OMB No. 6195032790564

Applied Cyber Security And The Smart Grid Implementing Security Controls Into The Modern Power Infrastructure

What Is Cyber Security | How It Works? | Cyber Security In 7 Minutes | Cyber Security | Simplilearn 3 Things I Wish I Knew. DO NOT Go Into Cyber Security Without Knowing! □ Cybersecurity for Dummies by Joseph Steinberg (Book Review) What You Should Learn Before \"Cybersecurity\" - 2023 Cybersecurity Books - For Professionals and Executives [And My Favorites] Add These CyberSecurity Books to Your Reading List Cyber Security Full Course 2024 | Cyber Security Course Training For Beginners 2024 | Simplilearn Here's How You Get A Job In Cyber Security With NO EXPERIENCE. 6 Must-Have Security Gadgets That Fit in Your Pocket Why Getting Into Government Technology is Easier Than you Think 3 Things I Wish I Knew. DO NOT Go Into CyberSecurity Without Knowing! the hacker’s roadmap (how to get started in IT in 2023) Add These Cybersecurity Books to Your Reading List | Story Books Top 10: Best Books For Hackers Do you have what it takes to get into Cybersecurity in 2024 2022 Cybersecurity roadmap: How to get started? Cyber Security Certificate Tier List – UPDATED (2023) □ Top 5 Cyber Security Certification 2023 ft. @BittenTech | Simplilearn Top 5 Best Ethical Hacking Books For Beginners | Top 5 Hacking Books | #Shorts | Simplilearn How I Would Learn Cyber Security (If I Could Start Over) Cybersecurity Mastery: Complete Course in a Single Video | Cybersecurity For Beginners How I would Apply to Cyber Security Jobs as a New Person (Viewer Request!) Top 5 Cyber Security Tools | Tools For Cyber Security | Top Cyber Security Tools | Intellipaat How I Would Learn Cyber Security If I Could Start Over in 2024 (6 Month Plan) My Top Hacking / Cyber Security Books In 2023 With InfoSec Pat Top 5 Ethical Hacking Books | Best Books To Learn Ethical Hacking | #Shorts | Simplilearn CERT Applied Data Science for Cybersecurity How I Would Start Learning Cyber Security in 2024 (If I Had To Start Over, Again) 15 BEST Hacking Books for Learning Hacking \u0026 Cybersecurity (from Beginner to Pro)

My Cybersecurity Degree in 7 Minutes (and 32 seconds)
Computer Security Fundamentals
Cybersecurity and Applied Mathematics
Applied Cyber Security and the Smart Grid
Machine Learning for Computer and Cyber Security
Applied Network Security Monitoring
Applied Network Security
Security Policies and Implementation Issues
Computer Security Fundamentals
Proceedings of the International Conference on Applied Cybersecurity (ACS) 2023
Web Application Security, A Beginner's Guide
Modern Cryptography
Improving Web Application Security
Applied Information Security
Cyber Security: Analytics, Technology and Automation
Cyber Security and IT Infrastructure Protection
Security Planning
Applied Incident Response
Applied Cyber-Physical Systems
Essential Cybersecurity Science
Proceedings of the International Conference on Applied CyberSecurity (ACS) 2021
Applied Information Security

Applied Cyber Security And The Smart Grid Implementing Security Controls Into The Modern Power Infrastructure ***OMB No. 6195032790564 edited by***

JOHNNY SHYANNE

Computer Security Fundamentals

Pearson IT Certification
Protect your business and family against cyber attacks Cybersecurity is the protection against the unauthorized or criminal use of electronic data and the practice of ensuring the integrity, confidentiality, and availability of information. Being "cyber-secure" means that a person or organization has both protected itself against attacks by cyber criminals and other online scoundrels, and ensured that it has the ability to recover if it is attacked. If keeping your business or your family safe from cybersecurity threats is on your to-do list, Cybersecurity For Dummies will introduce you to the basics of becoming cyber-secure! You’ll learn what threats exist, and how to identify, protect against, detect, and respond to these threats, as well as how to recover if you have been breached! The who and why of cybersecurity threats Basic cybersecurity concepts What to do to be cyber-secure Cybersecurity careers What to think about to stay cybersecure in the future Now is the time to identify vulnerabilities that may make you a victim of cyber-crime — and to defend yourself before it is too late.
Cybersecurity and Applied Mathematics Springer
Applied Information Security guides students through the installation and basic operation of IT Security software used in the industry today. This text is a great supplement for IT Security textbooks, offering over 21 chapters worth of hands-on assignments.
Applied Cyber Security and the Smart Grid CRC Press
Many people think of the Smart Grid as a power distribution group built on advanced smart metering—but that’s just one aspect of a much larger and more complex system. The "Smart Grid" requires new technologies throughout energy generation, transmission and distribution, and even the homes and businesses being served by the grid. This also represents new information paths between these new systems and services, all of which represents risk, requiring a more thorough approach to where and how cyber security controls are implemented. This insight provides a detailed architecture of the entire Smart Grid, with recommended cyber security measures for everything from the supply chain to the consumer. Discover the potential of the Smart Grid Learn in depth about its systems See its vulnerabilities and how best to protect it
Machine Learning for Computer and Cyber Security Springer Nature
Applied Network Security Monitoring is the essential guide to becoming an NSM analyst from the ground up. This book takes a fundamental approach to NSM, complete with dozens of real-world examples that teach you the key concepts of NSM. Network security monitoring is based on the principle that prevention eventually fails. In the current threat landscape, no matter how much you try, motivated attackers will eventually find their way into your network. At that point, it is your ability to detect and respond to that intrusion that can be the difference between a small incident and a major disaster. The book follows the three stages of the NSM cycle: collection, detection, and analysis. As you progress through each section, you will have access to insights from seasoned NSM professionals while being introduced to relevant, practical scenarios complete with sample data. If you've never performed NSM analysis, Applied Network Security Monitoring will give you an adequate grasp on the core concepts needed to become an effective analyst. If you are already a practicing analyst, this book will allow you to grow your analytic technique to make you more effective at your job. Discusses the proper methods for data collection, and teaches you how to become a skilled NSM analyst Provides thorough hands-on coverage of Snort, Suricata, Bro-IDS, SiLK, and Argus Loaded with practical examples containing real PCAP files you can replay, and uses Security Onion for all its lab examples Companion website includes up-to-date blogs from the authors about the latest developments in NSM
Applied Network Security Monitoring Scientific e-Resources
This book guides readers through building an IT security plan. Offering a template, it helps readers to prioritize risks, conform to regulation, plan their defense and secure proprietary/confidential information. The process is documented in the supplemental online security workbook. Security Planning is designed for the busy IT practitioner, who does not have time to become a security expert, but needs a security plan now. It also serves to educate the reader of a broader set of concepts related to the security environment through the Introductory Concepts and Advanced sections. The book serves entry level cyber-security courses through those in advanced security planning. Exercises range from easier questions to the challenging case study. This is the first text with an optional semester-long case study: Students plan security for a doctor’s office, which must adhere to HIPAA regulation. For software engineering-oriented students, a chapter on secure software development introduces security extensions to UML and use cases (with case study). The text also adopts the NSA’s Center of Academic Excellence (CAE) revamped 2014 plan, addressing five mandatory and 15 Optional Knowledge Units, as well as many ACM Information Assurance and Security core and elective requirements for Computer Science.
IOS Press
Mathematical methods and theories with interdisciplinary applications are presented in this book. The eighteen contributions presented in this Work have been written by eminent scientists; a few papers are based on talks which took place at the International Conference at the Hellenic Artillery School in May 2015. Each paper evaluates possible solutions to long-standing problems such as the solvability of the direct electromagnetic scattering problem, geometric approaches to cyber security, ellipsoid targeting with overlap, non-equilibrium solutions of dynamic networks, measuring ballistic dispersion, elliptic regularity theory for the numerical solution of variational problems, approximation theory for polynomials on the real line and the unit circle, complementarity and variational inequalities in electronics, new two-slope parameterized achievement scalarizing functions for nonlinear multiobjective optimization, and strong and weak convexity of closed sets in a Hilbert space. /divGraduate students, scientists, engineers and researchers in pure and applied mathematical sciences, operations research, engineering, and cyber security will find the interdisciplinary scientific perspectives useful to their overall understanding and further research.
Applied Network Security Syngress
Security Smarts for the Self-Guided IT Professional “Get to know the hackers—or plan on getting hacked. Sullivan and Liu have created a savvy, essentials-based approach to web app security packed with immediately applicable tools for any information security practitioner sharpening his or her tools or just starting out.” —Ryan McGeehan, Security Manager, Facebook, Inc. Secure web applications from today's most devious hackers. Web Application Security: A Beginner's Guide helps you stock your security toolkit, prevent common hacks, and defend quickly against malicious attacks. This practical resource includes chapters on authentication, authorization, and session management, along with browser, database, and file security--all supported by true stories from industry. You'll also get best practices for vulnerability detection and secure development, as well as a chapter that covers essential security fundamentals. This book's templates, checklists, and examples are designed to help you get started right away. Web Application Security: A Beginner's Guide features: Lingo--Common security terms defined so that you're in the know on the job IMHO--Frank and relevant opinions based on the authors' years of industry experience Budget Note--Tips for getting security technologies and processes into your organization's budget In Actual Practice--Exceptions to the rules of security explained in real-world contexts Your Plan--Customizable checklists you can use on the job now Into Action--Tips on how, why, and when to apply new skills and techniques at work

Security Policies and Implementation Issues

CRC Press
Cybersecurity and Applied Mathematics explores the mathematical concepts necessary for effective

cybersecurity research and practice, taking an applied approach for practitioners and students entering the field. This book covers methods of statistical exploratory data analysis and visualization as a type of model for driving decisions, also discussing key topics, such as graph theory, topological complexes, and persistent homology. Defending the Internet is a complex effort, but applying the right techniques from mathematics can make this task more manageable. This book is essential reading for creating useful and replicable methods for analyzing data. Describes mathematical tools for solving cybersecurity problems, enabling analysts to pick the most optimal tool for the task at hand Contains numerous cybersecurity examples and exercises using real world data Written by mathematicians and statisticians with hands-on practitioner experience

Computer Security Fundamentals

John Wiley & Sons
GAME THEORY AND MACHINE LEARNING FOR CYBER SECURITY Move beyond the foundations of machine learning and game theory in cyber security to the latest research in this cutting-edge field In Game Theory and Machine Learning for Cyber Security, a team of expert security researchers delivers a collection of central research contributions from both machine learning and game theory applicable to cybersecurity. The distinguished editors have included resources that address open research questions in game theory and machine learning applied to cyber security systems and examine the strengths and limitations of current game theoretic models for cyber security. Readers will explore the vulnerabilities of traditional machine learning algorithms and how they can be mitigated in an adversarial machine learning approach. The book offers a comprehensive suite of solutions to a broad range of technical issues in applying game theory and machine learning to solve cyber security challenges. Beginning with an introduction to foundational concepts in game theory, machine learning, cyber security, and cyber deception, the editors provide readers with resources that discuss the latest in hypergames, behavioral game theory, adversarial machine learning, generative adversarial networks, and multi-agent reinforcement learning. Readers will also enjoy: A thorough introduction to game theory for cyber deception, including scalable algorithms for identifying stealthy attackers in a game theoretic framework, honeypot allocation over attack graphs, and behavioral games for cyber deception An exploration of game theory for cyber security, including actionable game-theoretic adversarial intervention detection against advanced persistent threats Practical discussions of adversarial machine learning for cyber security, including adversarial machine learning in 5G security and machine learning-driven fault injection in cyber-physical systems In-depth examinations of generative models for cyber security Perfect for researchers, students, and experts in the fields of computer science and engineering, Game Theory and Machine Learning for Cyber Security is also an indispensable resource for industry professionals, military personnel, researchers, faculty, and students with an interest in cyber security.
Proceedings of the International Conference on Applied Cybersecurity (ACS) 2023 Jones & Bartlett Learning
In this book the author draws inspiration from Sun Tzu's Art of War, a work that explains conflict between nations, and he applies this to the computer security setting, examining how we should consider protecting information systems from accidents or malicious attacks. The author first briefly introduces Sun Tzu. Then each chapter in the book takes its inspiration from an original title in The Art of War, where the author offers a general introduction to the content and then describes its application in a cybersecurity setting. These chapters cover estimates; waging war; offensive strategy; how you prepare for an attack; energy; weaknesses and strengths; the variables that need consideration before embarking on a war; how infrastructure is related to the concept of ground; attack by fire or how skilled attackers hide behind noise; and employing secret agents. The book will be interesting for computer security researchers and professionals who would like some grounding in a security mindset.
Web Application Security, A Beginner's Guide John Wiley & Sons
Research Methods for Cyber Security teaches scientific methods for generating impactful knowledge, validating theories, and adding critical rigor to the cyber security field. This book shows how to develop a research plan, beginning by starting research with a question, then offers an introduction to the broad range of useful research methods for cyber security research: observational, mathematical, experimental, and applied. Each research method chapter concludes with recommended outlines and suggested templates for submission to peer reviewed venues. This book concludes with information on cross-cutting issues within cyber security research. Cyber security research contends with numerous unique issues, such as an extremely fast environment evolution, adversarial behavior, and the merging of natural and social science phenomena. Research Methods for Cyber Security addresses these concerns and much more by teaching readers not only the process of science in the context of cyber security research, but providing assistance in execution of research as well. Presents research methods from a cyber security science perspective Catalyzes the rigorous research necessary to propel the cyber security field forward Provides a guided method selection for the type of research being conducted, presented in the context of real-world usage
Modern Cryptography CRC Press
This book serves as a security practitioner’s guide to today’s most crucial issues in cyber security and IT infrastructure. It offers in-depth coverage of theory, technology, and practice as they relate to established technologies as well as recent advancements. It explores practical solutions to a wide range of cyber-physical and IT infrastructure protection issues. Composed of 11 chapters contributed by leading experts in their fields, this highly useful book covers disaster recovery, biometrics, homeland security, cyber warfare, cyber security, national infrastructure security, access controls, vulnerability assessments and audits, cryptography, and operational and organizational security, as well as an extensive glossary of security terms and acronyms. Written with instructors and students in mind, this book includes methods of analysis and problem-solving techniques through hands-on exercises and worked examples as well as questions and answers and the ability to implement practical solutions through real-life case studies. For example, the new format includes the following pedagogical elements: • Checklists throughout each chapter to gauge understanding • Chapter Review Questions/Exercises and Case Studies • Ancillaries: Solutions Manual; slide package; figure files This format will be attractive to universities and career schools as well as federal and state agencies, corporate security training programs, ASIS certification, etc. Chapters by leaders in the field on theory and practice of cyber security and IT infrastructure protection, allowing the reader to develop a new level of technical expertise Comprehensive and up-to-date coverage of cyber security issues allows the reader to remain current and fully informed from multiple viewpoints Presents methods of analysis and problem-solving techniques, enhancing the reader's grasp of the material and ability to implement practical solutions

Improving Web Application Security

O'Reilly Media
This is a monumental reference for the theory and practice of computer security. Comprehensive in scope, this text covers applied and practical elements, theory, and the reasons for the design of applications and security techniques. It covers both the management and the engineering issues of computer security. It provides excellent examples of ideas and mechanisms that demonstrate how disparate techniques and principles are combined in widely-used systems. This book is acclaimed for its scope, clear and lucid writing, and its combination of formal and theoretical aspects with real systems, technologies, techniques, and policies.
Applied Information Security Packt Publishing Ltd
This new volume, edited by industrial and organizational psychologists, will look at the important topic of cyber security work in the US and around the world. With contributions from experts in the fields of industrial and organizational psychology, human factors, computer science, economics, and applied anthropology, the book takes the position that employees in cyber security professions must maintain attention over long periods of time, must make decisions with imperfect information with the potential to exceed their cognitive capacity, may often need to contend with stress and fatigue, and must frequently interact with others in team settings and multiteam systems. Consequently, psychosocial dynamics become a critical driver of cyber security effectiveness. Chapters in the book reflect a multilevel perspective (individuals, teams, multiteam systems) and describe cognitive, affective and behavioral inputs, processes and outcomes that operate at each level. The book chapters also include contributions from both research scientists and cyber security policy-makers/professionals to promote a strong scientist-practitioner dynamic. The intent of the book editors is to inform both theory and practice regarding the psychosocial dynamics of cyber security work.
Cyber Security: Analytics, Technology and Automation Pearson IT Certification
The Cybersecurity Body of Knowledge explains the content, purpose, and use of eight knowledge areas that define the boundaries of the discipline of cybersecurity. The discussion focuses on, and is driven by, the essential concepts of each knowledge area that collectively capture the cybersecurity body of knowledge to provide a complete picture of the field. This book is based on a brand-new and up to this point unique, global initiative, known as CSEC2017, which was created and endorsed by ACM, IEEE-CS, AIS SIGSEC, and IFIP WG 11.8. This has practical relevance to every educator in the discipline of cybersecurity. Because the specifics of this body of knowledge cannot be imparted in a single text, the authors provide the necessary comprehensive overview. In essence, this is the entry-level survey of the comprehensive field of cybersecurity. It will serve as the roadmap for individuals to later drill down into a specific area of interest. This presentation is also explicitly designed to aid faculty members, administrators, CISOs, policy makers, and stakeholders involved with cybersecurity workforce development initiatives. The book is oriented toward practical application of a computing-based foundation, crosscutting concepts, and essential knowledge and skills of the cybersecurity discipline to meet workforce demands. Dan Shoemaker, PhD, is full professor, senior research scientist, and program director at the University of Detroit Mercy’s Center for Cyber Security and Intelligence Studies. Dan is a former chair of the Cybersecurity & Information Systems Department and has authored numerous books and journal articles focused on cybersecurity. Anne Kohnke, PhD, is an associate professor of cybersecurity and the principle investigator of the Center for Academic Excellence in Cyber Defence at the University of Detroit Mercy. Anne’s research is focused in cybersecurity, risk management, threat modeling, and mitigating attack vectors. Ken Sigler, MS, is a faculty member of the Computer Information Systems (CIS) program at the Auburn Hills campus of Oakland Community College in Michigan. Ken’s research is in the areas of software management, software assurance, and cybersecurity.
Cyber Security and IT Infrastructure Protection Springer Nature
This book presents a compendium of selected game- and decision-theoretic models to achieve and assess the security of critical infrastructures. Given contemporary reports on security incidents of various kinds, we can see a paradigm shift to attacks of an increasingly heterogeneous nature, combining different techniques into what we know as an advanced persistent threat. Security precautions must match these diverse threat patterns in an equally diverse manner; in response, this book provides a wealth of techniques for protection and mitigation. Much traditional security research has a narrow focus on specific attack scenarios or applications, and strives to make an attack “practically impossible.” A more recent approach to security views it as a scenario in which the cost of an attack exceeds the potential reward. This does not rule out the possibility of an attack but minimizes its likelihood to the least possible risk. The book follows this economic definition of security, offering a management scientific view that seeks a balance between security investments and their resulting benefits. It focuses on optimization of resources in light of threats such as terrorism and advanced persistent threats. Drawing on the authors’ experience and inspired by real case studies, the book provides a systematic approach to critical infrastructure security and resilience. Presenting a mixture of theoretical work and practical success stories, the book is chiefly intended for students and practitioners seeking an introduction to game- and decision-theoretic techniques for security. The required mathematical concepts are self-contained, rigorously introduced, and illustrated by case studies. The book also provides software tools that help guide readers in the practical use of the scientific models and computational frameworks.
Security Planning Springer Nature
ONE-VOLUME INTRODUCTION TO COMPUTER SECURITY Clearly explains core concepts, terminology, challenges, technologies, and skills Covers today's latest attacks and countermeasures The perfect beginner's guide for anyone interested in a computer security career Dr. Chuck Easttom brings together complete coverage of all basic concepts, terminology, and issues, along with all the skills you need to get started. Drawing on 30 years of experience as a security instructor, consultant, and researcher, Easttom helps you take a proactive, realistic approach to assessing threats and implementing countermeasures. Writing clearly and simply, he addresses crucial issues that many introductory security books ignore, while addressing the realities of a world where billions of new devices are Internet-connected. This guide covers web attacks, hacking, spyware, network defense, security appliances, VPNs, password use, and much more. Its many tips and examples refl ect new industry trends and the state-of-the-art in both attacks and defense. Exercises, projects, and review questions in every chapter help you deepen your understanding and apply all you've learned. LEARN HOW TO Identify and prioritize potential threats to your network Use basic networking knowledge to improve security Get inside the minds of hackers, so you can deter their attacks Implement a proven layered approach to network security Resist modern social engineering attacks Defend against today's most common Denial of Service (DoS) attacks Halt viruses, spyware, worms, Trojans, and other malware Prevent problems arising from malfeasance or ignorance Choose the best encryption methods for your organization Compare security technologies, including the latest security appliances Implement security policies that will work in your environment Scan your network for vulnerabilities Evaluate potential security consultants Master basic computer forensics and know what to do if you're attacked Learn how cyberterrorism and information warfare are evolving

Applied Incident Response

Addison-Wesley Professional
While many resources for network and IT security are available, detailed knowledge regarding modern web application security has been lacking—until now. This practical guide provides both offensive and defensive security concepts that software engineers can easily learn and apply. Andrew Hoffman, a senior security engineer at Salesforce, introduces three pillars of web application

security: recon, offense, and defense. You'll learn methods for effectively researching and analyzing modern web applications—including those you don't have direct access to. You'll also learn how to break into web applications using the latest hacking techniques. Finally, you'll learn how to develop mitigations for use in your own web applications to protect against hackers. Explore common vulnerabilities plaguing today's web applications Learn essential hacking techniques attackers use to exploit applications Map and document web applications for which you don't have direct access Develop and deploy customized exploits that can bypass common defenses Develop and deploy mitigations to protect your applications against hackers Integrate secure coding best practices into your development lifecycle Get practical tips to help you improve the overall security of your web applications

Applied Cyber-Physical Systems Applied Cyber Security and the Smart Grid

With the rising cost of data breaches, executives need to understand the basics of cybersecurity so they can make strategic decisions that keep companies out of headlines and legal battles. Although top executives do not make the day-to-day technical decisions related to cybersecurity, they can direct the company from the top down to have a security mindset. As this book explains, executives can build systems and processes that track gaps and security problems while still allowing for innovation and achievement of business objectives. Many of the data breaches occurring today are the result of fundamental security problems, not crafty attacks by insidious malware. The way many companies are moving to cloud environments exacerbates these problems. However, cloud platforms can also help organizations reduce risk if organizations understand how to leverage their benefits. If and when a breach does happen, a company that has the appropriate metrics can more quickly pinpoint and correct the root cause. Over time, as organizations mature, they can fend off and identify advanced threats more effectively. The book covers cybersecurity fundamentals such as encryption, networking, data breaches, cyber-attacks, malware, viruses, incident handling, governance, risk management, security automation, vendor assessments, and cloud security. RECOMMENDATION: As a former senior military leader, I learned early on that my personal expertise of a subject was less important than my ability to ask better questions of the experts. Often, I had no expertise at all but was required to make critical high risk decisions under very tight time constraints. In this book Teri helps us understand the better questions we should be asking about our data, data systems, networks, architecture development, vendors and cybersecurity writ large and why the answers to these questions matter to our organizations bottom line as well as our personal liability. Teri writes in a conversational tone adding personal experiences that bring life and ease of understanding to an otherwise very technical, complex and sometimes overwhelming subject. Each chapter breaks down a critical component that lends to a comprehensive understanding or can be taken individually. I am not steeped in cyber, but Teri's advice and recommendations have proven critical to my own work on Boards of Directors as well as my leadership work with corporate CISOs, cybersecurity teams, and C-Suite executives. In a time-constrained world this is a worthy read. - Stephen A. Clark, Maj Gen, USAF (Ret) AUTHOR: Teri Radichel (@teriradichel) is the CEO of 2nd Sight Lab, a cloud and cybersecurity training and consulting company. She has a Master of Software Engineering, a Master of Information Security Engineering, and over 25 years of technology, security, and business experience. Her certifications include GSE, GXPN, GCIH, GPEN, GCIA, GCPM, GCCC, and GREM. SANS Institute gave her the 2017 Difference Makers Award for cybersecurity innovation. She is on the IANS (Institute for Applied Network Security) faculty and formerly taught and helped with curriculum for cloud security classes at SANS Institute. She is an AWS hero and runs the Seattle AWS Architects and Engineers Meetup which has over 3000 members. Teri was on the original Capital One cloud team helping with cloud engineering, operations, and security operations. She wrote a paper called Balancing Security and Innovation With Event Driven Automation based on lessons learned from that experience. It explains how companies can leverage automation to improve cybersecurity. She went on to help a security vendor move a product to AWS as a cloud architect and later Director of SaaS Engineering, where she led a team that implemented the concepts described in her paper. She now helps companies around the world with cloud and cyber security as a sought-after speaker, trainer, security researcher, and pentester.

Essential Cybersecurity Science

John Wiley & Sons

Until recently, the Arctic was almost impossible for anyone other than indigenous peoples and explorers to traverse. Pervasive Arctic sea ice and harsh climatological conditions meant that the region was deemed incapable of supporting industrial activity or a Western lifestyle. In the last decade, however, that longstanding reality has been dramatically and permanently altered. Receding sea ice, coupled with growing geopolitical disputes over Arctic resources, territory, and transportation channels, has stimulated efforts to exploit newly-open waterways, to identify and extract desirable resources, and to leverage industrial, commercial, and transportation opportunities emerging throughout the region. This book presents papers from the NATO Advanced Research Workshop (ARW) Governance for Cyber Security and Resilience in the Arctic. Held in Rovaniemi, Finland, from 27-30 January 2019, the workshop brought together top scholars in cybersecurity risk assessment, governance, and resilience to discuss potential analytical and governing strategies and offer perspectives on how to improve critical Arctic infrastructure against various human and natural threats. The book is organized in three sections according to topical group and plenary discussions at the meeting on: cybersecurity infrastructure and threats, analytical strategies for infrastructure threat absorption and resilience, and legal frameworks and governance options to promote cyber resilience. Summaries and detailed analysis are included within each section as summary chapters in the book. The book provides a background on analytical tools relevant to risk and resilience analytics, including risk assessment, decision analysis, supply chain management and resilience analytics. It will allow government, native and civil society groups, military stakeholders, and civilian practitioners to understand better on how to enhance the Arctic's resilience against various natural and anthropogenic challenges.