Cloud Infrastructure Security Trends Redlock

A ground shaking exposé on the failure of popular cyber risk management methods How to Measure Anything in Cybersecurity Risk exposes the shortcomings of current "risk management" practices, and offers a series of improvement techniques that help you fill the holes and ramp up security. In his bestselling book How to Measure Anything, author Douglas W. Hubbard opened the business world's eyes to the critical need for better measurement. This book expands upon that premise and draws from The Failure of Risk Management to sound the alarm in the cybersecurity realm. Some of the field's premier risk management approaches actually create more risk than they mitigate, and questionable methods have been duplicated across industries and embedded in the products accepted as gospel. This book sheds light on these blatant risks, and provides alternate techniques that can help improve your current situation. You'll also learn which approaches are too risky to save, and are actually more damaging than a total lack of any security. Dangerous risk management methods abound; there is no industry more critically in need of solutions than cybersecurity. This book provides solutions where they exist, and advises when to change tracks entirely. Discover the shortcomings of cybersecurity's "best practices" Learn which risk management approaches actually create risk Improve your current practices with practical alterations Learn which methods are beyond saving, and worse than doing nothing Insightful and enlightening, this book will inspire a closer examination of your company's own risk management practices in the context of cybersecurity. The end goal is airtight data protection, so finding cracks in the vault is a positive thing—as long as you get there before the bad guys do. How to Measure Anything in Cybersecurity Risk is your guide to more robust protection through better quantitative processes, approaches, and techniques.

* Covers the A-to-Z of Axapta in 300 pages * Author is the world ' s leading Axapta expert * Provides essential guidance to a fast-growing community currently deprived of suitable documentation and training

This volume provides an up-to-date study of theory and practice on the importance of technology in teaching and learning. The contributions are carefully peer-reviewed from over 100 submissions to the International Conference on Teaching and Learning 2006, held in Hong Kong. Sample Chapter(s). Chapter 1: Faculty Perceptions of ICT Benefits (391 KB). Contents: Faculty Perceptions of ICT Benefits (R Fox et al.); Thinking about Thinking Online (K Downing et al.); Teacher"s Sharing Pedagogical Experiences in a Learning Environment that Supports Self-Regulated Learning (G Dettori et al.); Online Interaction: Trying to Get It Right (L Chow and R Sharman); Crossing Borders: How Cross-Cultural Videoconferencing can Satisfy Course Goals in Dissimilar Subjects (J S Wilkinson & A-L Wang); The Evaluation of Information and Communication Technology Use in Professional Schools (P Gabor & C Ing); Using Technology in Education: The Application of Data Mining (K H Chye et al.); A Comparison of WebCT, Blackboard and Moddle for the Teaching and Learning of Continuing Education Courses (K S Cheung); The Object-Oriented Database Application and the System Architecture of a National Learning Objects Repository for Cyprus (P Pouyioutas et al.); and other papers. Readership: Graduate students, researchers and practitioners involved in the development and education of e-learning.

This volume constitutes the proceedings of the 16th International Conference on Services Computing 2019, held as Part of SCF 2019 in San Diego, CA, USA in June 2019. The 9 full papers presented in this volume were carefully reviewed and selected from 15 submissions. They cover topics such as: foundations of services computing; scientific workflows; business process integration and management; microservices; modeling of services systems; service security and privacy; SOA service applications; and service lifecycle management.

Be More Strategic in Business
Do More Faster
The Emoji Code
How to Measure Anything in Cybersecurity Risk
The Linguistics Behind Smiley Faces and Scaredy Cats
Proceedings of the 2016 ACM SIGSAC Conference on Computer and Communications Security
How to Win through Stronger Leadership and Smarter Decisions

This book constitutes the refereed conference proceedings of the 20th International Symposium on Research in Attacks, Intrusions, and Defenses, RAID 2017, held in Atlanta, GA, USA, in September 2017. The 21 revised full papers were selected from 105 submissions. They are organized in the following topics: software security, intrusion detection, systems security, android security, cybercrime, cloud security, network security.

Information security is a rigged game and we have no choice but to play it every day. Rules are mandatory for the good guys but optional for the bad guys. And the good guys are losing. Now's the time to start playing offense and turn this game around. We can do it if we work together! UNSECURITY sounds the call and lays out the plan for information security professionals to unite in strength and fix this broken industry. Book jacket.

STRENGTHEN SOFTWARE SECURITY BY HELPING DEVELOPERS AND SECURITY EXPERTS WORK TOGETHER Traditional approaches to securing software are inadequate. The solution: Bring software engineering and network security teams together in a new, holistic approach to protecting the entire enterprise. Now, four highly respected security experts explain why this “confluence” is so crucial, and show how to implement it in your organization. Writing for all software and security practitioners and leaders, they show how software can play a vital, active role in protecting your organization. You’ll learn how to construct software that actively safeguards sensitive data and business processes and contributes to intrusion detection/response in sophisticated new ways. The authors cover the entire development lifecycle, including project inception, design, implementation, testing, deployment, operation, and maintenance. They also provide a full chapter of advice specifically for Chief Information Security Officers and other enterprise security executives. Whatever your software security responsibilities, Enterprise Software Security delivers indispensable big-picture guidance–and specific, high-value recommendations you can apply right now. COVERAGE INCLUDES: • Overcoming common obstacles to collaboration between developers and IT security professionals • Helping programmers design, write, deploy, and operate more secure software • Helping network security engineers use application output more effectively • Organizing a software security team before you’ve even created requirements • Avoiding the unmanageable complexity and inherent flaws of layered security • Implementing positive software design practices and identifying security defects in existing designs • Teaming to improve code reviews, clarify attack scenarios associated with vulnerable code, and validate positive compliance • Moving beyond pentesting toward more comprehensive security testing • Integrating your new application with your existing security infrastructure • “Ruggedizing” DevOps by adding infosec to the relationship between development and operations • Protecting application security during maintenance

The only security book to be chosen as a Dr. Dobbs Jolt Award Finalist since Bruce Schneier's Secrets and Lies and Applied Cryptography! Adam Shostack is responsible for security development lifecycle threat modeling at Microsoft and is one of a handful of threat modeling experts in the world. Now, he is sharing his considerable expertise into this unique book. With pages of specific actionable advice, he details how to build better security into the design of systems, software, or services from the outset. You'll explore various threat modeling approaches, find out how to test your designs against threats, and learn effective ways to address threats that have been validated at Microsoft and other top companies. Systems security managers, you'll find tools and a framework for structured thinking about what can go wrong. Software developers, you'll appreciate the jargon-free and accessible introduction to this essential skill. Security professionals, you'll learn to discern changing threats and discover the easiest ways to adopt a structured approach to threat modeling. Provides a unique how-to for security and software developers who need to design secure products and systems and test their designs Explains how to threat model and explores various threat modeling approaches, such as asset-centric, attacker-centric and software-centric Provides effective approaches and techniques that have been proven at Microsoft and elsewhere Offers actionable how-to advice not tied to any specific software, operating system, or programming language Authored by a Microsoft professional who is one of the most prominent threat modeling experts in the world As more software is delivered on the Internet or operates on Internet-connected devices, the design of secure software is absolutely critical. Make sure you're ready with Threat Modeling: Designing for Security.

Information Security Is Failing. Breaches Are Epidemic. How Can We Fix This Broken Industry?
Techstars Lessons to Accelerate Your Startup
Dynamics AX
Cloud Computing Law
Anyone, Anything, Anytime
A Guide to Microsoft Axapta
Computer Graphics from Scratch

Become a cyber-hero - know the common wireless weaknesses "Reading a book like this one is a worthy endeavor towardbecoming an experienced wireless security professional." --Devin Akin - CTO, The Certified Wireless Network Professional(CWNP) Program Wireless networks are so convenient - not only for you, but alsofor those nefarious types who'd like to invade them. The only wayto know if your system can be penetrated is to simulate an attack.This book shows you how, along with how to strengthen any weakspots you find in your network's armor. Discover how to: Perform ethical hacks without compromising a system Combat denial of service and WEP attacks Understand how invaders think Recognize the effects of different hacks Protect against war drivers and rogue devices

If you understand basic mathematics and know how to program with Python, you’re ready to dive into signal processing. While most resources start with theory to teach this complex subject, this practical book introduces techniques by showing you how they’re applied in the real world. In the first chapter alone, you’ll be able to decompose a sound into its harmonics, modify the harmonics, and generate new sounds. Author Allen Downey explains techniques such as spectral decomposition, filtering, convolution, and the Fast Fourier Transform. This book also provides exercises and code examples to help you understand the material. You’ll explore: Periodic signals and their spectrums Harmonic structure of simple waveforms Chirps and other sounds whose spectrum changes over time Noise signals and natural sources of noise The autocorrelation function for estimating pitch The discrete cosine transform (DCT) for compression The Fast Fourier Transform for spectral analysis Relating operations in time to filters in the frequency domain Linear time-invariant (LTI) system theory Amplitude modulation (AM) used in radio Other books in this series include Think Stats and Think Bayes, also by Allen Downey.

Ian Maxwell applies decades of research and application to present a novel approach to innovation, with an emphasis on sustainable and renewable practices that benefit many, and not just a handful of executives and shareholders. Featuring examples from a wide range of innovators around the world, from Google to Genentech to the Masdar “clean” city initiative in Abu Dhabi, Maxwell argues that organizations that embrace structured innovation management systems and drive a “top down” innovation culture will achieve sustainable high growth and strong shareholder returns. Countries that provide the right physical, financial and human resource infrastructure to support a highly innovative macro-economic environment will experience both strong GPD growth and high living standards. Those companies and countries that fail to support innovation will struggle to compete and raise living standards, respectively. Maxwell considers the cases of China and India, whose low-cost innovation strategies are posing a serious competitive threat to established multinationals in the developed world, and considers the impact of innovation on such timely issues as climate change, environmental pollution, fossil fuel shortages, third world poverty, rising healthcare costs and ageing populations.

Harness your company’s incumbent advantages to win the digital disruption game Goliath’s Revenge is the practical guide for how executives and aspiring leaders of established companies can run the Silicon Valley playbook for themselves and capitalize on digital disruption. Technologies like artificial intelligence, robotics, internet of things, blockchain, and immersive experiences are changing the basis of competition in every industry. New competitors are emerging while traditional ones are falling behind. Periods of intense change provide remarkable opportunities. Goliath’s Revenge delivers an insider’s view of how industry leaders like General Motors, NASA, The Weather Channel, Hitachi, Mastercard, Proctor & Gamble, Penn Medicine, Discovery, and Cisco are accelerating innovation, building new skills, and disrupting themselves to come out stronger in this post-digital age. Learn how to leverage your company’s scale, reach, data, and expertise to launch breakthrough offerings that fend off attackers and secure your position as a future industry leader. Using real success cases and recommendations, this invaluable resource shows how to realign your business model, reset your talent development priorities, and retake market share lost to digital-ready competitors. Drawing from extensive experience in digital transformation, leadership development, and strategic planning, the authors show how established companies can switch from defense to offense to thrive in this new digital environment. Learn the six new rules that separate winners from losers in the age of digital disruption Prioritize your innovation investments to rebuild your competitive moat Employ smart cannibalization to defend your core business Deliver step-change customer outcomes to grow into adjacent markets Reframe your purpose and make talent the centerpiece of your digital innovation strategy Goliath’s Revenge is a must-read for business leaders and innovators in small, mid-sized, and large organizations trying to win the digital disruption game. This book helps you reset both your company strategy and professional development priorities for long-term success.

Cybersecurity Framework Manufacturing Profile
Enterprise Software Security
How Established Companies Turn the Tables on Digital Disruptors
A Programmer's Introduction to 3D Rendering
COBIT 5: Enabling Information
The Power of Blockchain for Healthcare
Writing for Computer Science

Harness new techniques that let you see what is happening on your networks and take decisive action without getting lost in a sea of data.

The book provides insights into International Conference on Smart Innovations in Communications and Computational Sciences (ICSICCS 2017) held at North West Group of Institutions, Punjab, India. It presents new advances and research results in the fields of computer and communication written by leading researchers, engineers and scientists in the domain of interest from around the world. The book includes research work in all the areas of smart innovation, systems and technologies, embedded knowledge and intelligence, innovation and sustainability, advance computing, networking and informatics. It also focuses on the knowledge-transfer methodologies and innovation strategies employed to make this happen effectively. The combination of intelligent systems tools and a broad range of applications introduce a need for a synergy of disciplines from science and technology. Sample areas include, but are not limited to smart hardware, software design, smart computing technologies, intelligent communications and networking, web and informatics and computational sciences.

"A wonderful picture of an important period in the practice of medicine in the United States." (from the Foreword by Peter Rosen, MD) Here is the very first book to comprehensively explore the evolution of the field of emergency medicine -- from its origins following World War II, through the sociopolitical changes of the 1950s, 1960s, and 1970s, to the present. First-hand narratives from more than 45 founders and pioneers of emergency medicine provide a vivid portrayal of the important events and viewpoints that have given rise to today's practice. Represents the first comprehensive history of emergency medicine as a specialty. Provides first-hand oral histories from more than 45 of the key figures who witnessed and helped to shape the developments chronicled in the book. Offers keen insights into how the sociopolitical changes of the 1950s through 1970s influenced public health, health care delivery, and emergency medicine. Includes many unique photographs of important leaders in emergency medicine.

Did you hear about blockchain technology, and how it impacts finance but were more interested in blockchain's impact on healthcare? The biggest opportunities for blockchain, still lie undiscovered-that is until now. In fact, investors, entrepreneurs, innovators, and executives are searching to identify the changes that will result from the introduction of blockchain technology to healthcare. Previously, a book didn't exist that comprehensively covered the impact of blockchain for healthcare in a practical and fun discussion. Today, we will step outside the headlines and into the unchained world of blockchain technology.In The Power of Blockchain for Healthcare, author Peter B. Nichol highlights where blockchain is emerging with the potential to transform the patient experience-from payers to providers to patients-embracing blockchain to create sustainable competitive advantages. Nichol magnifies the principles and use cases pioneering a new frontier to revolutionize the healthcare experience. Based on his articles, blogs, and musings, the book shows what is required to transform healthcare from the inside. It explains practical uses for blockchain in a straightforward conversation by answering: What can blockchain do? How will it impact our health? Why should you care as a business leader? Within these parts, you'll learn:* How blockchain can help patients.* How to unchain, existing models to rebuild trust in healthcare.* How pockets of innovation will energize healthcare.* How curiosity will uncover new value for our healthcare ecosystem .This book also includes a practical enterprise readiness assessment, to aid in the transformation of your organization into a blockchain leader.The Power of Blockchain for Healthcare is the must-read guide to reframe your thinking and to help your organization excel in the new age of healthcare transformation-the blockchain revolution is here.

Proceedings of ICSICCS 2017
Goliath's Revenge
Detect the Signals, Stop the Hack
Managing Sustainable Innovation
Digital Forensics and Incident Response
How Blockchain Will Ignite the Future of Healthcare
A Confluence of Disciplines

The basics of the profession and practice of architecture, presented in illustrated A–Z form. The word "architect" is a noun, but Doug Patt uses it as a verb—coining a term and making a point about using parts of speech and parts of buildings in new ways. Changing the function of a word, or a room, can produce surprise and meaning. In How to Architect, Patt—an architect and the creator of a series of wildly popular online videos about architecture—presents the basics of architecture in A–Z form, starting with "A is for Asymmetry" (as seen in Chartres Cathedral and Frank Gehry), detouring through "N is for Narrative," and ending with "Z is for Zeal" (a quality that successful architects tend to have, even in fiction—see The Fountainhead's architect-hero Howard Roark.) How to Architect is a book to guide you on the road to architecture. If you are just starting on that journey or thinking about becoming an architect, it is a place to begin. If you are already an architect and want to remind yourself of what drew you to the profession, it is a book of affirmation. And if you are just curious about what goes into the design and construction of buildings, this book tells you how architects think. Patt introduces each entry with a hand-drawn letter, and accompanies the text with illustrations that illuminate the concept discussed: a fallen Humpty Dumpty illustrates the perils of fragile egos; photographs of an X-Acto knife and other hand tools remind us of architecture's nondigital origins. How to Architect offers encouragement to aspiring architects but also mounts a defense of architecture as a profession—by calling out a defiant verb: architect!

A practical guide to deploying digital forensic techniques in response to cyber security incidents About This Book Learn incident response fundamentals and create an effective incident response framework Master forensics investigation utilizing digital investigative techniques Contains real-life scenarios that effectively use threat intelligence and modeling techniques Who This Book Is For This book is targeted at Information Security professionals, forensics practitioners, and students with knowledge and experience in the use of software applications and basic command-line experience. It will also help professionals who are new to the incident response/digital forensics role within their organization. What You Will Learn Create and deploy incident response capabilities within your organization Build a solid foundation for acquiring and handling suitable evidence for later analysis Analyze collected evidence and determine the root cause of a security incident Learn to integrate digital forensic techniques and procedures into the overall incident response process Integrate threat intelligence in digital evidence analysis Prepare written documentation for use internally or with external parties such as regulators or law enforcement agencies In Detail Digital Forensics and Incident Response will guide you through the entire spectrum of tasks associated with incident response, starting with preparatory activities associated with creating an incident response plan and creating a digital forensics capability within your own organization. You will then begin a detailed examination of digital forensic techniques including acquiring evidence, examining volatile memory, hard drive assessment, and network-based evidence. You will also explore the role that threat intelligence plays in the incident response process. Finally, a detailed section on preparing reports will help you prepare a written report for use either internally or in a courtroom. By the end of the book, you will have mastered forensic techniques and incident response and you will have a solid foundation on which to increase your ability to investigate such incidents in your organization. Style and approach The book covers practical scenarios and examples in an enterprise setting to give you an understanding of how digital forensics integrates with the overall response to cyber security incidents. You will also

learn the proper use of tools and techniques to investigate common cyber security incidents such as malware infestation, memory analysis, disk analysis, and network analysis.
"The fox knows many things, but the hedgehog knows one big thing." This ancient Greek aphorism, preserved in a fragment from the poet Archilochus, describes the central thesis of Isaiah Berlin's masterly essay on Leo Tolstoy and the philosophy of history, the subject of the epilogue to War and Peace. Although there have been many interpretations of the adage, Berlin uses it to mark a fundamental distinction between human beings who are fascinated by the infinite variety of things and those who relate everything to a central, all-embracing system. Applied to Tolstoy, the saying illuminates a paradox that helps explain his philosophy of history: Tolstoy was a fox, but believed in being a hedgehog. One of Berlin's most celebrated works, this extraordinary essay offers profound insights about Tolstoy, historical understanding, and human psychology. This new edition features a revised text that supplants all previous versions, English translations of the many passages in foreign languages, a new foreword in which Berlin biographer Michael Ignatieff explains the enduring appeal of Berlin's essay, and a new appendix that provides rich context, including excerpts from reviews and Berlin's letters, as well as a startling new interpretation of Archilochus's epigram.
Drawing from disciplines as diverse as linguistics, cognitive science, psychology, and neuroscience, The Emoji Code explores how emojis are expanding communication and not ending it. For all the handwringing about the imminent death of written language, emoji—those happy faces and hearts—is not taking us backward to the dark ages of illiteracy. Every day 41.5 billion texts are sent by one quarter of the world, using 6 million emoji. Evans argues that these symbols enrich our ability to communicate and allow us to express our emotions and induce empathy—ultimately making us all better communicators. Vyvyan Evans's Emoji Code charts the evolutionary origins of language, the social and cultural factors that govern its use, change, and development; as well as what it reveals about the human mind. In most communication, nonverbal cues are our emotional expression, signal our personality, and are our attitude toward our addressee. They provide the essential means of nuance and are essential to getting our ideas across. But in digital communication, these cues are missing, which can lead to miscommunication. The explosion of emoji, in less than four years, has arisen precisely because it fulfills exactly these functions which are essential for communication but are otherwise absent in texts and emails. Evans persuasively argues that emoji add tone and an emotional voice and nuance, making us more effective communicators in the digital age.
Bombay 3
An Essay on Tolstoy's View of History - Second Edition
Designing for Security
How to Architect
Digital Signal Processing in Python
Enhancing Learning Through Technology
Covid-19 and Business Law

CCS'16: 2016 ACM SIGSAC Conference on Computer and Communications Security Oct 24, 2016-Oct 28, 2016 Vienna, Austria. You can view more information about this proceeding and all of ACM's other published conference proceedings from the ACM Digital Library: http://www.acm.org/dl.
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.
A compelling argument that the Internet of things threatens human rights and security "Sobering and important."--Financial Times, "Best Books of 2020: Technology" The Internet has leapt from human-facing display screens into the material objects all around us. In this so-called Internet of things--connecting everything from cars to cardiac monitors to home appliances--there is no longer a meaningful distinction between physical and virtual worlds. Everything is connected. The social and economic benefits are tremendous, but there is a downside: an outage in cyberspace can result not only in loss of communication but also potentially in loss of life. Control of this infrastructure has become a proxy for political power, since countries can easily reach across borders to disrupt real-world systems. Laura DeNardis argues that the diffusion of the Internet into the physical world radically escalates governance concerns around privacy, discrimination, human safety, democracy, and national security, and she offers new cyber-policy solutions. In her discussion, she makes visible the sinews of power already embedded in our technology and explores how hidden technical governance arrangements will become the constitution of our future.
Increase efficiency while saving money with "on-demand" computing The biggest game-changing force in business since the creation of the Internet, cloud computing simplifies and lowers the cost of operations while providing flexibility and power you never dreamed possible. Make your strategic move now, with Management Strategies for the Cloud Revolution! "Management Strategies for the Cloud Revolution is an important work that captures the concepts and technological advances fueling the rapid adoption of cloud computing today. It illuminates how specific core technologies have led to the emergence of those patterns as the foundation for the next generation of IT-managed infrastructure." —Rich Wolski, Chief Technology Officer and cofounder of Eucalyptus Systems, Inc., and Professor of Computer Science at the University of California, Santa Barbara "Explains in marvelously plain English how clouds will change our world. . . . If the potential of cloud computing doesn't excite you now, it will after you read this book. Buy a copy and put it on your CEO's desk. Babcock explains it all." —Paul Gillin, bestselling author of The New Influencers "A valuable primer and handbook. It will help you master the technology and follow the story as innovators craft the future of cloud computing." —Ted schadler, VP and Principal Analyst, Forrester Research, Inc., and coauthor of Empowered "This readable, thought-provoking book will be especially useful to business professionals and practitioners." Choice magazine About the Book Everyday business as we know it is poised for a monumental shift, courtesy of cloud computing—the biggest game-changer since the creation of the Internet itself. There's no doubt about it: If you want to compete in the future, you must begin educating yourself about cloud computing now. From InformationWeek editor Charles Babcock, a leading authority on the business benefits and pitfalls of cloud computing, Management Strategies for the Cloud Revolution provides the tools every manager needs to create a new business strategy that harnesses all the power cloud computing has to offer. Cloud computing is the equivalent of renting time on a computing infrastructure over the Internet, rather than building your own from the ground up. Access to the cloud is growing quickly, and the benefits are undeniable. Those who begin incorporating cloud computing into their business strategy will enjoy: Dramatic Cost Savings: The cloud makes available innovative technologies that would otherwise be too expensive. Ubiquitous Access: Employees can access the server power they need anytime, anywhere, and send it the program they want to run. Unprecedented Agility: Business processes and business infrastructures can be altered quicker than ever. Steady Traffic Flow: Even during peak loads, systems in the cloud can overcome bottlenecks and expand to meet the user's needs. Working on the cloud, your analysts, business intelligence experts, and researchers can access large-scale, high-speed, highly reliable systems while paying only for short-term use. You didn't set up your own electrical grid to power your computers. Why pay big money to use them when you don't have to? The cloud is on the horizon, and it's looming larger by the day. Learn how to take full advantage of it with Management Strategies for the Cloud Revolution.
Research in Attacks, Intrusions, and Defenses
Legal Implications of a Global Pandemic
Management Strategies for the Cloud Revolution: How Cloud Computing Is Transforming Business and Why You Can't Afford to Be Left Behind
Threat Modeling
International Journal of Information Technology and Web Engineering (IJITWE).
Think DSP
The Driver for Global Growth

March 2017 If you like this book (or the Kindle version), please leave positive review. This document provides the Cybersecurity Framework implementation details developed for the manufacturing environment. The "Manufacturing Profile" of the Cybersecurity Framework can be used as a roadmap for reducing cybersecurity risk for manufacturers that is aligned with manufacturing sector goals and industry best practices. The Profile gives manufacturers:* A method to identify opportunities for improving the current cybersecurity posture of the manufacturing system* An evaluation of their ability to operate the control environment at their acceptable risk level* A standardized approach to preparing the cybersecurity plan for ongoing assurance of the manufacturing system's security Why buy a book you can download for free? First you gotta find it and make sure it's the latest version (not always easy). Then you gotta print it using a network printer you share with 100 other people - and its outta paper - and the toner is low (take out the toner cartridge, shake it, then put it back). If it's just 10 pages, no problem, but if it's a 250-page book, you will need to punch 3 holes in all those pages and put it in a 3-ring binder. Takes at least an hour. An engineer that's paid $75 an hour has to do this himself (who has assistant's anymore?). If you are paid more than $10 an hour and use an ink jet printer, buying this book will save you money. It's much more cost-effective to just order the latest version from Amazon.com This book is published by 4th Watch Books and includes copyright material. We publish compact, tightly-bound, full-size books (8 by 11 inches), with glossy covers. 4th Watch Books is a Service Disabled Veteran-Owned Small Business (SDVOSB), and is not affiliated with the National Institute of Standards and Technology. For more titles published by 4th Watch Books, please visit: cybah.webplus.net A full copy of all the pertinent cybersecurity standards is available on DVD-ROM in the CyberSecurity Standards Library disc which is available at Amazon.com. NIST SP 500-299 NIST Cloud Computing Security Reference Architecture NIST SP 500-291 NIST Cloud Computing Standards Roadmap Version 2 NIST SP 500-293 US Government Cloud Computing Technology Roadmap Volume 1 & 2 NIST SP 500-293 US Government Cloud Computing Technology Roadmap Volume 3 DRAFT NIST SP 1800-8 Securing Wireless Infusion Pumps NISTIR 7497 Security Architecture Design Process for Health Information Exchanges (HIEs) NIST SP 800-66 Implementing the Health Insurance Portability and Accountability Act (HIPAA) Security Rule NIST SP 1800-1 Securing Electronic Health Records on Mobile Devices NIST SP 800-177 Trustworthy Email NIST SP 800-184 Guide for Cybersecurity Event Recovery NIST SP 800-190 Application Container Security Guide NIST SP 800-193 Platform Firmware Resiliency Guidelines NIST SP 1800-1 Securing Electronic Health Records on Mobile Devices NIST SP 1800-2 Identity and Access Management for Electric Utilities NIST SP 1800-5 IT Asset Management: Financial Services NIST SP 1800-6 Domain Name Systems-Based Electronic Mail Security NIST SP 1800-7 Situational Awareness for Electric Utilities Computer Graphics from Scratch demystifies the algorithms used in modern graphics software and guides beginners through building photorealistic 3D renders. Computer graphics programming books are often math-heavy and intimidating for newcomers. Not this one. Computer Graphics from Scratch takes a simpler approach by keeping the math to a minimum and focusing on only one aspect of computer graphics, 3D rendering. You'll build two complete, fully functional renderers: a raytracer, which simulates rays of light as they bounce off objects, and a rasterizer, which converts 3D models into 2D pixels. As you progress you'll learn how to create realistic reflections and shadows, and how to render a scene from any point of view. Pseudocode examples throughout make it easy to write your renderers in any language, and links to live JavaScript demos of each algorithm invite you to explore further on your own. Learn how to: • Use perspective projection to draw 3D objects on a 2D plane • Simulate the way rays of light interact with surfaces • Add mirror-like reflections and cast shadows to objects • Render a scene from any camera position using clipping planes • Use flat, Gouraud, and Phong shading to mimic real surface lighting • Paint texture details onto basic shapes to create realistic-looking objects Whether you're an aspiring graphics engineer or a novice programmer curious about how graphics algorithms work, Gabriel Gambetta's simple, clear explanations will quickly put computer graphics concepts and rendering techniques within your reach. All you need is basic coding knowledge and high school math. Computer Graphics from Scratch will cover the rest.
The COVID-19 pandemic has had extraordinary effects on human lives and economies around the world. Many countries have introduced various measures to stop the spread of the virus and preserve human lives and livelihoods. Some commentators have considered these measures extreme, such as the restrictions imposed on people's movement and lockdown of countries' borders. While these measures have undoubtedly saved lives and curbed the spread of the deadly virus, they have also produced some unintended legal implications for individuals and businesses, particularly in the areas of contractual obligations, employment relationships, tourism and hospitality, company law, competition law, human rights and the rule of law, protection of vulnerable groups like migrant workers, and access to judicial and legal services. COVID-19 and Business Law: Legal Implications of a Global Pandemic identifies and discusses specific legal challenges caused by the COVID-19 pandemic in these areas and suggests possible ways in which they could be remedied.
Kubernetes is the operating system of the cloud native world, providing a reliable and scalable platform for running containerized workloads. In this friendly, pragmatic book, cloud experts John Arundel and Justin Domingus show you what Kubernetes can do—and what you can do with it. You'll learn all about the Kubernetes ecosystem, and use battle-tested solutions to everyday problems. You'll build, step by step, an example cloud native application and its supporting infrastructure, along with a development environment and continuous deployment pipeline that you can use for your own applications. Understand containers and Kubernetes from first principles; no experience necessary Run your own clusters or choose a managed Kubernetes service from Amazon, Google, and others Use Kubernetes to manage resource usage and the container lifecycle Optimize clusters for cost, performance, resilience, capacity, and scalability Learn the best tools for developing, testing, and deploying your applications Apply the latest industry practices for security, observability, and monitoring Adopt DevOps principles to help make your development teams lean, fast, and effective
Critical Infrastructure Protection Reliability Standards (Us Federal Energy Regulatory Commission Regulation) (Ferc) (2018 Edition)
20th International Symposium, RAID 2017, Atlanta, GA, USA, September 18 – 20, 2017, Proceedings
Hacking Wireless Networks For Dummies
Applied Security Visualization
The Hedgehog and the Fox
Next Level Cybersecurity
Services Computing – SCC 2019

Critical Infrastructure Protection Reliability Standards (US Federal Energy Regulatory Commission Regulation) (FERC) (2018 Edition) The Law Library presents the complete text of the Critical Infrastructure Protection Reliability Standards (US Federal Energy Regulatory Commission Regulation) (FERC) (2018 Edition). Updated as of May 29, 2018 The Federal Energy Regulatory Commission (Commission) approves seven critical infrastructure protection (CIP) Reliability Standards: CIP-003-6 (Security Management Controls), CIP-004-6 (Personnel and Training), CIP-006-6 (Physical Security of BES Cyber Systems), CIP-007-6 (Systems Security Management), CIP-009-6 (Recovery Plans for BES Cyber Systems), CIP-010-2 (Configuration Change Management and Vulnerability Assessments), and CIP-011-2 (Information Protection). The proposed Reliability Standards address the cyber security of the bulk electric system and improve upon the current Commission-approved CIP Reliability Standards. In addition, the Commission directs NERC to develop certain modifications to improve the CIP Reliability Standards. This book contains: - The complete text of the Critical Infrastructure Protection Reliability Standards (US Federal Energy Regulatory Commission Regulation) (FERC) (2018 Edition) - A table of contents with the page number of each section
Services Computing - SCC 201916th International Conference, Held as Part of the Services Conference Federation, SCF 2019, San Diego, CA, USA, June 25-30, 2019, ProceedingsSpringer
Mumbai is an ever-evolving city, bustling and brimming, never sleeping for a wink. But the past four decades brought upheavals of great magnitude that shaped the city as we know today. Marred by communal riots, gang wars and terrorism, the spirit of Mumbai has emerged indomitable every single time. Born and raised in the lanes of Bombay 3, this is the story of Jagan Kumar who dreams of being a television journalist and changing the world. But once he achieves this, he realises that television journalism has lost its path, now afflicted with sensationalism, corruption and bias. As a crime reporter, he comes across various unscrupulous means that law enforcement agencies adopt to combat organised crime syndicates. He is shocked to witness interdepartmental rivalry that often jeopardises public security. Disenchanted, in conflict with his conscience and confused about his calling, he is about to quit when something happens that changes the course of his life. Bombay 3 begins from the bylanes of old Bombay of the seventies and then takes you to Mosul in ISIS's Iraq of 2014 and finally to the streets of Bangkok where the underworld of Mumbai has spread its tentacles. A fast-paced thriller, it answers certain questions about life in Mumbai and raises a few new ones.
Building on innovative research undertaken by the 'Cloud Legal Project' at Queen Mary, University of London, this work analyses the key legal and regulatory issues relevant to cloud computing under European and English law.
Smart Innovations in Communication and Computational Sciences
Computer Security Handbook
Cyber Risk Leaders
Vaderlandsche chronyk; of Jaarboek van Holland; Zeeland; en Friesland: van de vroegste tyden af tot op den dood van Hertog Albrecht van Beijeren, etc. [Sometimes wrongly attributed to Daniel van Alphen.]
Whitepaper (Final Draft)

16th International Conference, Held as Part of the Services Conference Federation, SCF 2019, San Diego, CA, USA, June 25-30, 2019, Proceedings

A complete update to a classic, respected resource Invaluable reference, supplying a comprehensive overview on how to undertake and present research
"If you've ever been told to 'be more strategic' and wondered how to do it, this is the book for you." —Marshall Goldsmith, #1 New York Times–bestselling author of What Got You Here Won't Get You There Finalist, Business/Careers category, 2018 Best Book Awards sponsored by American Book Fest Strong leaders are those who successfully navigate a great shift: from tactical doer to strategic leader. Regardless of your industry, line of business, or sector, your organization desperately needs strategic leaders—those who are tuned in to the needs of the business, understand how their actions impact corporate objectives, and use data to make smart decisions. Whether leading a department or running a company, a strategic leader propels business performance. Stephen R. Covey famously portrayed a strategic leader as one who was able to climb a tree and tell everyone they were laboring in the wrong jungle. This book lets you start out on the jungle floor and build a ladder to give you that strategic view over the tops of the trees. You'll learn how to: Show up strategic Set meaningful direction Leverage stakeholders Achieve success Make a difference in the areas that matter You'll learn from the personal career journeys of two authors who have taken very different career paths, yet come together to create a proven approach to understanding the big picture of what your organization is trying to accomplish, setting measurable goals, making smart decisions, and continually getting better at what you're doing.
Practical advice from some of today's top early stage investors and entrepreneurs TechStars is a mentorship-driven startup accelerator with operations in three U.S. cities. Once a year in each city, it funds about ten Internet startups with a small amount of capital and surrounds them with around fifty top Internet entrepreneurs and investors. Historically, about seventy-five percent of the companies that go through TechStars raise a meaningful amount of angel or venture capital. Do More Faster: TechStars Lessons to Accelerate Your Startup is a collection of advice that comes from individuals who have passed through, or are part of, this proven program. Each vignette is an exploration of information often heard during the TechStars program and provides practical insights into early stage entrepreneurship. Contains seven sections, each focusing on a major theme within the TechStars program, including idea and vision, fundraising, legal and structure, and work/life balance Created by two highly regarded experts in the world of early stage investing Essays in each section come from the experienced author team as well as TechStar mentors, entrepreneurs, and founders of companies While you'll ultimately have to make your own decisions about what's right for your business, Do More Faster: TechStars Lessons to Accelerate Your Startup can get your entrepreneurial endeavor headed in the right direction.
Even with over $100 billion spent each year on security, attackers break in. They stay hidden and steal data or disrupt with ransomware. Can anything be done to stop the hack?The answer is yes. Intensive reviews of the world's largest hacks uncovered the secret: detect attackers' signals early. This book reveals what those signals are and shows how to detect them. In this game-changing book by Sai Huda, a globally recognized risk and cybersecurity expert, you will: Discover the top 15 signals of cyber attackers' behavior and activity; Find out how these signals can detect the attackers; Discover how these signals were missed and could have detected the attackers in the theft of 3 billion user accounts and in seven other world's largest hacks; Learn how the cloud and Internet of Things (IoT) are danger zones and what are the signals to look for; Find out how to implement the signals in seven steps.With this method you will detect the attackers early, stop the hack and prevent damage. Everyone is at risk. This book will help you take it to the next level so you can stay one step ahead. It is a must-read. Cybersecurity is everyone's business.Grab your copy now to take your cybersecurity to the next level!
The Internet in Everything
Building, Deploying, and Scaling Modern Applications in the Cloud
Unsecurity
Cloud Native DevOps with Kubernetes
Justice a Poem
A History of Emergency Medicine