and has become a huge illegal money-making business, affecting users and organizations ranging from small businesses to large enterprises. This is an insightful study spelling out in detail the ways and means employed by cyber criminals in targeting various devices and the multiple dangers such malicious activity embodies. Here will be found an overview of methods employed to impact and infect computers, smartphones, servers, and the IoT for cyber extortion. Then, it will move on to specific subjects in more detail, covering attacks such as DDoS-based extortion, cryptoviruses, and ransomware. You will learn how to prevent such attacks and eliminate them if you are compromised. This book will help you become a pro at securing your data and preventing your organization from paying a hefty ransom. Style and approach This step-by-step guide will start with the fundamentals of digital or cyber extortion and the various techniques used by hackers to demand ransom from an organization. It also focuses on types of ransomware and how it can infect your computer, mobile, cloud, server, and IOT. This practical guide will also explain how you can eliminate such attacks by leveraging various open source/commercial tools.

Online Version - Discusses current cybercrime laws and practices. Available online for downloading.

This book constitutes the thoroughly refereed post-conference proceedings of the Third International ICST Conference on e-Infrastructure and e-Services for Developing Countries, AFRICOMM 2011, held in Zanzibar, Tansania, in November 2011. The 24 revised full papers presented together with 2 poster papers were carefully reviewed and selected from numerous submissions. The papers cover a wide range of topics in the field of information and communication infrastructures. They are organized in two tracks: communication infrastructures for developing countries and electronic services, ICT policy, and regulatory issues for developing countries.

This book contains a selection of thoroughly refereed and revised papers from the Fourth International ICST Conference on Digital Forensics and Cyber Crime, ICDF2C 2012, held in October 2012 in Lafayette, Indiana, USA. The 20 papers in this volume are grouped in the following topical sections: cloud investigation; malware; behavioral; law; mobile device forensics; and cybercrime investigations.

Sailing Safe in Cyberspace is an excellent resource on safe computing. It gives in-depth exposure to the various ways in which security of information might be compromised, how cybercrime markets work and measures that can be taken to ensure safety at individual and organizational levels. Cyber security is not just a technical subject that can be resolved like any other IT-related problem—it is a ‘risk’ that can be mitigated by creating awareness and getting the right combination of technology and practices based on careful analysis. This book combines insights on cybersecurity from academic research, media reports, vendor reports, practical consultation and research experience. The first section of the book discusses motivation and types of cybercrimes that can take place. The second lists the major types of threats that users might encounter. The third discusses the impact, trend and role of the government in combating cybercrime. The fourth section of the book tells the readers about ways to protect themselves and secure their data/information stored in computers and the cyberspace. It concludes by offering suggestions for building a secure cyber environment.

Cybercrime and Security is edited by Pauline Reich, an American lawyer and professor at Waseda University School of Law in Tokyo, Japan, hailed by The Japan Times as a pioneer in the field of cybercrime. The set provides detailed coverage of a full range of issues - including attacks on computers, electronic evidence, advance fee fraud, and critical information infrastructure protection. It includes sections on national legislation with commentaries, regional approaches, industry case studies, and more.

Cybercafes, which are places where Internet access is provided for free, provide the opportunity for people without access to the Internet, or who are traveling, to access Web mail and instant messages, read newspapers, and explore other resources of the Internet. Due to the important role Internet cafes play in facilitating access to information, there is a need for their systems to have well-installed software in order to ensure smooth service delivery. Security and Software for Cybercafes provides relevant theoretical frameworks and current empirical research findings on the security measures and software necessary for cybercafes, offering information technology professionals, scholars, researchers, and educators detailed knowledge and understanding of this innovative and leading-edge issue, both in industrialized and developing countries.

THE INSTANT NEW YORK TIMES BESTSELLER SHORTLISTED FOR THE FT & McKINSEY BUSINESS BOOK OF THE YEAR AWARD 2021 'An intricately detailed, deeply sourced and reported history of the origins and growth of the cyberweapons market . . . Hot, propulsive . . . Sets out from the start to scare us out of our complacency' New York Times 'A terrifying exposé' The Times 'Part John le Carré and more parts Michael Crichton . . . Spellbinding' New Yorker Zero day: a software bug that allows a hacker to break in and scamper through the world's computer networks invisibly until discovered. One of the most coveted tools in a spy's arsenal, a zero day has the power to tap into any iPhone, dismantle safety controls at a chemical plant and shut down the power in an entire nation – just ask the Ukraine. Zero days are the blood diamonds of the security trade, pursued by nation states, defense contractors, cybercriminals, and security defenders alike. In this market, governments aren't regulators; they are clients – paying huge sums to hackers willing to turn over gaps in the Internet, and stay silent about them. This Is How They Tell Me the World Ends is cybersecurity reporter Nicole Perlroth's discovery, unpacked. A intrepid journalist unravels an opaque, code-driven market from the outside in – encountering spies, hackers, arms dealers, mercenaries and a few unsung heroes along the way. As the stakes get higher and higher in the rush to push the world's critical infrastructure online, This Is How They Tell Me the World Ends is the urgent and alarming discovery of one of the world's most extreme threats.

What makes behavior deviant, and who gets to decide what deviance is? Deviant Behavior seeks to answer these questions and more. This compelling new text covers the social forces that shape deviance, the motivations and consequences of deviant behaviors, and how our definition of deviance changes over time. Authors John A. Humphrey and Frank Schmalleger discuss a wide range of deviant behaviors—from criminal acts to extreme forms of everyday behavior—and provide students the necessary foundation to understand the impact of globalization on traditional and emerging forms of deviance. Readers will explore deviance in the modern world using a systematic application of social and criminological theories to a range of deviant behaviors to help them better understand themselves, others, and society.

Malicious software - designed to infect computers to steal bank details and identity information - poses a growing threat in the UK as more people use the internet and an increasing proportion of economic activity takes place online. The Science and Technology Committee say the Government must do more to help the public understand how to stay safe online. It calls for a prolonged awareness raising campaign to increase public understanding of personal online security. Eighty per cent of protection against cyber-attack is routine IT hygiene, yet currently there is no single first point of advice and help for consumers and much of the online information about internet security is often technical or jargon filled. Television exposure is crucial to gain the widest possible exposure to the safety message, and more should be done to promote and resource the existing Government website Get Safe Online. Advice from Get Safe Online should be provided with every device capable of accessing the internet and all Government websites should link to the website and highlight the latest security updates. The provision of Government services by the 'digital by default' policy will increasingly require those in receipt of Government benefits and services to access these online. The Committee raises concerns that the scheme will be of greater use in protecting the Government against welfare fraud than the individual user against crime. The Government should investigate the potential for imposing statutory safety standards if the industry cannot demonstrate that voluntary self-regulation can improve security.

THE INSTANT NEW YORK TIMES BESTSELLER 'An intricately detailed, deeply sourced and reported history of the origins and growth of the cyberweapons market . . . Hot, propulsive . . . Sets out from the start to scare us out of our complacency' New York Times 'A terrifying exposé' The Times 'Part John le Carré and more parts Michael Crichton . . . Spellbinding' New Yorker Zero day: a software bug that allows a hacker to break in and scamper through the world's computer networks invisibly until discovered. One of the most coveted tools in a spy's arsenal, a zero day has the power to tap into any iPhone, dismantle safety controls at a chemical plant and shut down the power in an entire nation – just ask the Ukraine. Zero days are the blood diamonds of the security trade, pursued by nation states, defense contractors, cybercriminals, and security defenders alike. In this market, governments aren't regulators; they are clients – paying huge sums to hackers willing to turn over gaps in the Internet, and stay silent about them. This Is How They Tell Me the World Ends is cybersecurity reporter Nicole Perlroth's discovery, unpacked. A intrepid journalist unravels an opaque, code-driven market from the outside in – encountering spies, hackers, arms dealers, mercenaries and a few unsung heroes along the way. As the stakes get higher and higher in the rush to push the world's critical infrastructure online, This Is How They Tell Me the World Ends is the urgent and alarming discovery of one of the world's most extreme threats.

This important reference work is an extensive, up-to-date resource for students wanting to immerse themselves in the world of cybercrime, or for those seeking further knowledge of specific attacks both domestically and internationally. Cybercrime is characterized by criminal acts that take place in the borderless digital realm. It takes on many forms, and its perpetrators and victims are varied. From financial theft, destruction of systems, fraud, corporate espionage, and ransoming of information to the more personal, such as stalking and web-cam spying as well as cyberterrorism, this work covers the full spectrum of crimes committed via cyberspace. This comprehensive encyclopedia covers the most noteworthy attacks while also focusing on the myriad issues that surround cybercrime. It includes entries on such topics as the different types of cyberattacks, cybercrime techniques, specific cybercriminals and cybercrime groups, and cybercrime investigations. While objective in its approach, this book does not shy away from covering such relevant, controversial topics as Julian Assange and Russian interference in the 2016 U.S. presidential election. It also provides detailed information on all of the latest developments in this constantly evolving field. Includes an introductory overview essay that discusses all aspects of cybercrime—how it's defined, how it developed, and its massive expansion in recent years Offers a wide array of entries regarding cybercrime and the many ways it can be committed Explores the largest, most costly cyber attacks on a variety of victims, including corporations, governments, consumers, and individuals Provides up-to-date information on the ever-evolving field of cybercrime