Cybersecurity Leadership Powering The Modern Organization

"The insights ... go beyond cyber security alone to examine the critical concepts and often misunderstood distinction between leadership and management. This should be required reading on every college campus." - Collin Smith, CISSP - Cybersecurity Professional. "...this book will change both the way we think about leadership and the way we understand information technology. I recommend this book highly to everyone." - Eric Schwartz - Executive Director at Advena World LLC and Adjunct Professor in Economics at Montgomery College. "...explains what an organization needs to know to implement cybersecurity governance." Council of Graduate Schools Testimony at the US Senate Appropriations Committee Meeting, April 29, 2014. "...exposes the common faults with which we are all struggling in this industry. It's humorous ... engaging, and I feel helps a reader question their own approaches. I was originally looking for a compendium that works as collateral reading for Cyber Security training courses, and I found it. I genuinely recommend this work tool." - David Bickel - Chief Information Security Officer, Department of Health and Mental Hygiene, State of Maryland. Written by one of the leading global thought leaders in cybersecurity with 30 years of practical experience in the field, this book addresses the most neglected area of cybersecurity -- cybersecurity governance -- the management, leadership, and engagement of people for the purposes of cybersecurity. This book is an essential book for anyone interested in understanding how cybersecurity should be led in an organization. All business executives or students at any level will benefit from this book. Cybersecurity can be a source of productivity and innovation and be a revenue driver. The leadership principles are applicable in any field and in any organization.

As one review on cybersecurity-professionals.com sums up:"If you are ready to make a fundamental change to the way you operate, that will save you money yet allow you to achieve so much more, this book is a must read!"Information Security spending is skyrocketing, both in absolute terms and as a percentage of IT spending. It seems the only thing increasing faster is the frequency and impact of breaches. It doesn't seem like the current approach is working very well, does it? Interestingly, the bulk of large breaches is caused by simple issues for which we've had the answers for decades, yet no one spotted. The answer, according to the nearly $250bn Information Security industry, is to spend more on technologies and services. Is it perhaps time to take a step back, shed our indoctrination, and have a fresh look at things?Greg van der Gaast started as one of the most notorious hackers of the late 1990's. He is now the Head of Information Security for the University of Salford, Managing Director of InfoSec Strategy consultancy CMCG, and a university lecturer and private trainer in Information Security leadership. He also is a frequent speaker on making security more human, accountable, and proactive. A candid critic of the security status quo, he is considered a nutter by many in the field. Conversely, he's lost count of how many management teams have told him he was the first security guy to ever make sense to them. Who's crazy? You decide.Rethinking InfoSec presents views on what causes many of today's issues and costs and thoughts on how we can create a lot more assurance with far, far less.Some of the topics covered:-Strategically implement effective InfoSec programmes.-Boost business alignment, collaboration, and buy-in.-Simplify and achieve assurance and compliance.-Ensure holistic coverage.-Avoid costly reactive approaches.-Reduce issues through proactivity.-Establish brand and influence.-Structure teams for maximum effectiveness.-Leverage human potential.Reduce information security pressure, stress, and spending, all while increasing assurance and reward. We can do better, lets.

Countering Cyber Sabotage: Introducing Consequence-Driven, Cyber-Informed Engineering (CCE) introduces a new methodology to help critical infrastructure owners, operators and their security practitioners make demonstrable improvements in securing their most important functions and processes. Current best practice approaches to cyber defense struggle to stop targeted attackers from creating potentially catastrophic results. From a national security perspective, it is not just the damage to the military, the economy, or essential critical infrastructure companies that is a concern. It is the cumulative, downstream effects from potential regional blackouts, military mission kills, transportation stoppages, water delivery or treatment issues, and so on. CCE is a validation that engineering first principles can be applied to the most important cybersecurity challenges and in so doing, protect organizations in ways current approaches do not. The most pressing threat is cyber-enabled sabotage, and CCE begins with the assumption that well-resourced, adaptive adversaries are already in and have been for some time, undetected and perhaps undetectable. Chapter 1 recaps the current and near-future states of digital technologies in critical infrastructure and the implications of our near-total dependence on them. Chapters 2 and 3 describe the origins of the methodology and set the stage for the more in-depth examination that follows. Chapter 4 describes how to prepare for an engagement, and chapters 5-8 address each of the four phases. The CCE phase chapters take the reader on a more granular walkthrough of the methodology with examples from the field, phase objectives, and the steps to take in each phase. Concluding chapter 9 covers training options and looks towards a future where these concepts are scaled more broadly.

Cyber Risk Leaders: Global C-Suite Insights - Leadership and Influence in the Cyber Age’, by Shamane Tan - explores the art of communicating with executives, tips on navigating through corporate challenges, and reveals what the C-Suite looks for in professional partners. For those who are interested in learning from top industry leaders, or an aspiring or current CISO, this book is gold for your career. It’s the go-to book and your CISO kit for the season.

Passwords are not the problem. The management of passwords is the real security nightmare. User authentication is the most ignored risk to enterprise cybersecurity. When end users are allowed to generate, know, remember, type and manage their own passwords, IT has inadvertently surrendered the job title Network Security Manager to employees - the weakest link in the cybersecurity chain. Dovell Bonnett reveals the truth about the elephant in the room that no one wants to mention: Expensive backend security is

worthless when the virtual front door has a lousy lock! Dovell proves that making passwords secure is not only possible, passwords can actually become an effective, cost efficient and user friendly feature of robust cybersecurity. After examining how encryption keys are secured, this book introduces a new strategy called Password Authentication Infrastructure (PAI) that rivals digital certificates. Passwords are not going away. What needs to be fixed is how passwords are managed.

Cyber Attacks, Student Edition, offers a technical, architectural, and management approach to solving the problems of protecting national infrastructure. This approach includes controversial themes such as the deliberate use of deception to trap intruders. This volume thus serves as an attractive framework for a new national strategy for cyber security. A specific set of criteria requirements allows any organization, such as a government agency, to integrate the principles into their local environment. In this edition, each principle is presented as a separate security strategy and illustrated with compelling examples. The book adds 50-75 pages of new material aimed specifically at enhancing the student experience and making it more attractive for instructors teaching courses such as cyber security, information security, digital security, national security, intelligence studies, technology and infrastructure protection. It now also features case studies illustrating actual implementation scenarios of the principles and requirements discussed in the text, along with a host of new pedagogical elements, including chapter outlines, chapter summaries, learning checklists, and a 2-color interior. Furthermore, a new and complete ancillary package includes test bank, lesson plans, PowerPoint slides, case study questions, and more. This text is intended for security practitioners and military personnel as well as for students wishing to become security engineers, network operators, software designers, technology managers, application developers, etc. Provides case studies focusing on cyber security challenges and solutions to display how theory, research, and methods, apply to real-life challenges Utilizes, end-of-chapter case problems that take chapter content and relate it to real security situations and issues Includes instructor slides for each chapter as well as an instructor’s manual with sample syllabi and test bank

Rootkits and Bootkits will teach you how to understand and counter sophisticated, advanced threats buried deep in a machine’s boot process or UEFI firmware. With the aid of numerous case studies and professional research from three of the world’s leading security experts, you’ll trace malware development over time from rootkits like TDL3 to present-day UEFI implants and examine how they infect a system, persist through reboot, and evade security software. As you inspect and dissect real malware, you’ll learn: • How Windows boots—including 32-bit, 64-bit, and UEFI mode—and where to find vulnerabilities • The details of boot process security mechanisms like Secure Boot, including an overview of Virtual Secure Mode (VSM) and Device Guard • Reverse engineering and forensic techniques for analyzing real malware, including bootkits like Rovnix/Carberp, Gapz, TDL4, and the infamous rootkits TDL3 and Festi • How to perform static and dynamic analysis using emulation and tools like Bochs and IDA Pro • How to better understand the delivery stage of threats against BIOS and UEFI firmware in order to create detection capabilities • How to use virtualization tools like VMware Workstation to reverse engineer bootkits and the Intel Chipsec tool to dig into forensic analysis Cybercrime syndicates and malicious actors will continue to write ever more persistent and covert attacks, but the game is not lost. Explore the cutting edge of malware analysis with Rootkits and Bootkits. Covers boot processes for Windows 32-bit and 64-bit operating systems.

Cybersecurity experts from across industries and sectors share insights on how to think like scientists to master cybersecurity challenges Humankind’s efforts to explain the origin of the cosmos birthed disciplines such as physics and chemistry. Scientists conceived of the cosmic ‘Big Bang’ as an explosion of particles—everything in the universe centered around core elements and governed by laws of matter and gravity. In the modern era of digital technology, we are experiencing a similar explosion of ones and zeros, an exponentially expanding universe of bits of data centered around the core elements of speed and connectivity. One of the disciplines to emerge from our efforts to make sense of this new universe is the science of cybersecurity. Cybersecurity is as central to the Digital Age as physics and chemistry were to the Scientific Age. The Digital Big Bang explores current and emerging knowledge in the field of cybersecurity, helping readers think like scientists to master cybersecurity principles and overcome cybersecurity challenges. This innovative text adopts a scientific approach to cybersecurity, identifying the science’s fundamental elements and examining how these elements intersect and interact with each other. Author Phil Quade distills his over three decades of cyber intelligence, defense, and attack experience into an accessible, yet detailed, single-volume resource. Designed for non-specialist business leaders and cybersecurity practitioners alike, this authoritative book is packed with real-world examples, techniques, and strategies no organization should be without. Contributions from many of the world’s leading cybersecurity experts and policymakers enable readers to firmly grasp vital cybersecurity concepts, methods, and practices. This important book: Guides readers on both fundamental tactics and advanced strategies Features observations, hypotheses, and conclusions on a wide range of cybersecurity issues Helps readers work with the central elements of cybersecurity, rather than fight or ignore them Includes content by cybersecurity leaders from organizations such as Microsoft, Target, ADP, Capital One, Verisign, AT&T, Samsung, and many others Offers insights from national-level security experts including former Secretary of Homeland Security Michael Chertoff and former Director of National Intelligence Mike McConnell The Digital Big Bang is an invaluable source of information for anyone faced with the challenges of 21st century cybersecurity in all industries and sectors, including business leaders, policy makers, analysts and researchers as well as IT professionals, educators, and students.

Cybersecurity LeadershipPowering the Modern Organization; Black and White EditionCreateSpace

From data security company Code42, Inside Jobs offers companies of all sizes a new way to secure today’s collaborative cultures—one that works without compromising sensitive company data or slowing business down. Authors Joe Payne, Jadee Hanson, and Mark Wojtasiak, seasoned veterans in the cybersecurity space, provide a top-down

and bottom-up picture of the rewards and perils involved in running and securing organizations focused on rapid, iterative, and collaborative innovation. Modern day data security can no longer be accomplished by “Big Brother” forms of monitoring or traditional prevention solutions that rely solely on classification and blocking systems. These technologies frustrate employees, impede collaboration, and force productivity work-arounds that risk the very data you need to secure. They provide the illusion that your trade secrets, customer lists, patents, and other intellectual property are protected. That couldn’t be farther from the truth, as insider threats continue to grow. These include: Well-intentioned employees inadvertently sharing proprietary data Departing employees taking your trade secrets with them to the competition A high-risk employee moving source code to an unsanctioned cloud service What’s the solution? It’s not the hunt for hooded, malicious wrongdoers that you might expect. The new world of data security is built on security acting as an ally versus an adversary. It assumes positive intent, creates organizational transparency, establishes acceptable data use policies, increases security awareness, and provides ongoing training. Whether you are a CEO, CIO, CISO, CHRO, general counsel, or business leader, this book will help you understand the important role you have to play in securing the collaborative cultures of the future.

These proceedings represent the work of researchers participating in the 13th International Conference on Cyber Warfare and Security (ICCWS 2018) which is being hosted this year by the National Defense University in Washington DC, USA on 8-9 March 2018.

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.

In a world of several billion people we are a supply of one! We must find the unique gifts we have inside, polish them, showcase them, and monetize them for multiple customers all over the world.

We know why diversity is important, but how do we drive real change at work? Diversity and inclusion expert Jennifer Brown provides a step-by-step guide for the personal and emotional journey we must undertake to create an inclusive workplace where everyone can thrive. Human potential is unleashed when we feel like we belong. That's why inclusive workplaces experience higher engagement, performance, and profits. But the reality is that many people still feel unable to bring their true selves to work. In a world where the talent pool is becoming increasingly diverse, it's more important than ever for leaders to truly understand how to support inclusion. Drawing on years of work with many leading organizations, Jennifer Brown shows what leaders at any level can do to spark real change. She guides readers through the Inclusive Leader Continuum, a set of four developmental stages: unaware, aware, active, and advocate. Brown describes the hallmarks of each stage, the behaviors and mind-sets that inform it, and what readers can do to keep progressing. Whether you're a powerful CEO or a new employee without direct reports, there are actions you can take that can drastically change the day-to-day reality for your colleagues and the trajectory of your organization. Anyone can—and should—be an inclusive leader. Brown lays out simple steps to help you understand your role, boost your self-awareness, take action, and become a better version of yourself in the process. This book will meet you where you are and provide a road map to create a workplace of greater mutual understanding where everyone's talents can shine.

Todd Fitzgerald, co-author of the ground-breaking (ISC)2 CISO Leadership: Essential Principles for Success, Information Security Governance Simplified: From the Boardroom to the Keyboard, co-author for the E-C Council CISO Body of Knowledge, and contributor to many others including Official (ISC)2 Guide to the CISSP CBK, COBIT 5 for Information Security, and ISACA CSX Cybersecurity Fundamental Certification, is back with this new book incorporating practical experience in leading, building, and sustaining an information security/cybersecurity program. CISO COMPASS includes personal, pragmatic perspectives and lessons learned of over 75 award-winning CISOs, security leaders, professional association leaders, and cybersecurity standard setters who have fought the tough battle. Todd has also, for the first time, adapted the McKinsey 7S framework (strategy, structure, systems, shared values, staff, skills and style) for organizational effectiveness to the practice of leading cybersecurity to structure the content to ensure comprehensive coverage by the CISO and security leaders to key issues impacting the delivery of the cybersecurity strategy and demonstrate to the Board of Directors due diligence. The insights will assist the security leader to create programs appreciated and supported by the organization, capable of industry/ peer award-winning recognition, enhance cybersecurity maturity, gain confidence by senior management, and avoid pitfalls. The book is a comprehensive, soup-to-nuts book enabling security leaders to effectively protect information assets and build award-winning programs by covering topics such as developing cybersecurity strategy, emerging trends and technologies, cybersecurity organization structure and reporting models, leveraging current incidents, security control frameworks, risk management, laws and regulations, data protection and privacy, meaningful policies and procedures, multi-generational workforce team dynamics, soft skills, and communicating with the Board of Directors and executive management. The book is valuable to current and future security leaders as a valuable resource and an integral part of any college program for information/ cybersecurity.

Caught in the crosshairs of “Leadership” and “Information Technology”, Information Security professionals are increasingly tapped to operate as business executives. This often puts them on a career path they did not expect, in a field not yet clearly defined. IT training does not usually includemanagerial skills such as leadership, team-building, communication, risk assessment, and corporate business savvy, needed by CISOs. Yet a lack in any of these areas can short circuit a career in information security. CISO Leadership: Essential Principles for Success captures years of hard knocks, success stories, and yes, failures. This is not a how-to book or a collection of technical data. It does not cover products or technology or provide a recapitulation of the common body of knowledge. The book delineates information needed by security leaders and includes from-the-trenches advice on how to have a successful career in the field. With a stellar panel of contributors including William H. Murray, Harry Demaio, James Christiansen, Randy Sanovic, Mike Corby, Howard Schmidt, and other thought leaders, the book brings together the collective experience of trail blazers. The authors have learned through experience—been there, done that, have the t-shirt—and yes, the scars. A glance through the contents demonstrates the breadth and depth of coverage, not only in topics included but also in expertise provided by the chapter authors. They are the pioneers, who, while initially making it up as they went along, now provide the next generation of information security professionals with a guide to success.

Rely on this practical, end-to-end guide on cyber safety and online security written expressly for a non-technical audience. You will have just what you need to protect yourself—step by step, without judgment, and with as little jargon as possible. Just how secure is your computer right now? You probably don't really know. Computers and the Internet have revolutionized the modern world, but if you're like most people, you have no clue how these things work and don't know the real threats. Protecting your computer is like defending a medieval castle. While moats, walls, drawbridges, and castle guards can be effective, you'd go broke trying to build something dragon-proof. This book is not about protecting yourself from a targeted attack by the NSA; it's about armoring yourself against common hackers and mass surveillance. There are dozens of no-brainer things we all should be doing to protect our computers and safeguard our data—just like wearing a seat belt, installing smoke alarms, and putting on sunscreen. Author Carey Parker has structured this book to give you maximum benefit with minimum effort. If you just want to know what to do, every chapter has a complete checklist with step-by-step instructions and pictures. The book contains more than 150 tips to make you and your family safer. It includes: Added steps for Windows 10 (Spring 2018) and Mac OS X High Sierra Expanded coverage on mobile device safety Expanded coverage on safety for kids online More than 150 tips with complete step-by-step instructions and pictures What You’ll Learn Solve your password problems once and for all Browse the web safely and with confidence Block online tracking and dangerous ads Choose the right antivirus software for you Send files and messages securely Set up secure home networking Conduct secure shopping and banking online Lock down social media accounts Create automated backups of all your devices Manage your home computers Use your smartphone and tablet safely Safeguard your kids online And more! Who This Book Is For Those who use computers and mobile devices, but don’t really know (or frankly care) how they work. This book is for people who just want to know what they need to do to protect themselves—step by step, without judgment, and with as little jargon as possible.

This volume represents the 18th International Conference on Information Technology - New Generations (ITNG), 2021. ITNG is an annual event focusing on state of the art technologies pertaining to digital information and communications. The applications of advanced information technology to such domains as astronomy, biology, education, geosciences, security, and health care are the among topics of relevance to ITNG. Visionary ideas, theoretical and experimental results, as well as prototypes, designs, and tools that help the information readily flow to the user are of special interest. Machine Learning, Robotics, High Performance Computing, and Innovative Methods of Computing are examples of related topics. The conference features keynote speakers, a best student award, poster award, service award, a technical open panel, and workshops/exhibits from industry, government and academia. This publication is unique as it captures modern trends in IT with a balance of theoretical and experimental work. Most other work focus either on theoretical or experimental, but not both. Accordingly, we do not know of any competitive literature.

A powerful investigation into a grisly political murder and the authoritarian regime behind it: DO NOT DISTURB upends the narrative that Rwanda sold the world after the deadliest genocide of the twentieth century. We think we know the story of Africa’s Great Lakes region. Following the Rwandan genocide, an idealistic group of young rebels overthrew the brutal regime in Kigali, ushering in an era of peace and stability that made Rwanda the donor darling of the West, winning comparisons with Switzerland and Singapore. But the truth was considerably more sinister. Vividly sourcing her story with direct testimony from key participants, Wrong uses the story of the murder of Patrick Karegeya, once Rwanda’s head of external intelligence and a quicksilver operator of supple charm, to paint the portrait of a modern African dictatorship created in the chilling likeness of Paul Kagame, the president who sanctioned his former friend’s assassination.

Marvin Kalb, a former journalist and Harvard professor, traces how the Crimea of Catherine the Great became a global tinder box. The world was stunned when Vladimir Putin invaded and seized Crimea in March 2014. In the weeks that followed, pro-Russian rebels staged uprisings in southeastern Ukraine. The United States and its Western allies immediately imposed strict sanctions on Russia and whenever possible tried to isolate it diplomatically. This sharp deterioration in East-West relations has raised basic questions about Putin's provocative policies and the future of Russia and Ukraine. Marvin Kalb, who wrote commentaries for Edward R. Murrow before becoming CBS News' Moscow bureau chief in the late 1950's, and who also served as a translator and junior press officer at the US Embassy in Moscow, argues that, contrary to conventional wisdom, Putin did not "suddenly" decide to invade Crimea. He had been waiting for the right moment ever since disgruntled Ukrainians rose in revolt against his pro-Russian regime in Kiev's Maidan Square. These demonstrations led Putin to conclude that Ukraine's opposition constituted an existential threat to Russia. Imperial Gamble examines how Putin reached that conclusion by taking a critical look at the recent political history of post-Soviet Russia. It also journeys deep into Russian and Ukrainian history to explain what keeps them together and yet at the same time drives them apart. Kalb believes that the post-cold war world hangs today on the resolution of the Ukraine crisis. So long as it is treated as a problem to be resolved by Russia, on the one side, and the United States and Europe, on the other, it will remain a danger zone with global consequences. The only sensible solution lies in both Russia and Ukraine recognizing that their futures are irrevocably linked by geography, power, politics, and the history that

Kalb brings to life in Imperial Gamble.

World-renowned economist Klaus Schwab, Founder and Executive Chairman of the World Economic Forum, explains that we have an opportunity to shape the fourth industrial revolution, which will fundamentally alter how we live and work. Schwab argues that this revolution is different in scale, scope and complexity from any that have come before. Characterized by a range of new technologies that are fusing the physical, digital and biological worlds, the developments are affecting all disciplines, economies, industries and governments, and even challenging ideas about what it means to be human. Artificial intelligence is already all around us, from supercomputers, drones and virtual assistants to 3D printing, DNA sequencing, smart thermostats, wearable sensors and microchips smaller than a grain of sand. But this is just the beginning: nanomaterials 200 times stronger than steel and a million times thinner than a strand of hair and the first transplant of a 3D printed liver are already in development. Imagine "smart factories" in which global systems of manufacturing are coordinated virtually, or implantable mobile phones made of biosynthetic materials. The fourth industrial revolution, says Schwab, is more significant, and its ramifications more profound, than in any prior period of human history. He outlines the key technologies driving this revolution and discusses the major impacts expected on government, business, civil society and individuals. Schwab also offers bold ideas on how to harness these changes and shape a better future--one in which technology empowers people rather than replaces them; progress serves society rather than disrupts it; and in which innovators respect moral and ethical boundaries rather than cross them. We all have the opportunity to contribute to developing new frameworks that advance progress.

The New York Times bestseller, now updated with new material on cyber attacks, digital sovereignty, and tech in a pandemic. From Microsoft's president and one of the tech industry's broadest thinkers, a frank and thoughtful reckoning with how to balance enormous promise and existential risk as the digitization of everything accelerates. “A colorful and insightful insiders’ view of how technology is both empowering and threatening us. From privacy to cyberattacks, this timely book is a useful guide for how to navigate the digital future.” —Walter Isaacson Microsoft president Brad Smith operates by a simple core belief: When your technology changes the world, you bear a responsibility to help address the world you have helped create. In Tools and Weapons, Brad Smith and Carol Ann Browne bring us a captivating narrative from the top of Microsoft, as the company flies in the face of a tech sector long obsessed with disruption as an end in itself, and in doing so navigates some of the thorniest issues of our time—from privacy to cyberwar to the challenges for democracy, far and near. As the tumultuous events of 2020 brought technology and Big Tech even further into the lives of almost all Americans, Smith and Browne updated the book throughout to reflect a changed world. With three new chapters on cybersecurity, technology and nation-states, and tech in the pandemic, Tools and Weapons is an invaluable resource from the cockpit of one of the world’s largest tech companies.

"This is the book executives have been waiting for. It is clear: With deep expertise but in nontechnical language, it describes what cybersecurity risks are and the decisions executives need to make to address them. It is crisp: Quick and to the point, it doesn't waste words and won't waste your time. It is candid: There is no sure cybersecurity defense, and Chris Moschovitis doesn't pretend there is; instead, he tells you how to understand your company's risk and make smart business decisions about what you can mitigate and what you cannot. It is also, in all likelihood, the only book ever written (or ever to be written) about cybersecurity defense that is fun to read." —Thomas A. Stewart, Executive Director, National Center for the Middle Market and Co-Author of Woo, Wow, and Win: Service Design, Strategy, and the Art of Customer Delight Get answers to all your cybersecurity questions In 2016, we reached a tipping point—a moment where the global and local implications of cybersecurity became undeniable. Despite the seriousness of the topic, the term "cybersecurity" still exasperates many people. They feel terrorized and overwhelmed. The majority of business people have very little understanding of cybersecurity, how to manage it, and what's really at risk. This essential guide, with its dozens of examples and case studies, breaks down every element of the development and management of a cybersecurity program for the executive. From understanding the need, to core risk management principles, to threats, tools, roles and responsibilities, this book walks the reader through each step of developing and implementing a cybersecurity program. Read cover-to-cover, it’s a thorough overview, but it can also function as a useful reference book as individual questions and difficulties arise. Unlike other cybersecurity books, the text is not bogged down with industry jargon Speaks specifically to the executive who is not familiar with the development or implementation of cybersecurity programs Shows you how to make pragmatic, rational, and informed decisions for your organization Written by a top-flight technologist with decades of experience and a track record of success If you’re a business manager or executive who needs to make sense of cybersecurity, this book demystifies it for you.

Digital leadership has been seen as a phenomenon allowing competitive advantages for organizations, but some studies do not include the risks, benefits, and challenges of this type of leadership. Consequently, the objective of this book is to fill this gap by combining several studies from different perspectives. The various chapters presented here follow several approaches and applications that researchers explore in different contexts. This book intends therefore to add to the body of knowledge in leadership and digital areas. On the other hand, this work shows how digital leadership can stimulate organizational development in various countries and regions worldwide.

Through the rise of big data and the internet of things, terrorist organizations have been freed from geographic and logistical confines and now have more power than ever before to strike the average citizen directly at home. This, coupled with the inherently asymmetrical nature of cyberwarfare, which grants great advantage to the attacker, has created an unprecedented national security risk that both governments and their citizens are woefully ill-prepared to face. Examining cyber warfare and terrorism through a critical and academic perspective can lead to a better understanding of its foundations and implications. Cyber Warfare and Terrorism: Concepts, Methodologies, Tools, and Applications is an essential reference for the latest research on the utilization of online tools by terrorist organizations to communicate with and recruit potential extremists and examines effective countermeasures employed by law enforcement agencies to defend against such threats. Highlighting a range of topics such as cyber threats, digital intelligence, and counterterrorism, this multi-volume book is ideally designed for law enforcement, government officials, lawmakers, security analysts, IT specialists, software developers, intelligence and security practitioners, students, educators, and researchers.

Insights into the true history of cyber warfare, and the strategies, tactics, and cybersecurity tools that can be used to better defend yourself and your organization against cyber threat. Key Features Define and determine a cyber-defence strategy based on current and past real-life examples Understand how future technologies will impact cyber warfare campaigns and society Future-ready yourself and your business against any cyber threat Book Description The era of cyber warfare is now upon us. What we do now and how we determine what we will do in the

future is the difference between whether our businesses live or die and whether our digital self survives the digital battlefield. Cyber Warfare – Truth, Tactics, and Strategies takes you on a journey through the myriad of cyber attacks and threats that are present in a world powered by AI, big data, autonomous vehicles, drones video, and social media. Dr. Chase Cunningham uses his military background to provide you with a unique perspective on cyber security and warfare. Moving away from a reactive stance to one that is forward-looking, he aims to prepare people and organizations to better defend themselves in a world where there are no borders or perimeters. He demonstrates how the cyber landscape is growing infinitely more complex and is continuously evolving at the speed of light. The book not only covers cyber warfare, but it also looks at the political, cultural, and geographical influences that pertain to these attack methods and helps you understand the motivation and impacts that are likely in each scenario. Cyber Warfare – Truth, Tactics, and Strategies is as real-life and up-to-date as cyber can possibly be, with examples of actual attacks and defense techniques, tools. and strategies presented for you to learn how to think about defending your own systems and data. What you will learn Hacking at scale – how machine learning (ML) and artificial intelligence (AI) skew the battlefield Defending a boundaryless enterprise Using video and audio as weapons of influence Uncovering DeepFakes and their associated attack vectors Using voice augmentation for exploitation Defending when there is no perimeter Responding tactically to counter-campaign-based attacks Who this book is for This book is for any engineer, leader, or professional with either a responsibility for cyber security within their organizations, or an interest in working in this ever-growing field.
The real-world guide to defeating hackers and keeping your business secure Many books discuss the technical underpinnings and complex configurations necessary for cybersecurity—but they fail to address the everyday steps that boards, managers, and employees can take to prevent attacks. The Cybersecurity Playbook is the step-by-step guide to protecting your organization from unknown threats and integrating good security habits into everyday business situations. This book provides clear guidance on how to identify weaknesses, assess possible threats, and implement effective policies. Recognizing that an organization’s security is only as strong as its weakest link, this book offers specific strategies for employees at every level. Drawing from her experience as CMO of one of the world’s largest cybersecurity companies, author Allison Cerra incorporates straightforward assessments, adaptable action plans, and many current examples to provide practical recommendations for cybersecurity policies. By demystifying cybersecurity and applying the central concepts to real-world business scenarios, this book will help you: Deploy cybersecurity measures using easy-to-follow methods and proven techniques Develop a practical security plan tailor-made for your specific needs Incorporate vital security practices into your everyday workflow quickly and efficiently The ever-increasing connectivity of modern organizations, and their heavy use of cloud-based solutions present unique challenges: data breaches, malicious software infections, and cyberattacks have become commonplace and costly to organizations worldwide. The Cybersecurity Playbook is the invaluable guide to identifying security gaps, getting buy-in from the top, promoting effective daily security routines, and safeguarding vital resources. Strong cybersecurity is no longer the sole responsibility of IT departments, but that of every executive, manager, and employee.
Ten Strategies of a World-Class Cyber Security Operations Center conveys MITRE's accumulated expertise on enterprise-grade computer network defense. It covers ten key qualities of leading Cyber Security Operations Centers (CSOCs), ranging from their structure and organization, to processes that best enable smooth operations, to approaches that extract maximum value from key CSOC technology investments. This book offers perspective and context for key decision points in structuring a CSOC, such as what capabilities to offer, how to architect large-scale data collection and analysis, and how to prepare the CSOC team for agile, threat-based response. If you manage, work in, or are standing up a CSOC, this book is for you. It is also available on MITRE's website, www.mitre.org.
This collection of essays is based on a dialogue organized by CSIS to examine national perspectives on Asianism (regional exceptionalism) and universalism (democratic norms) across Asia, as well as the role of regional democracies in developing a common understanding of rules and norms as the foundation for a more stable regional order. The volume includes essays analyzing normative debates in Japan, South Korea, India, Indonesia, and the United States and explores the potential for like-minded states in Asia to prioritize democracy promotion in foreign policy strategy.
The Power of Empowering Others Leadership isn't easy. It takes grit, courage, and vision, among other things, that can be hard to come by on your toughest days. When leaders and aspiring leaders seek out advice, they're often told to try harder. Dig deeper. Look in the mirror and own your natural-born strengths and fix any real or perceived career-limiting deficiencies. Frances Frei and Anne Morriss offer a different worldview. They argue that this popular leadership advice glosses over the most important thing you do as a leader: build others up. Leadership isn't about you. It's about how effective you are at empowering other people—and making sure this impact endures even in your absence. As Frei and Morriss show through inspiring stories from ancient Rome to present-day Silicon Valley, the origins of great leadership are found, paradoxically, not in worrying about your own status and advancement, but in the unrelenting focus on other people's potential. Unleashed provides radical advice for the practice of leadership today. Showing how the boldest, most effective leaders use a special combination of trust, love, and belonging to create an environment in which other people can excel, Frei and Morriss offer practical, battle-tested tools—based on their work with companies such as Uber, Riot Games, WeWork, and others—along with interviews and stories from their own personal experience, to make these ideas come alive. This book is your indispensable guide for unleashing greatness in other people . . . and, ultimately, in yourself. To learn more, please visit theleadersguide.com.
Originally published in hardcover in 2019 by Doubleday.
China is at a critical juncture in its economic transformation as it tries to rebalance what is generally seen as an exhausted growth model. A unifying theme across the reforms that will deliver this transformation is that it can no longer be achieved by raising the amount of physical investment and government direction of resource allocation. Instead China is building a new set of policy frameworks that will allow markets to function more effectively—not unfettered markets, but markets that work efficiently, in line with broad social and other policy goals, and in a sustainable way. Hence, China is now building a new soft infrastructure, that is, the institutional plumbing that underpins and guides the functioning of markets as the key organizing principle toward achieving sustained economic and social progress. Against this background, this volume provides policymakers, academics, and the public with valuable information about policies and institutions in China today. It also looks at the road ahead and key principles that can help China in navigating it. The book focuses on issues crucial in the country’s transformation, such as

tax policy and administration, social security, state-owned enterprise reform, medium-term expenditure frameworks, the role of local government finances, capital account liberalization, and renminbi internationalization. As China moves toward a more price-based allocation of resources, strengthening monetary policy frameworks and financial sector regulation will be particularly important in channeling resources to the most productive sectors and minimizing the risks of financial sector stress. Also, upgrading statistical frameworks will be critical for macroeconomic policymaking and investors. Visit : http://www.elibrary.imf.org/page/modernizing-china

Is it actually possible? …that we might emerge from this pandemic with a peaceful global power switch from those who have too much to those who don't have enough? With billionaires able to decide the fate of nations, private corporations more powerful and less accountable than ever, and political autocrats around the world shaking our confidence in democratic institutions, power resides in all the wrong places. And so our world is in crisis. In such moments, activists find opportunities. Not to restore the pre-crises order, but to transform it. Paul O'Brien argues that progressive activists may never have a better opportunity to rewrite economic rules, systems and outcomes in favor of those who don't have enough. His book offers practical action steps for activists who want to drive a power switch that overcomes extreme inequalities in our world.

“One of the finest books on information security published so far in this century—easily accessible, tightly argued, superbly well-sourced, intimidatingly perceptive.” —Thomas Rid, author of Active Measures “The best examination I have read of how increasingly dramatic developments in cyberspace are defining the ‘new normal’ of geopolitics in the digital age. Buchanan...captures the dynamics of all of this truly brilliantly.” —General David Petraeus, former Director of the CIA and Commander of Coalition Forces in Iraq and Afghanistan Few national-security threats are as potent—or as nebulous—as cyber attacks. Ben Buchanan reveals how hackers are transforming spycraft and statecraft, catching us all in the crossfire, whether we know it or not. Ever since WarGames, we have been bracing for the cyberwar to come, conjuring images of exploding power plants and mass panic. But while cyber attacks are now disturbingly common, they don’t look anything like we thought they would. Packed with insider information based on interviews, declassified files, and forensic analysis of company reports, The Hacker and the State sets aside fantasies of cyber-annihilation to explore the real geopolitical competition of the digital age. Tracing the conflict of wills and interests among modern nations, Ben Buchanan reveals little-known details of how China, Russia, North Korea, Britain, and the United States hack one another in a relentless struggle for dominance. His analysis moves deftly from underseas cable taps to underground nuclear sabotage, from blackouts and data breaches to billion-dollar heists and election interference. Buchanan brings to life this continuous cycle of espionage and deception, attack and counterattack, destabilization and retaliation. He explains why cyber attacks are far less destructive than we anticipated, far more pervasive, and much harder to prevent. With little fanfare and far less scrutiny, they impact our banks, our tech and health systems, our democracy, and every aspect of our lives. Quietly, insidiously, they have reshaped our national-security priorities and transformed spycraft and statecraft. The contest for geopolitical advantage has moved into cyberspace. The United States and its allies can no longer dominate the way they once did. The nation that hacks best will triumph.

Cyberattack-an ominous word that strikes fear in the hearts of nearly everyone, especially business owners, CEOs, and executives. With cyberattacks resulting in often devastating results, it's no wonder executives hire the best and brightest of the IT world for protection. But are you doing enough? Do you understand your risks? What if the brightest aren't always the best choice for your company? ? In The Smartest Person in the Room, Christian Espinosa shows you how to leverage your company's smartest minds to your benefit and theirs. Learn from Christian's own journey from cybersecurity engineer to company CEO. He describes why a high IQ is a lost superpower when effective communication, true intelligence, and self-confidence are not embraced. With his seven-step methodology and stories from the field, Christian helps you develop your team's technical minds so they become better humans and strong leaders who excel in every role. This book provides you with an enlightening perspective of how to turn your biggest unknown weakness into your strongest defense.

One of 2021's Most Highly Anticipated New Books—Newsweek One of The 20 Leadership Books to Read in 2020—Adam Grant One of The Best New Wellness Books Hitting Shelves in January 2021—Shape.com A Top Business Book for January 2021—Financial Times A Next Big Idea Club Nominee Social Chemistry will utterly transform the way you think about “networking.” Understanding the contours of your social network can dramatically enhance personal relationships, work life, and even your global impact. Are you an Expansionist, a Broker, or a Convener? The answer matters more than you think. . . . Yale professor Marissa King shows how anyone can build more meaningful and productive relationships based on insights from neuroscience, psychology, and network analytics. Conventional wisdom says it's the size of your network that matters, but social science research has proven there is more to it. King explains that the quality and structure of our relationships has the greatest impact on our personal and professional lives. As she shows, there are three basic types of networks, so readers can see the role they are already playing: Expansionist, Broker, or Convener. This network decoder enables readers to own their network style and modify it for better alignment with their life plans and values. High-quality connections in your social network strongly predict cognitive functioning, emotional resilience, and satisfaction at work. A well-structured network is likely to boost the quality of your ideas, as well as your pay. Beyond the office, social connections are the lifeblood of our health and happiness. The compiled results from dozens of previous studies found that our social relationships have an effect on our likelihood of dying prematurely—equivalent to obesity or smoking. Rich stories of Expansionists like Vernon Jordan, Brokers like Yo-Yo Ma, and Conveners like Anna Wintour, as well as personal experiences from King's own world of connections, inform this warm, engaging, revelatory investigation into some of the most consequential decisions we can make about the trajectory of our lives.

This book is written by a C(I)SO for C(I)SOs - and also addresses CEOs, CROs, CLOs, CIOs, CTOs, Security Managers, Privacy Leaders, Lawyers, and even Marketing and Sales executives. It is written by a seven-time career CISO for other visionaries, leaders, strategists, architects, compliance and audit experts, those politically interested, as well as, revolutionaries, and students of IS, IT, and STEM subjects that want to step up their game in InfoSec and Cybersecurity. The book connects the dots about past data breaches and their misconceptions; provides an international perspective on privacy laws like GDPR and several others, about threat actors and threat vectors; introduces strategy and tactics for securing your organization; presents a first glimpse on leadership; explains security program planning and backup plans; examines team building; conceptualizes the governance board; explores budgets; cooperates with the PMO; divulges into tactics; further elaborates on leadership; establishes the reporting structure; illustrates risk assessments; elucidates security processes, principals, and architectural designs; enumerates security metrics; skims compliance; demonstrates attack surface reduction; explicates security intelligence; conceptualizes S-SDLC (SecDevOps); depicts security management; epitomizes global leadership; illustrates the cloud's weaknesses; and finishes with an outlook on IoT. If you are in need of strong, proven, battle-tested security advice for a progressing security career, if you're looking for the security wisdom of a global, experienced leader to make smart decisions, if you are an architect and want to know how to securely architect and design using guiding principles, design patterns, and controls, or even if you work in sales and want to understand how (not) to sell to the CISO - this is your almanac - and you will read and reference it many times.

Dependence on computers has had a transformative effect on human society. Cybernetics is now woven into the core functions of virtually every basic institution, including our oldest ones. War is one such institution, and the digital revolution's impact on it has been profound. The American military, which has no peer, is almost completely reliant on high-tech computer systems. Given the Internet's potential for

full-spectrum surveillance and information disruption, the marshaling of computer networks represents the next stage of cyberwar. Indeed, it is upon us already. The recent Stuxnet episode, in which Israel fed a malignant computer virus into Iran's nuclear facilities, is one such example. Penetration into US government computer systems by Chinese hackers-presumably sponsored by the Chinese government-is another. Together, they point to a new era in the evolution of human conflict. In Cybersecurity and Cyerbwar: What Everyone Needs to Know, noted experts Peter W. Singer and Allan Friedman lay out how the revolution in military cybernetics occurred and explain where it is headed. They begin with an explanation of what cyberspace is before moving on to discussions of how it can be exploited and why it is so hard to defend. Throughout, they discuss the latest developments in military and security technology. Singer and Friedman close with a discussion of how people and governments can protect themselves. In sum, Cybersecurity and Cyerbwar is the definitive account on the subject for the educated general reader who wants to know more about the nature of war, conflict, and security in the twenty-first century.
How the best companies prepare for and manage modern vulnerabilities—from cybersecurity risks to climate change: new tools, processes and organizations for developing corporate resilience. A catastrophic earthquake is followed by a tsunami that inundates the coastline, and around the globe manufacturing comes to a standstill. State-of-the-art passenger jets are grounded because of a malfunctioning part. A strike halts shipments through a major port. A new digital device decimates the sales of other brands and sends established firms to the brink of bankruptcy. The interconnectedness of the global economy today means that unexpected events in one corner of the globe can ripple through the world's supply chain and affect customers everywhere. In this book, Yossi Sheffi shows why modern vulnerabilities call for innovative processes and tools for creating and embedding corporate resilience and risk management. Sheffi offers fascinating case studies that illustrate how companies have prepared for, coped with, and come out stronger following disruption—from the actions of Intel after the 2011 Japanese tsunami to the disruption in the “money supply chain” caused by the 2008 financial crisis. Sheffi, author of the widely read The Resilient Enterprise, focuses here on deep tier risks as well as corporate responsibility, cybersecurity, long-term disruptions, business continuity planning, emergency operations centers, detection, and systemic disruptions. Supply chain risk management, Sheffi shows, is a balancing act between taking on the risks involved in new products, new markets, and new processes—all crucial for growth—and the resilience created by advanced risk management.
"I've had the pleasure of taking Dr. Hasib's class and learning about both Cybersecurity Management and Ethical Leadership. In an ever changing field, there are certain principles that we can apply consistently. Dr. Hasib covers these principles and does it in a way that easy to learn and understand. He has a great passion for his work and it shows in both his teaching styles and writing. I'd strongly suggest anyone within the Cybersecurity field to read his book. Whether you are a CEO or the technical support, this gives a thorough overview of an entire organization. If you are management, the ethical leadership portion helps build a strong community within an organization." - B. Avery Greene - Graduate student of cybersecurity at UMBC. ..".The dynamic of his classroom was so different than any class I've had. He is paving the way for future CEO's CISO's and entrepreneurs and is making a direct positive impact for cybersecurity students. Even though my background is not very technical, I was able to fully comprehend and excel in his classroom. Great class, strongly recommend his teaching..." -Sarah Purdum - Graduate student of cybersecurity at UMBC. Managing cybersecurity requires a multi-disciplinary holistic business approach. Many of the current cybersecurity approaches in organizations and most books are based on an outdated 1991 model of cybersecurity - focused solely on technology solutions. This book provides the 2014 model and shows why leadership engagement of people within an organization is critical for success. Culture development through leadership is essential because culture governs behavior. Apply the time tested principles explained in this book for success in any organization. Today cybersecurity strategy is the same as information technology strategy. Cybersecurity drives the mission of the modern organization. Done right it can be a hallmark of distinction and a source of productivity and innovation in an organization. Failure to lead cybersecurity can easily lead to business failure. This book is an essential read for CIOs, CISOs, or any organizational business leader or student who wishes to understand how to build successful organizations. No prior background in cybersecurity or technology is required to understand this book. ..".explains what an organization needs to know to implement cybersecurity governance." Council of Graduate Schools Testimony at the US Senate Appropriations Committee Meeting, April 29, 2014. ..".this book will change both the way we think about leadership and the way we understand information technology. I recommend this book highly to everyone." - Eric Schwartz - Executive Director at Advena World LLC.