Spam Nation: The Inside Story Of Organized Cybercrime From Global Epidemic To Your Front Door

This is an exciting new edition of a core textbook that explores innovation management from a global perspective. Innovation management is increasingly significant, both as an academic discipline and as an integral part of the way businesses seek to change and grow. However the key factors behind successful innovation and the process by which innovation is turned into profit in the global arena remain largely undefined. The new edition provides a unique answer to these questions and offers a step-by-step guide to innovation strategy development, taking into account the global context in which businesses today operate. Written by a highly experienced instructor, this is an ideal companion for undergraduate students of innovation as well as postgraduate and MBA students taking modules with an innovation component. New to this Edition: - Completely rewritten and restructured to explore in more depth how innovative ideas are identified and strategized in an increasingly globalized world - Fully updated and extended case studies on world-leading companies - Increased attention to commercialized innovation, including factors such as intellectual property laws, technology acceleration and the competition for venture capital and finance - Coverage of new topics such as open innovation and service innovation - Expanded coverage of the tools and methods needed to understand financial gain and risk

The Australian Labor Party is one of the oldest labour parties and was the first in the world to form a government. 2011 marks its 120th birthday This short and lively book tells the story of the ALPs numerous successes in winning government at all levels and making policy that has transformed lives.

Documents how a troubled young computer hacker seized control of a massive international computer fraud network in 2006, tracing the efforts of FBI and Secret Service agents as well as an undercover operator to locate and arrest him. Reprint.

Now a New York Times bestseller! There is a Threat Lurking Online with the Power to Destroy Your Finances, Steal Your Personal Data, and Endanger Your Life. In Spam Nation, investigative journalist and cybersecurity expert Brian Krebs unmasks the criminal masterminds driving some of the biggest spam and hacker operations targeting Americans and their bank accounts. Tracing the rise, fall, and alarming resurrection of the digital mafia behind the two largest spam pharmacies-and countless viruses, phishing, and spyware attacks-he delivers the first definitive narrative of the global spam problem and its threat to consumers everywhere. Blending cutting-edge research, investigative reporting, and firsthand interviews, this terrifying true story reveals how we unwittingly invite these digital thieves into our lives every day. From unassuming computer programmers right next door to digital mobsters like "Cosma"-who unleashed a massive malware attack that has stolen thousands of Americans' logins and passwords-Krebs uncovers the shocking lengths to which these people will go to profit from our data and our wallets. Not only are hundreds of thousands of Americans exposing themselves to fraud and dangerously toxic products from rogue online pharmacies, but even those who never open junk messages are at risk. As Krebs notes, spammers can-and do-hack into accounts through these emails, harvest personal information like usernames and passwords, and sell them on the digital black market. The fallout from this global epidemic doesn't just cost consumers and companies billions, it costs lives too. Fast-paced and utterly gripping, Spam Nation ultimately proposes concrete solutions for protecting ourselves online and stemming this tidal wave of cybercrime-before it's too late. "Krebs's talent for exposing the weaknesses in online security has earned him respect in the IT business and loathing among cybercriminals... His track record of scoops...has helped him become the rare blogger who supports himself on the strength of his reputation for hard-nosed reporting." -Bloomberg Businessweek

Click Here to Kill Everybody: Security and Survival in a Hyper-connected World

Leading Security Experts Explain How They Think

Fight Fire with Fire

Nation

The Beautiful Struggle (Adapted for Young Adults)

Raising Confident, Independent, and Thoughtful Children in an Age of Instant Gratification

CyberThieves, CyberCops and You

NEW YORK TIMES BESTSELLER WASHINGTON POST BESTSELLER Winner of the getAbstract 17th International Book Award "The Seventh Sense is a concept every businessman, diplomat, or student should aspire to master--a powerful idea, backed by stories and figures that will be impossible to forget." -- Walter Isaacson, author of Steve Jobs and Leonardo da Vinci Endless terror. Refugee waves. An unfixable global economy. Surprising election results. New billion-dollar fortunes. Miracle medical advances. What if they were all connected? What if you could understand why? The Seventh Sense is the story of what all of today's successful figures see and feel: the forces that are invisible to most of us but explain everything from explosive technological change to uneasy political ripples. The secret to power now is understanding our new age of networks. Not merely the Internet, but also webs of trade, finance, and even DNA. Based on his years of advising generals, CEOs, and politicians, Ramo takes us into the opaque heart of our world's rapidly connected systems and teaches us what the losers are not yet seeing--and what the victors of this age already know.

This volume contains a comprehensive examination of the crucial first ten years of the Arab League and of the continuing dilemma it faces in juggling opposing local and regional interests.

"People are stupid, Davis Wolfgang Hawke thought as he stared at the nearly empty box of Swastika pendants on his desk." So begins Spam Kings, an investigative look into the shady world of email spammers and the people trying to stop them. This compelling exposé explores the shadowy world of the people responsible for today's junk-email epidemic. Investigative journalist Brian McWilliams delivers a fascinating account of the cat-and-mouse game played by spam entrepreneurs in search of easy fortunes and anti-spam activists. McWilliams chronicles the activities of several spam kings, including Hawke, a notorious Jewish-born neo-Nazi leader. You'll follow this 20-year-old's rise in the trade, where he became a major player in the lucrative penis pill market—a business that would make him a millionaire and the target of lawsuits. You'll also meet cyber-vigilantes, such as Susan Gunn, who have taken up the fight against spammers like Hawke. Explore the sleazy spammer business practices, the surprising new partnership between spammers and computer hackers, and the rise of a new breed of computer viruses designed to turn the PCs of innocent bystanders into secret spam factories.

From the bestselling author of Black Hawk Down, the gripping story of the Conficker worm—the cyberattack that nearly toppled the world. The Conficker worm infected its first computer in November 2008, and within a month had infiltrated 1.5 million computers in 195 countries. Banks, telecommunications companies, and critical government networks—including British Parliament and the French and German military—became infected almost instantaneously. No one had ever seen anything like it. By January 2009, the worm lay hidden in at least eight million computers, and the botnet of linked computers it had created was big enough that an attack might crash the world. In this "masterpiece" (The Philadelphia Inquirer), Mark Bowden expertly lays out a spellbinding tale of how hackers, researchers, millionaire Internet entrepreneurs, and computer security experts found themselves drawn into a battle between those determined to exploit the Internet and those committed to protecting it.

Unleashing Demons

Crime Mapping, Information Technology, and the Rationality of Crime Control

Crime Online

Building an Effective Security Program

How a New Illicit Economy Is Threatening Our Future

Social Media, Crime, and the Criminal Legal System

No One Would Listen

As research continues to accumulate on the connections between media and crime, #Crime explores the impact of social media on the criminal legal system. It examines how media influences our perceptions of crime, the perpetration of crime, and the implementation of punishment, whilst emphasizing the significance of race, ethnicity, class, gender, and sexuality. It offers an accessible and in-depth examination of media and in each chapter there are case studies and examples from both legacy and new media, including discussions from Twitter that are being used to raise awareness of criminal legal issues. It also includes interviews with international scholars and practitioners from Australia, Belgium, and the United States to voice a range of global perspectives. This book speaks broadly to those interested in criminology, criminal justice, media and culture, sociology, and gender studies.

"In light of the increasing adoption of technology, it is critical that researchers explore the complex effects of computer technology on human behavior and the intersection of real world and virtual experiences. Crime Online uses empirical tests and unique data to provide detailed criminological explorations of multiple forms of cybercrime, including phishing, hacking, and sex crimes. This text also includes a comprehensive exploration of cyberterrorism and activism in online environments. The law enforcement and policy responses to cybercrimes at the local, state, and federal level are also discussed in detail. This work provides practical policy discussions that will benefit academics, law enforcement, legal counsel, and students at the undergraduate and graduate level"--

A world of "smart" devices means the Internet can kill people. We need to act. Now. Everything is a computer. Ovens are computers that make things hot; refrigerators are computers that keep things cold. These computers—from home thermostats to chemical plants—are all online. The Internet, once a virtual abstraction, can now sense and touch the physical world. As we open our lives to this future, often called the Internet of Things, we are beginning to see its enormous potential in ideas like driverless cars, smart cities, and personal agents equipped with their own behavioral algorithms. But every knife cuts two ways. All computers can be hacked. And Internet-connected computers are the most vulnerable. Forget data theft: cutting-edge digital attackers can now crash your car, your pacemaker, and the nation's power grid. In Click Here to Kill Everybody, renowned expert and best-selling author Bruce Schneier examines the hidden risks of this new reality. After exploring the full implications of a world populated by hyperconnected devices, Schneier reveals the hidden web of technical, political, and market forces that underpin the pervasive insecurities of today. He then offers common-sense choices for companies, governments, and individuals that can allow us to enjoy the benefits of this omnipotent age without falling prey to its vulnerabilities. From principles for a more resilient Internet of Things, to a recipe for sane government regulation and oversight, to a better way to understand a truly new environment, Schneier's vision is required reading for anyone invested in human flourishing.

As David Cameron's director of Politics and communications, Craig Oliver was in the room at every key moment during the EU referendum - the biggest political event in the UK since World War 2. Craig Oliver worked with all the players, including David Cameron, George Osbourne, Barack Obama, Angela Merkel, Jeremy Corbyn, Boris Johnson,Michael Gove, Theresa May and Peter Mandelson. Unleashing Demons is based on his extensive notes, detailing everything from the decision to call a referendum, to the subsequent civil war in the Conservative Party and the aftermath of the shocking result. This is raw history at its very best, packed with enthralling detail and colourful anecdotes from behind the closed doors of the campaign that changed British history.

How One Hacker Took Over the Billion-Dollar Cybercrime Underground

Power, Fortune, and Survival in the Age of Networks

A Brief History with Skills and Sources, For the AP® Course

The Real Stories Behind the Exploits of Hackers, Intruders and Deceivers

The Technology of Policing

The Crystallization of the Arab State System, 1945-1954

Native America from 1890 to the Present

Spam NationThe Inside Story of Organized Cybercrime-from Global Epidemic to Your Front DoorSourcebooks, Inc.

Before the Internet became widely known as a global tool for terrorists, one perceptive U.S. citizen recognized its ominous potential. Armed with clear evidence of computer espionage, he began a highly personal quest to expose a hidden network of spies that threatened national security. But would the authorities back him up? Cliff Stoll's dramatic firsthand account is "a computer-age detective story, instantly fascinating [and] astonishingly gripping" (Smithsonian). Cliff Stoll was an astronomer turned systems manager at Lawrence Berkeley Lab when a 75-cent accounting error alerted him to the presence of an unauthorized user on his system. The hacker's code name was "Hunter"—a mysterious invader who managed to break into U.S. computer systems and steal sensitive military and security information. Stoll began a one-man hunt of his own: spying on the spy. It was a dangerous game of deception, broken codes, satellites, and missile bases—a one-man sting operation that finally gained the attention of the CIA . . . and ultimately trapped an international spy ring fueled by cash, cocaine, and the KGB.

Why Do Kids These Days Expect Everything to be Given to Them? Today's kids don't know how to read a map. They can Google the answer to any question at lightning speed. If a teen forgets his homework, a quick call to mom or dad has it hand-delivered in minutes. Fueled by the rapid pace of technology, the Instant Gratification Generation not only expects immediate solutions to problems—they're more dependent than ever on adults. Today's kids are being denied opportunities to make mistakes, and more importantly, to learn from them. They are being taught not to think. In Teaching Kids to Think, Dr. Darlene Sweetland and Dr. Ron Stolberg offer insight into the social, emotional, and neurological challenges unique to this generation. They identify the five parent traps that cause adults to unknowingly increase their children's need for instant gratification, and offer practical tips and easy-to-implement solutions to address topics relevant to children of all ages. A must-read for parents and educators, Teaching Kids to Think will help you understand where this sense of entitlement comes from—and how to turn it around in order to raise children who are confident, independent, and thoughtful.

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

A True Financial Thriller

The Untold Story of Abraham Lincoln and Mary Todd

Answering the Call

#Crime

The Seventh Sense

Dark Commerce

Stuxnet and the Launch of the World's First Digital Weapon

This student-friendly text provides a comprehensive and unique view into the world of women interacting with the criminal justice system. Authors Stacy L. Mallicoat and Connie explore key topics on women as victims, offenders, and criminal justice workers as they interact with various areas in criminal justice. They investigate relevant subjects that are not found in many traditional texts, including women who work as victim advocates, and international issues of crime and justice for women. They highlight important discussions such as rape in the military or the Girls Scouts Beyond Bars program, and offer case studies on well-known offenders such as Mary Kay Letourneau and Andrea Yates. The text also provides a unique vignette on the story of Karla and Diana, two childhood friends whose lives take a dramatic turn throughout different aspects of the criminal justice system. This vignette, a composite of many subjects and case studies from the authors' research and field experiences, highlights many of the major concepts for each chapter.

Profiles computer hackers who overstep ethical boundaries and break the law to penetrate society's most sensitive computer networks.

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.

Harry Markopolos and his team of financial sleuths discuss first-hand how they cracked the Madoff Ponzi scheme No One Would Listen is the thrilling story of how the Harry Markopolos, a little-known number cruncher from a Boston equity derivatives firm, and his investigative team uncovered Bernie Madoff's scam years before it made headlines, and how they desperately tried to warn the government, the industry, and the financial press. Page by page, Markopolos details his pursuit of the greatest financial criminal in history, and reveals the massive fraud, governmental incompetence, and criminal collusion that has changed thousands of lives forever-as well as the world's financial system. The only book to tell the story of Madoff's scam and the SEC's failings by those who saw both first hand Describes how Madoff was enabled by investors and fiduciaries alike Discusses how the SEC missed the red flags raised by Markopolos Despite repeated written and verbal warnings to the SEC by Harry Markopolos, Bernie Madoff was allowed to continue his operations. No One Would Listen paints a vivid portrait of Markopolos and his determined team of financial sleuths, and what impact Madoff's scam will have on financial markets and regulation for decades to come.

Fabric of a Nation

Outlaws and Hackers on the Computer Frontier, Revised

CUCKOO'S EGG

Everything Is Connected, Everyone Is Vulnerable and What We Can Do About It

Global Innovation Management

Beautiful Security

Why Don't You Like Me?

In 2014, College Board rolled out a new AP® U.S. History course, which centered less on memorizing content and more on developing skills. Since then, the course has been modified here and there, but very little has changed in AP® textbooks--content is still king. Until now. Fabric of a Nation is the first book to truly embrace this dramatic shift in the AP® course and in how history is taught. Built from the ground up by long-time AP® leaders Jason Stacy and Matthew Ellington, this book offers a new approach to AP® US History by seamlessly integrating: A brief historical narrative AP® skills practice Primary source documents Exact alignment to the AP® course Now, that's revolutionary!

"A memoir from Ta-Nehisi Coates, in which he details the challenges on the streets and within one's family, especially the eternal struggle for peace between a father and son and the important role family plays in such circumstances"--

NEW YORK TIMES and WALL STREET JOURNAL BESTSELLER ONE OF THE WASHINGTON POST'S 10 BEST BOOKS OF 2015 One of the world's leading authorities on global security, Marc Goodman takes readers deep into the digital underground to expose the alarming ways criminals, corporations, and even countries are using new and emerging technologies against you—and how this makes everyone more vulnerable than ever imagined. Technological advances have benefited our world in immeasurable ways, but there is an ominous flip side: our technology can be turned against us. Hackers can activate baby monitors to spy on families, thieves are analyzing social media posts to plot home invasions, and stalkers are exploiting the GPS on smart phones to track their victims' every move. We all know today's criminals can steal identities, drain online bank accounts, and wipe out computer servers, but that's just the beginning. To date, no computer has been created that could not be hacked—a sobering fact given our radical dependence on these machines for everything from our nation's power grid to air traffic control to financial services. Yet, as ubiquitous as technology seems today, just over the horizon is a tidal wave of scientific progress that will leave our heads spinning. If today's Internet is the size of a golf ball, tomorrow's will be the size of the sun. Welcome to the Internet of Things, a living, breathing, global information grid where every physical object will be online. But with greater connections come greater risks. Implantable medical devices such as pacemakers can be hacked to deliver a lethal jolt of electricity and a car's brakes can be disabled at high speed from miles away. Meanwhile, 3-D printers can produce AK-47s, bioterrorists can download the recipe for Spanish flu, and cartels are using fleets of drones to ferry drugs across borders. With explosive insights based upon a career in law enforcement and counterterrorism, Marc Goodman takes readers on a vivid journey through the darkest recesses of the Internet. Reading like science fiction, but based in science fact, Future Crimes explores how bad actors are primed to hijack the technologies of tomorrow, including robotics, synthetic biology, nanotechnology, virtual reality, and artificial intelligence. These fields hold the power to create a world of unprecedented abundance and prosperity. But the technological bedrock upon which we are building our common future is deeply unstable and, like a house of cards, can come crashing down at any moment. Future Crimes provides a mind-blowing glimpse into the dark side of technological innovation and the unintended consequences of our connected world. Goodman offers a way out with clear steps we must take to survive the progress unfolding before us. Provocative, thrilling, and ultimately empowering, Future Crimes will serve as an urgent call to action that shows how we can take back control over our own devices and harness technology's tremendous power for the betterment of humanity—before it's too late.

Jonathan Lusthaus lifts the veil on cybercriminals in the most extensive account yet of the lives they lead and the vast international industry they have created. Having traveled to hotspots around the world to meet with hundreds of law enforcement agents, security gurus, hackers, and criminals, he charts how this industry based on anonymity works.

Kingpin

The Art of Intrusion

The SAGE Encyclopedia of Surveillance, Security, and Privacy

An Introduction to Solving Crimes in Cyberspace

Industry of Anonymity

Correlates, Causes, and Context

The Heartbeat of Wounded Knee

Top cybersecurity journalist Kim Zetter tells the story behind the virus that sabotaged Iran's nuclear efforts and shows how its existence has ushered in a new age of warfare—one in which a digital attack can have the same destructive capability as a megaton bomb. In January 2010, inspectors with the International Atomic Energy Agency noticed that centrifuges at an Iranian uranium enrichment plant were failing at an unprecedented rate. The cause was a complete mystery—apparently as much to the technicians replacing the centrifuges as to the inspectors observing them. Then, five months later, a seemingly unrelated event occurred: A computer security firm in Belarus was called in to troubleshoot some computers in Iran that were crashing and rebooting repeatedly. At first, the firm's programmers believed the malicious code on the machines was a simple, routine piece of malware. But as they and other experts around the world investigated, they discovered a mysterious virus of unparalleled complexity. They had, they soon learned, stumbled upon the world's first digital weapon. For Stuxnet, as it came to be known, was unlike any other virus or worm built before: Rather than simply hijacking targeted computers or stealing information from them, it escaped the digital realm to wreak actual, physical destruction on a nuclear facility. In these pages, Wired journalist Kim Zetter draws on her extensive sources and expertise to tell the story behind Stuxnet's planning, execution, and discovery, covering its genesis in the corridors of Bush's White House and its unleashing on systems in Iran—and telling the spectacular, unlikely tale of the security geeks who managed to unravel a sabotage campaign years in the making. But Countdown to Zero Day ranges far beyond Stuxnet itself. Here, Zetter shows us how digital warfare developed in the US. She takes us inside today's flourishing zero-day "grey markets," in which intelligence agencies and militaries pay huge sums for the malicious code they need to carry out infiltrations and attacks. She reveals just how vulnerable many of our own critical systems are to Stuxnet-like strikes, from nation-state adversaries and anonymous hackers alike—and shows us just what might happen should our infrastructure be targeted by such an attack. Propelled by Zetter's unique knowledge and access, and filled with eye-opening explanations of the technologies involved, Countdown to Zero Day is a comprehensive and prescient portrait of a world at the edge of a new kind of war.

"This book uncovers and explains how surveillance has come to be an integral part of how our contemporary society operates worldwide and how it impacts our security and privacy. It explores all types of surveillance, including political, security, corporate, and economic, at all levels of social structure, from the personal to the political to the economic to the judicial."--

Shortlisted for the Orwell Prize and the CWA Gold Dagger for Non-Fiction Award The benefits of living in a digital, globalised society are enormous; so too are the dangers. The world has become a law enforcer's nightmare and every criminal's dream. We bank online, shop online, date, learn, work and live online. But have the institutions that keep us safe on the streets learned to protect us in the burgeoning digital world? Have we become complacent about our personal security -- sharing our thoughts, beliefs and the details of our daily lives with anyone who cares to relieve us of them? In this fascinating and compelling book, Misha Glenny, author of the international bestseller McMafia, explores the three fundamental threats facing us in the twenty-first century: cyber crime, cyber warfare and cyber industrial espionage. Governments and the private sector are losing billions of dollars each year, fighting an ever-morphing, often invisible, and highly intelligent new breed of criminal: the hacker. Glenny has travelled and trawled the world. And by exploring the rise and fall of the criminal website, DarkMarket, he has uncovered the most vivid, alarming and illuminating stories. Whether JiLsi or Matrix, Iceman, Master Splynter or Lord Cyric; whether Detective Sergeant Chris Dawson in Bolton or Agent Keith Mularski in Pittsburgh, Glenny has tracked down and interviewed all the players -- the criminals, the geeks, the police, the security experts and the victims -- and he places everyone and everything in a rich brew of politics, economics and history. The result is simply unputdownable. DarkMarket is authoritative and completely engrossing. It's a must-read for everyone who uses a computer: the essential crime book for our times.

Organizations around the world are in a struggle for survival, racing to transform themselves in a herculean effort to adapt to the digital age, all while protecting themselves from headline-grabbing cybersecurity threats. As organizations succeed or fail, the centrality and importance of cybersecurity and the role of the CISO—Chief Information Security Officer—becomes ever more apparent. It's becoming clear that the CISO, which began as a largely technical role, has become nuanced, strategic, and a cross-functional leadership position. Fight Fire with Fire: Proactive Cybersecurity Strategies for Today's Leaders explores the evolution of the CISO's responsibilities and delivers a blueprint to effectively improve cybersecurity across an organization. Fight Fire with Fire draws on the deep experience of its many all-star contributors. For example: Learn how to talk effectively with the Board from engineer-turned-executive Marianne Bailey, a top spokesperson well-known for global leadership in cyber Discover how to manage complex cyber supply chain risk with Terry Roberts, who addresses this complex area using cutting-edge technology and emerging standards Tame the exploding IoT threat landscape with Sonia Arista, a CISO with decades of experience across sectors, including healthcare where edge devices monitor vital signs and robots perform surgery These are just a few of the global trailblazers in cybersecurity who have banded together to equip today's leaders to protect their enterprises and inspire tomorrow's leaders to join them. With fires blazing on the horizon, there is no time for a seminar or boot camp. Cyber leaders need information at their fingertips. Readers will find insight on how to close the diversity and skills gap and become well-versed in modern cyber threats, including attacks coming from organized crime and nation-states. This book highlights a three-pronged approach that encompasses people, process, and technology to empower everyone to protect their organization. From effective risk management to supply chain security and communicating with the board, Fight Fire with Fire presents discussions from industry leaders that cover every critical competency in information security. Perfect for IT and information security professionals seeking perspectives and insights they can't find in certification exams or standard textbooks, Fight Fire with Fire is an indispensable resource for everyone hoping to improve their understanding of the realities of modern cybersecurity through the eyes of today's top security leaders.

Proactive Cybersecurity Strategies for Today's Leaders

Amazing Peace

DarkMarket

The true story of Max Butler, the master hacker who ran a billion dollar cyber crime network

Data and Goliath: The Hidden Battles to Collect Your Data and Control Your World

Countdown to Zero Day

A comprehensive look at the world of illicit trade Though mankind has traded tangible goods for millennia, recent technology has changed the fundamentals of trade, in both legitimate and illegal economies. In the past three decades, the most advanced forms of illicit trade have broken with all historical precedents and, as Dark Commerce shows, now operate as if on steroids, tied to computers and social media. In this new world of illicit commerce, which benefits states and diverse participants, trade is impersonal and anonymized, and vast profits are made in short periods with limited accountability to sellers, intermediaries, and purchasers. Louise Shelley examines how new technology, communications, and globalization fuel the exponential growth of dangerous forms of illegal trade—the markets for narcotics and child pornography online, the escalation of sex trafficking through web advertisements, and the sale of endangered species for which revenues total in the hundreds of millions of dollars. The illicit economy exacerbates many of the world's destabilizing phenomena: the perpetuation of conflicts, the proliferation of arms and weapons of mass destruction, and environmental degradation and extinction. Shelley explores illicit trade in tangible goods—drugs, human beings, arms, wildlife and timber, fish, antiquities, and ubiquitous counterfeits—and contrasts this with the damaging trade in cyberspace, where intangible commodities cost consumers and organizations billions as they lose identities, bank accounts, access to computer data, and intellectual property. Demonstrating that illicit trade is a business the global community cannot afford to ignore and must work together to address, Dark Commerce considers diverse ways of responding to this increasing challenge.

With the rise of surveillance technology in the last decade, police departments now have an array of sophisticated tools for tracking, monitoring, even predicting crime patterns. In particular crime mapping, a technique used by the police to monitor crime by the neighborhoods in their geographic regions, has become a regular and relied-upon feature of policing. Many claim that these technological developments played a role in the crime drop of the 1990s, and yet no study of these techniques and their relationship to everyday

police work has been made available. Noted scholar Peter K. Manning spent six years observing three American police departments and two British constabularies in order to determine what effects these kinds of analytic tools have had on modern police management and practices. While modern technology allows the police to combat crime in sophisticated, detail-oriented ways, Manning discovers that police strategies and tactics have not been altogether transformed as perhaps would be expected. In The Technology of Policing, Manning untangles the varying kinds of complex crime-control rhetoric that underlie much of today's police department discussion and management, and provides valuable insight into which are the most effective—and which may be harmful—in successfully tracking criminal behavior. The Technology of Policing offers a new understanding of the changing world of police departments and information technology's significant and undeniable influence on crime management.

Building an Effective Security Program provides readers with a comprehensive approach to securing the IT systems in use at their organizations. This book provides information on how to structure and operate an effective cybersecurity program that includes people, processes, technologies, security awareness, and training. This program will establish and maintain effective security protections for the confidentiality, availability, and integrity of organization information. In this book, the authors take a pragmatic approach to building organization cyberdefenses that are effective while also remaining affordable. This book is intended for business leaders, IT professionals, cybersecurity personnel, educators, and students interested in deploying real-world cyberdefenses against today's persistent and sometimes devastating cyberattacks. It includes detailed explanation of the following IT security topics: IT Security Mindset—Think like an IT security professional, and consider how your IT environment can be defended against potential cyberattacks. Risk Management—Identify the assets, vulnerabilities and threats that drive IT risk, along with the controls that can be used to mitigate such risk. Effective Cyberdefense—Consider the components of an effective organization cyberdefense to successfully protect computers, devices, networks, accounts, applications and data. Cyber Operations—Operate cyberdefense capabilities and controls so that assets are protected, and intruders can be detected and repelled before significant damage can be done. IT Security Awareness and Training—Promote effective cybersecurity practices at work, on travel, and at home, among your organization's business leaders, IT professionals, and staff. Resilient IT Security—Implement, operate, monitor, assess, and improve your cybersecurity program on an ongoing basis to defend against the cyber threats of today and the future.

Hacker extraordinaire Kevin Mitnick delivers the explosive encore to his bestselling The Art of Deception Kevin Mitnick, the world's most celebrated hacker, now devotes his life to helping businesses and governments combat data thieves, cybervandals, and other malicious computer intruders. In his bestselling The Art of Deception, Mitnick presented fictionalized case studies that illustrated how savvy computer crackers use "social engineering" to compromise even the most technically secure computer systems. Now, in his new book, Mitnick goes one step further, offering hair-raising stories of real-life computer break-ins-and showing how the victims could have prevented them. Mitnick's reputation within the hacker community gave him unique credibility with the perpetrators of these crimes, who freely shared their stories with him-and whose exploits Mitnick now reveals in detail for the first time, including: A group of friends who won nearly a million dollars in Las Vegas by reverse-engineering slot machines Two teenagers who were persuaded by terrorists to hack into the Lockheed Martin computer systems Two convicts who joined forces to become hackers inside a Texas prison A "Robin Hood" hacker who penetrated the computer systems of many prominent companies-andthen told them how he gained access With riveting "you are there" descriptions of real computer break-ins, indispensable tips on countermeasures security professionals need to implement now, and Mitnick's own acerbic commentary on the crimes he describes, this book is sure to reach a wide audience-and attract the attention of both law enforcement agencies and the media.

A Little History of the Australian Labor Party

Spam Kings

Worm

Cyberpunk

Dawn of the Code War

The First Digital World War

Teaching Kids to Think

Although most people don't give security much attention until their personal or business systems are attacked, this thought-provoking anthology demonstrates that digital security is not only worth thinking about, it's also a fascinating topic. Criminals succeed by exercising enormous creativity, and those defending against them must do the same. Beautiful Security explores this challenging subject with insightful essays and analysis on topics that include: The underground economy for personal information: how it works, the relationships among criminals, and some of the new ways they pounce on their prey How social networking, cloud computing, and other popular trends help or hurt our online security How metrics, requirements gathering, design, and law can take security to a higher level The real, little-publicized history of PGP This book includes contributions from: Peiter "Mudge" Zatko Jim Stickley Elizabeth Nichols Chenxi Wang Ed Bellis Ben Edelman Phil Zimmermann and Jon Callas Kathy Wang Mark Curphey John McManus James Routh Randy V. Sabett Anton Chuvakin Grant Geyer and Brian Dunphy Peter Wayner Michael Wood and Fernando Francisco All royalties will be donated to the Internet Engineering Task Force (IETF).

When a giant wave destroys his village, Mau is the only one left. Daphne—a traveler from the other side of the globe—is the sole survivor of a shipwreck. Separated by language and customs, the two are united by catastrophe. Slowly, they are joined by other refugees. And as they struggle to protect the small band, Mau and Daphne defy ancestral spirits, challenge death himself, and uncover a long-hidden secret that literally turns the world upside down.

“Bruce Schneier’s amazing book is the best overview of privacy and security ever written.”—Clay Shirky “Bruce Schneier’s amazing book is the best overview of privacy and security ever written.”—Clay Shirky Your cell phone provider tracks your location and knows who’s with you. Your online and in-store purchasing patterns are recorded, and reveal if you're unemployed, sick, or pregnant. Your e-mails and texts expose your intimate and casual friends. Google knows what you’re thinking because it saves your private searches. Facebook can determine your sexual orientation without you ever mentioning it. The powers that surveil us do more than simply store this information. Corporations use surveillance to manipulate not only the news articles and advertisements we each see, but also the prices we’re offered. Governments use surveillance to discriminate, censor, chill free speech, and put people in danger worldwide. And both sides share this information with each other or, even worse, lose it to cybercriminals in huge data breaches. Much of this is voluntary: we cooperate with corporate surveillance because it promises us convenience, and we submit to government surveillance because it promises us protection. The result is a mass surveillance society of our own making. But have we given up more than we’ve gained? In Data and Goliath, security expert Bruce Schneier offers another path, one that values both security and privacy. He brings his bestseller up-to-date with a new preface covering the latest developments, and then shows us exactly what we can do to reform government surveillance programs, shake up surveillance-based business models, and protect our individual privacy. You'll never look at your phone, your computer, your credit cards, or even your car in the same way again.

The inside story of how America's enemies launched a cyber war against us-and how we've learned to fight back With each passing year, the internet-linked attacks on America's interests have grown in both frequency and severity. Overmatched by our military, countries like North Korea, China, Iran, and Russia have found us vulnerable in cyberspace. The "Code War" is upon us. In this dramatic book, former Assistant Attorney General John P. Carlin takes readers to the front lines of a global but little-understood fight as the Justice Department and the FBI chases down hackers, online terrorist recruiters, and spies. Today, as our entire economy goes digital, from banking to manufacturing to transportation, the potential targets for our enemies multiply. This firsthand account is both a remarkable untold story and a warning of dangers yet to come.

The Real Story Behind the High-Rolling Hucksters Pushing Porn, Pills, and %*@)# Enlargements

A Christmas Poem

The Inside Story of Brexit

Inside the Business of Cybercrime

An American Marriage

Spam Nation

Future Crimes

An enlightening narrative exploring an oft-overlooked aspect of the sixteenth president's life, An American Marriage reveals the tragic story of Abraham Lincoln's marriage to Mary Todd. Abraham Lincoln was apparently one of those men who regarded “connubial bliss” as an untenable fantasy. During the Civil War, he pardoned a Union soldier who had deserted the army to return home to wed his sweetheart. As the president signed a document sparing the soldier's life, Lincoln said: “I want to punish the young man—probably in less than a year he will wish I had withheld the pardon.” Based on thirty years of research, An American Marriage describes and analyzes why Lincoln had good reason to regret his marriage to Mary Todd. This revealing narrative shows that, as First Lady, Mary Lincoln accepted bribes and kickbacks, sold permits and pardons, engaged in extortion, and peddled influence. The reader comes to learn that Lincoln wed Mary Todd because, in all likelihood, she seduced him and then insisted that he protect her honor. Perhaps surprisingly, the 5’2” Mrs. Lincoln often physically abused her 6’4” husband, as well as her children and servants; she humiliated her husband in public; she caused him, as president, to fear that she would disgrace him publicly. Unlike her husband, she was not profoundly opposed to slavery and hardly qualifies as the “ardent abolitionist” that some historians have portrayed. While she providid a useful stimulus to his ambition, she often “crushed his spirit,” as his law partner put it. In the end, Lincoln may not have had as successful a presidency as he did—where he showed a preternatural ability to deal with difficult people—if he had not had so much practice at home.

This dazzling Christmas poem by Maya Angelou is powerful and inspiring for people of all faiths. In this beautiful, deeply moving poem, Maya Angelou inspires us to embrace the peace and promise of Christmas, so that hope and love can once again light up our holidays and the world. “Angels and Mortals, Believers and Nonbelievers, look heavenward,” she writes, “and speak the word aloud. Peace.” Read by the poet at the lighting of the National Christmas Tree at the White House on December 1, 2005, Maya Angelou’ s celebration of the “Glad Season” is a radiant affirmation of the goodness of life.

FINALIST FOR THE 2019 NATIONAL BOOK AWARD LONGLISTED FOR THE 2020 ANDREW CARNEGIE MEDAL FOR EXCELLENCE A NEW YORK TIMES BESTSELLER Named a best book of 2019 by The New York Times, TIME, The Washington Post, NPR, Hudson Booksellers, The New York Public Library, The Dallas Morning News, and Library Journal. "Chapter after chapter, it's like one shattered myth after another." - NPR "An informed, moving and kaleidoscopic portrait... Treuer's powerful book suggests the need for soul-searching about the meanings of American history and the stories we tell ourselves about this nation's past.." - New York Times Book Review, front page A sweeping history—and counter-narrative—of Native American life from the Wounded Knee massacre to the present. The received idea of Native American history—as promulgated by books like Dee Brown's mega-bestselling 1970 Bury My Heart at Wounded Knee—has been that American Indian history essentially ended with the 1890 massacre at Wounded Knee. Not only did one hundred fifty Sioux die at the hands of the U. S. Cavalry, the sense was, but Native civilization did as well. Growing up Ojibwe on a reservation in Minnesota, training as an anthropologist, and researching Native life past and present for his nonfiction and novels, David Treuer has uncovered a different narrative. Because they did not disappear—and not despite but rather because of their intense struggles to preserve their language, their traditions, their families, and their very existence—the story of American Indians since the end of the nineteenth century to the present is one of unprecedented resourcefulness and reinvention. In The Heartbeat of Wounded Knee, Treuer melds history with reportage and memoir. Tracing the tribes' distinctive cultures from first contact, he explores how the depredations of each era spawned new modes of survival. The devastating seizures of land gave rise to increasingly sophisticated legal and political maneuvering that put the lie to the myth that Indians don't know or care about property. The forced assimilation of their children at government-run boarding schools incubated a unifying Native identity. Conscription in the US military and the pull of urban life brought Indians into the mainstream and modern times, even as it steered the emerging shape of self-rule and spawned a new generation of resistance. The Heartbeat of Wounded Knee is the essential, intimate story of a resilient people in a transformative era.

“Jones, a trailblazing African American judge, delivers an urgently needed perspective on American history . . . [A] passionate and informative account” (Booklist, starred review). Answering the Call is an extraordinary eyewitness account from an unsung hero of the battle for racial equality in America—a battle that, far from ending with the great victories of the civil rights era, saw some of its signal achievements in the desegregation fights of the 1970s and its most notable setbacks in the affirmative action debates that continue into the present in Ferguson, Baltimore, and beyond. Judge Nathaniel R. Jones's groundbreaking career was forged in the 1960s: As the first African American assistant US attorney in Ohio; as assistant general counsel of the Kerner Commission; and, beginning in 1969, as general counsel of the NAACP. In that latter role, Jones coordinated attacks against Northern school segregation—a vital, divisive, and poorly understood chapter in the movement for equality—twice arguing in the pivotal US Supreme Court case Bradley v. Milliken, which addressed school desegregation in Detroit. He also led the national response to the attacks against affirmative action, spearheading and arguing many of the signal legal cases of that effort. Answering the Call is “a stunning, inside story of the contemporary struggle for civil rights . . . Essential reading for understanding where we are today—underscoring just how much work is left to be done” (Vernon E. Jordan Jr., civil rights activist). “A forthright testimony by a witness to history.” —Kirkus Reviews

The Inside Story of Organized Cybercrime—from Global Epidemic to Your Front Door

America's Battle Against Russia, China, and the Rising Global Cyber Threat

An Autobiography of the Modern Struggle to End Racial Discrimination in America

Investigating Internet Crimes

Women and Crime