Cyber Risks I Mia

Corporate litigator Mia Shaw suffers the shock of her life when she finds her colleague and friend brutally murdered. Grief-stricken and furious, Mia vows that she will do anything to seek justice and make the killer pay. The man accused of the murder is a friend of security tech guru Noah Ramirez, but the evidence just doesn't add up. To save his former ATF partner, Noah needs to convince Mia that the real killer is still on the loose. Mia soon has more than the criminal prosecution to worry about, however. She is tasked with taking over her friend's last case and learns he was hiding secrets about his client. She thinks she may have stumbled upon corporate espionage that has turned deadly, but she has no idea of the danger involved. Her only ally is Noah, despite their difference of opinion on the homicide case. Can he win Mia over to his side and protect her from ever-growing threats?
An easy-to-read guide to protecting your digital life and your family online The rise of new technologies in our lives, which has taken us from powerful mobile phones to fitness trackers and smart appliances in under a decade, has also raised the need for everyone who uses these to protect themselves from cyber scams and hackers. Every new device and online service you use that improves your life also opens new doors for attackers looking to discover your passwords, banking accounts, personal photos, and anything else you want to keep secret. In Cyber Smart, author Bart McDonough uses his extensive cybersecurity experience speaking at conferences for the FBI, major financial institutions, and other clients to answer the most common question he hears: "How can I protect myself at home, on a personal level, away from the office?" McDonough knows cybersecurity and online privacy are daunting to the average person so Cyber Smart simplifies online good hygiene with five simple "Brilliance in the Basics" habits anyone can learn. With those habits and his careful debunking of common cybersecurity myths you'll be able to protect yourself and your family from: Identify theft Compromising your children Lost money Lost access to email and social media accounts Digital security is one of the most important, and least understood, aspects of our daily lives. But it doesn't have to be. Thanks to its clear instruction, friendly tone, and practical strategies, Cyber Smart will help you rest more easily, knowing you and your family are protected from digital attack.
The Maidan Revolution in Ukraine created an opportunity for change and reforms in a system that had resisted them for 25 years. This report provides an overview of recommendations for the reform of Ukraine s security and defense institutions."
With the current security crisis in the Ukraine, border security has become a pressing issue. Both the annexation of Crimea and the temporary occupation of the Donbas region represent serious violations of the country's territorial integrity and of the wider international legal order. This book contains 13 presentations delivered during the two-day NATO Advanced Research Workshop (ARW) 'Addressing Security Risks at the Ukrainian Border through Best Practices on Good Governance – Sources and Counter Measures', which took place in Kyiv, Ukraine, in February

2016. The workshop consisted of 5 expert panels devoted to various aspects of building the integrity of the Ukrainian border management agencies to enhance the border security of the eastern flank of NATO. The topics of these panels were: the integrity of the security sector in Ukraine; corruption as a security risk in border management; institutional tools to combat corruption in border management; increasing preparedness for cross-border crises; and bilateral and multilateral dimensions of international cooperation to enhance the integrity of border management agencies. The workshop contributed to raising awareness of emerging border security challenges, as well as providing a forum for the close cooperation of and the exchange of knowledge between the most relevant local and international agencies. It also made possible the discussion of issues such as the current refugee crisis and the implications - for security - of corruption in border management in a wider context.

Cybercrimes

Official Gazette

Executive's Guide to Cyber Risk

A Mia Quinn Mystery

The Making of Modern Georgia, 1918-2012

Securing the Future Today

Cyber Baby

This best-selling guide provides a complete, practical, and thoroughly up-to-date introduction to network and computer security. COMPTIA SECURITY+ GUIDE TO NETWORK SECURITY FUNDAMENTALS, Seventh Edition, maps to the new CompTIA Security+ SY0-601 Certification Exam, providing comprehensive coverage of all domain objectives to help readers prepare for professional certification and career success. Important Notice: Media content referenced within the product description or the product text may not be available in the ebook version.

The publication provides unique and indispensable guidance to all in the insurance industry, other businesses and their counsel in identifying and understanding the risks -- notably including cyber risks -- they face by using social media in the business world and mitigating those risks through a compilation of best practices by industry experts and rulings by courts and regulatory authorities. It features analyses of pertinent policies, statutes, and cases. A few of the Highlights in the 2022-2023 Edition include: • Discussion of developing litigation against social media companies for censoring of online postings. • Discussion of developing litigation against social media companies for censoring of online postings. • Discussion of how informal social media discovery is the new norm and may also be a dereliction of an attorney's duty if an attorney fails to perform social media searches. • Discussion of recent developments in underwriting for cyber and social media risks. •

Analysis of recent case law addressing insurers' utilization of price optimization. • Analysis of recent case law concerning liability in connection with the use of social media. • Discussion of the Strengthening American Cybersecurity Act, which brings in sweeping changes to the federal legal landscape regarding cybersecurity and cyber incident response within critical infrastructure sectors. • Assessing the impact of Artificial Intelligence risks on the insurance industry. • Examining developments in emerging technologies, including virtual reality and augmented reality, and their impact on insurance. • Discussion of the Cyberspace Solarium Commission and the "CSC 2.0 Project." • Discussion of anticipated changes to the National Labor Relations Board's policies for employers' work rules concerning employee use of social media.

This volume addresses American prisoners of war (POW) and missing in action (MIA) cases who were not repatriated following the Korean War, with particular emphasis on whether any American servicemen were transferred to USSR territory during the war.

Adult Science Fiction Trilogy CYBER BABY. Ash, a present-day computer guru, is dragged through time to the year 2022 by a sophisticated and highly-manipulative matriarch in the race to address critical issues of pollution and fuel supply that must use exotic but environmentally sound solutions. Ash teams up with Mia, a beautiful animate powered by a quantum computer brain, they set out to address one of the greatest threats to civilization. But Mia isn't all she appears. Lurking in her unconscious is a powerful and dangerous post-biological entity that was conceived when close to Ash. The Baby's evolution is much the same as for a human baby, but much faster and without moral guidance. The baby develops throughout the story until an unexpected event changes everything. Add to this the babies ability to have unlimited scope for both time travel, and computing power there evolves a very powerful set of sequences manipulated by Cyber Baby, especially when a tempestuous love triangle develops. The world is driven by love, sex and passion. So these elements are carefully woven into the plot to make the story breathtakingly exciting and realistic. Cyber Baby is set against a fast moving backdrop of intrigue, scientific developments, exotic locations in many countries, personal rivalries and passions and has been written for male and female audiences. Be careful Cyber Baby will take your thoughts to another level.144,000 words.

Information Security and Cryptology

InsurTech: A Legal and Regulatory View

Today's Leading Research and Best Practices for Tomorrow's Executives

Hearings Before the Military Personnel Subcommittee of the Committee on National Security, House of Representatives, One Hundred Fourth Congress, First Session, Hearings Held November 20, 30, 1995

Accounting for U.S. POW/MIA's in Southeast Asia

Department of Defense's Comprehensive Review of POW/MIA Cases

Captive In His Bed

This book outlines risk management theory systematically and comprehensively while distinguishing it from academic fields such as insurance theory. In addition, the book builds a risk financing theory that is independent of insurance theory. Until now, risk management (RM) theory has been discussed while the framework of the theory has remained unclear. However, this book, unlike previous books of this type, provides risk management theory after presenting a framework for it. Enterprise risk management (ERM) is seen differently depending on one's position. For accountants, it is a means for internal control to prevent accounting fraud, whereas for financial institutions, it quantifies the risk that administrators can take to meet supervisory standards. Therefore, most of the ERM outlines are written to suit the intended uses or topics, with no systematic RM overviews. This book discusses a systematic RM theory linked to the framework of it, unlike previous books that were written according to topic. After the Enron scandal in December 2001 and WorldCom accounting fraud in June 2002, several laws were enacted or revised throughout the world, such as the SOX Act(Sarbanes-Oxley Act) in the United States and the Financial Instruments and Exchange Law and Companies Act in Japan. In this process, the COSO(Committee of Sponsoring Organizations of Treadway Commission) published their ERM framework, while the ISO (International Organization for Standardization) published their RM framework. The author believes that the competition between these frameworks was an opportunity to systematize RM theory and greatly develop it as an independent discipline from insurance. On the other hand, the Great East Japan Earthquake that occurred on March 11, 2011, caused enormous losses. Also, because pandemics and cyber risks are increasing, businesses must have a comprehensive and systematic ERM for these risks associated with their business activities

The continued growth of e-commerce mandates the emergence of new technical standards and method that will securely integrate online activities with pre-existing infrastructures, laws and processes. Protocols for Secure Electronic Commerce, Second Edition addresses the security portion of this challenge. It is a full compendium of the protocols for securing online commerce and payments, serving as an invaluable resource for students and professionals in the fields of computer science and engineering, IT security, and financial and banking technology. The initial sections provide a broad overview of electronic commerce, money, payment systems, and business-to-business commerce, followed by an examination of well-known protocols (SSL, TLS, WTLS, and SET). The book also explores encryption algorithms and methods, EDI, micropayment, and multiple aspects of digital money. Like its predecessor, this edition is a general analysis that provides many references to more technical resources. It delivers extensive revisions of previous chapters, along with new chapters on electronic commerce in society, new e-commerce systems, and the security of integrated circuit cards.

Maritime Liabilities in a Global and Regional Context consists of edited versions of the papers delivered at the Institute of International Shipping and Trade Law's 13th International Colloquium at Swansea Law School in September 2017. Written by a combination of top academics and highly-experienced legal practitioners, these papers have been carefully co-ordinated to give the reader a first-class insight into the issues surrounding maritime liabilities. The book is set out in two parts: - Part I offers a detailed and critical analysis of issues of contemporary importance concerning maritime liabilities - Part 2 discusses contemporary issues concerning the enforcement of maritime liabilities. An invaluable guide to recent legal and practical developments in maritime liabilities, this book is vital reading for both professional and academic readers.

Cyber-risks are moving targets and societal responses to combat cyber-victimization are often met by

the distrust of young people. Drawing on original research, this book explores how young people define, perceive, and experience cyber-risks, how they respond to both the messages they are receiving from society regarding their safety online, and the various strategies and practices employed by society in regulating their online access and activities. This book complements existing quantitative examinations of cyberbullying assessing its extent and frequency, but also aims to critique and extend knowledge of how cyber-risks such as cyberbullying are perceived and responded to. Following a discussion of their methodology and their experiences of conducting research with teens, the authors discuss the social network services that teens are using and what they find appealing about them, and address teens' experiences with and views towards parental and school-based surveillance. The authors then turn directly to areas of concern expressed by their participants, such as relational aggression, cyberhacking, privacy, and privacy management, as well as sexting. The authors conclude by making recommendations for policy makers, educators and teens – not only by drawing from their own theoretical and sociological interpretations of their findings, but also from the responses and recommendations given by their participants about going online and tackling cyber-risk. One of the first texts to explore how young people respond to attempts to regulate online activity, this book will be key reading for those involved in research and study surrounding youth crime, cybercrime, youth culture, media and crime, and victimology – and will inform those interested in addressing youth safety online how to best approach what is often perceived as a sensitive and volatile social problem.

5th International Workshop, CRITIS 2010, Athens, Greece, September 2010, Revised Papers

Sweet Time

How to Think about Homeland Security

Maritime Organisation, Management and Liability

Addressing Security Risks at the Ukrainian Border Through Best Practices on Good Governance

Proceedings and Debates of the ... Congress

Project SAVE

Accounting for U.S. POW/MIA's in Southeast AsiaHearing Before the Military Personnel Subcommittee of the Committee on National Security, House of Representatives, One Hundred Fourth Congress, First Session, Hearing Held June 28, 1995Maritime Organisation, Management and LiabilityA Legal Analysis of New Challenges in the Maritime IndustryBloomsbury Publishing

Risk detection and cyber security play a vital role in the use and success of contemporary computing. By utilizing the latest technological advances, more effective prevention techniques can be developed to protect against cyber threats. Detecting and Mitigating Robotic Cyber Security Risks is an essential reference publication for the latest research on new methodologies and applications in the areas of robotic and digital security. Featuring extensive coverage on a broad range of topics, such as authentication techniques, cloud security, and mobile robotics, this book is ideally designed for students, researchers, scientists, and engineers seeking current research on methods, models, and implementations of optimized security in digital contexts.

This book argues that we should approach the relationship between climate change and security through the lens of ecosystem resilience.

Unlock the incredible potential of enterprise risk management There has been much evolution in terms of ERM best practices, experience, and standards and regulation over the past decade. Enterprise Risk Management: Today's Leading Research and Best Practices for Tomorrow's Executives, Second Edition is the revised and updated essential guide to the now immensely popular topic of enterprise risk management (ERM). With contributions from leading academics and practitioners, this book offers insights into what practitioners are doing and what the future holds. You'll discover how

you can implement best practices, improve ERM tools and techniques, and even learn to teach ERM. Retaining the holistic approach to ERM that made the first edition such a success, this new edition adds coverage of new topics including cybersecurity risk, ERM in government, foreign exchange risk, risk appetite, innovation risk, outsourcing risk, scenario planning, climate change risk, and much more. In addition, the new edition includes important updates and enhancements to topics covered in the first edition; so much of it has been revised and enhanced that it is essentially an entirely new book. Enterprise Risk Management introduces you to the concepts and techniques that allow you to identify risks and prioritize the appropriate responses. This invaluable guide offers a broad overview, covering key issues while focusing on the principles that drive effective decision making and determine business success. This comprehensive resource also provides a thorough introduction to ERM as it relates to credit, market, and operational risk, as well as the evolving requirements of the board of directors ' role in overseeing ERM. Through the comprehensive chapters and leading research and best practices covered, this book: Provides a holistic overview of key topics in ERM, including the role of the chief risk officer, development and use of key risk indicators and the risk-based allocation of resources Contains second-edition updates covering additional material related to teaching ERM, risk frameworks, risk culture, credit and market risk, risk workshops and risk profiles and much more. Over 90% of the content from the first edition has been revised or enhanced Reveals how you can prudently apply ERM best practices within the context of your underlying business activities Filled with helpful examples, tables, and illustrations, Enterprise Risk Management, Second Edition offers a wealth of knowledge on the drivers, the techniques, the benefits, as well as the pitfalls to avoid, in successfully implementing ERM.

Cyber Smart

Risk, Threats, and the New Normal

The First Georgian Republic and its Successors

Information and Communications Security

Maritime Liabilities in a Global and Regional Context

The Untold Story of the Women Who Took on the U.S. Government to Bring Their Husbands Home

Global Crime: An Encyclopedia of Cyber Theft, Weapons Sales, and Other Illegal Activities [2 volumes]

When most of Eastern Europe was struggling with dictatorships of one kind or another, the Democratic Republic of Georgia (1918–1921) established a constitution, a parliamentary system with national elections, an active opposition, and a free press. Like the Democratic Republic of Georgia in 1918, its successors emerged after 1991 from a bankrupt empire, and faced, yet again, the task of establishing a new economic, political and social system from scratch. In both 1918 and 1991, Georgia was confronted with a hostile Russia and followed a pro-Western and pro-democratic course. The top regional experts in this book explore the domestic and external parallels between the

Georgian post-colonial governments of the early twentieth and twenty-first centuries. How did the inexperienced Georgian leaders in both eras deal with the challenge of secessionism, what were their state building strategies, and what did democracy mean to them? What did their electoral systems look like, why were their economic strategies so different, and how did they negotiate with the international community neighbouring threats. These are the central challenges of transitional governments around the world today. Georgia's experience over one hundred years suggests that both history and contemporary political analysis offer the best (and most interesting) explanation of the often ambivalent outcomes.

A definitive resource for understanding such far-reaching and often interconnected crimes as cyber theft, drug trafficking, human smuggling, identity theft, wildlife poaching, and sex tourism. • Includes primary source documents such as international treaties and conventions related to global crime • Provides quick access to key terms, events, individuals, and organizations playing a key role in combating global crime • Includes suggested sources for additional information in each entry to aid readers who want to examine the topic in more detail • Features scholars and practitioners from more than 10 countries who have specific knowledge of, and experience with, many of the global crimes covered in the work

Terrorism is not a new phenomenon, but almost all communities, regardless of ethnicity, religion, social status or location, are now increasingly facing the challenge of terrorist threat. What makes a terrorist organization attractive to some citizens? A better understanding of the reasons why individuals choose to join terror groups may well enhance efforts to disrupt the recruitment process of terrorist organizations and thereby support current and future counter-terrorism initiatives. This book presents the proceedings of the NATO Advanced Research Workshop, 'Countering Terrorist Recruitment in the Context of Armed Counter-Terrorism Operations', held in Antalya, Turkey, in May 2015. The goal of the workshop was to share existing ideas and develop new ones to tackle terrorist recruitment. The book contains 18 articles covering topics which include: the role of NATO and other international entities in counter-terrorism; understanding

recruitment methods and socialization techniques of terror networks by comparing them to gangs; social media in terrorist recruitment; drug money links with terrorist financing; and counter-terrorism and human rights. The book will be of interest to all those involved in developing, planning and executing prevention programs and policies in relation to both armed and non-armed counter-terrorism operations.

Here's what you get in this book: - 350 practice questions covering the breadth of topics under the Security+ exam, including risk management, application security, and cryptography - Focus on the most frequently asked interview questions. Avoid information overload - Compact format: easy to read, easy to carry, so you can study on-the-go Now, you finally have what you need to crush your cybersecurity certification, and land that dream job. About The Author Mike Spolsky has been building secure software systems since 1999. Early in his career, he developed a lightweight encryption algorithm to secure and sign commerce transactions for mobile phones. His current focus is using machine learning to analyze cyberattacks. He is based in New York City.

Hearing Before the Military Personnel Subcommittee of the Committee on National Security, House of Representatives, One Hundred Fourth Congress, First Session, Hearing Held June 28, 1995

21st International Conference, ICICS 2019, Beijing, China, December 15–17, 2019, Revised Selected Papers

Risk Management

Cyber Risks, Social Media and Insurance: A Guide to Risk Assessment and Management 8/2022-8/2023 Edition

Fundamentals, Theory, and Practice in Asia

Accounting for POW/MIA's from the Korean War and the Vietnam War

A Matter of Trust

"With astonishing verve, The League of Wives persisted to speak truth to power to bring their POW/MIA husbands home from Vietnam. And with astonishing verve, Heath Hardage Lee has chronicled their little-known story a profile of courage that spotlights 1960s-era military wives who forge secret codes with bravery, chutzpah and style. Honestly, I couldn't put it down." Beth Macy, author of Dopesick and Factory Man The true story of the fierce band of women who battled Washington and Hanoi to bring their husbands home from the jungles of Vietnam. On February 12, 1973, one hundred and sixteen men who, just six years earlier, had been high flying Navy and Air Force pilots, shuffled, limped, or were carried off a huge military transport

plane at Clark Air Base in the Philippines. These American servicemen had endured years of brutal torture, kept shackled and starving in solitary confinement, in rat-infested, mosquito-laden prisons, the worst of which was The Hanoi Hilton. Months later, the first Vietnam POWs to return home would learn that their rescuers were their wives, a group of women that included Jane Denton, Sybil Stockdale, Louise Mulligan, Andrea Rander, Phyllis Galanti, and Helene Knapp. These women, who formed The National League of Families, would never have called themselves "feminists," but they had become the POW and MIAs most fervent advocates, going to extraordinary lengths to facilitate their husbands' freedom—and to account for missing military men—by relentlessly lobbying government leaders, conducting a savvy media campaign, conducting covert meetings with antiwar activists, and most astonishingly, helping to code secret letters to their imprisoned husbands. In a page-turning work of narrative non-fiction, Heath Hardage Lee tells the story of these remarkable women for the first time. The League of Wives is certain to be on everyone's must-read list.

A solid, non-technical foundation to help executives and board members understand cyber risk In the Executive's Guide to Cyber Risk: Securing the Future Today, distinguished information security and data privacy expert Siegfried Moyo delivers an incisive and foundational guidance for executives tasked with making sound decisions regarding cyber risk management. The book offers non-technical, business-side executives with the key information they need to understand the nature of cyber risk and its impact on organizations and their growth. In the book, readers will find: Strategies for leading with foresight (as opposed to hindsight) while maintaining the company's vision and objectives Focused, jargon-free explanations of cyber risk that liken it to any other business risk Comprehensive discussions of the fundamentals of cyber risk that enable executive leadership to make well-informed choices Perfect for chief executives in any functional area, the Executive's Guide to Cyber Risk also belongs in the libraries of board members, directors, managers, and other business leaders seeking to mitigate the risks posed by malicious actors or from the failure of its information systems.

This book constitutes the thoroughly refereed post-conference proceedings of the 6th International Conference on Information Security and Cryptology, Inscrypt 2010, held in Shanghai, China, in October 2010. The 35 revised full papers presented were carefully reviewed and selected from 125 submissions. The papers are organized in topical sections on encryption schemes, stream ciphers, sequences and elliptic curves, secure computing, hash functions, key management, digital signatures, privacy and algebraic cryptanalysis, hashing and authentication, and hardware and software issues.

This new textbook offers a systematic introduction to a wide array of cybercrimes, exploring their diversity and the range of possible responses to them. Combining coverage of theoretical perspectives with more technical knowledge, the book is divided into ten chapters which first lay the foundations of the topic and then consider the most important types of cybercrimes – from crimes against devices to political offences – before finally exploring ways to prevent, disrupt, analyse and better comprehend them. Examples from several countries are included, in the attempt to show how crime and deviance in cyberspace are truly global problems, with different countries experiencing comparable sets of challenges. At the same time, the author illustrates how these challenges manifest themselves differently, depending on the socio-legal culture of reference. This text offers an accessible introduction to the topic for all those studying cybercrimes at undergraduate or postgraduate level. Whether students approach the topic from a criminological, legal or computer science perspective, this multidisciplinary approach of this text provides a common language to guide them through the intricacies of criminal and deviant

behaviours in cyberspace.
Detecting and Mitigating Robotic Cyber Security Risks
Game Theory for Cyber Deception
The League of Wives
Digital Citizenship, Privacy and Surveillance
Critical Issues in a Global Context
CompTIA Security + Guide to Network Security Fundamentals
Security Sector Reform in Ukraine

This book introduces game theory as a means to conceptualize, model, and analyze cyber deception. Drawing upon a collection of deception research from the past 10 years, the authors develop a taxonomy of six species of defensive cyber deception. Three of these six species are highlighted in the context of emerging problems such as privacy against ubiquitous tracking in the Internet of things (IoT), dynamic honeynets for the observation of advanced persistent threats (APTs), and active defense against physical denial-of-service (PDoS) attacks. Because of its uniquely thorough treatment of cyber deception, this book will serve as a timely contribution and valuable resource in this active field. The opening chapters introduce both cybersecurity in a manner suitable for game theorists and game theory as appropriate for cybersecurity professionals. Chapter Four then guides readers through the specific field of defensive cyber deception. A key feature of the remaining chapters is the development of a signaling game model for the species of leaky deception featured in honeypots and honeyfiles. This model is expanded to study interactions between multiple agents with varying abilities to detect deception. Game Theory for Cyber Deception will appeal to advanced undergraduates, graduate students, and researchers interested in applying game theory to cybersecurity. It will also be of value to researchers and professionals working on cybersecurity who seek an introduction to game theory.

❤ WARNING! This book contains caramel coffee with rainbow sprinkles, fairy coloring books, Rodents Of Unusual Size, and a hot controlling hero who does dirty things with a whoopie pie. Stuck in a boring insurance job, vivacious Mia Donovan has spent the last few years searching for her life's true path. She fills her time helping plan the wedding of her best friend to the CEO of the Sugar Rush company. Mia has also been trying to attract the impossibly rigid Sugar Rush security chief Gavin Knight. But for well over a year, the unyielding Mr. Knight has ignored her, despite her short skirts, tight sweaters, and patently obvious flirting. And when he finally approaches her, it's only to assess the wedding plans for potential security risks. A former soldier, Gavin has intercepted hostile anonymous letters threatening the high-profile wedding. Determined to keep everyone safe, he's forced to work with

the maddeningly sexy Miss Donovan of the thousand-watt charm and irresistible body. Irked by Gavin's many months of disregard, Mia takes her teasing flirtations to a whole new level. But her coquettish ways are no match for the demanding lover he conceals behind his impassive exterior. And when Gavin exerts his full control, Mia discovers he can protect everything except her heart. SWEET TIME is a hot contemporary romance by New York Times and USA Today bestselling author Nina Lane. It can be read as a standalone or enjoyed as part of the Sugar Rush series. The Sugar Rush series in order: SWEET DREAMS SWEET ESCAPE SWEET SURRENDER SWEET TIME SWEET LIFE

This book identifies and examines the legal challenges facing the shipping industry and ship management today. It first addresses flag state rules and private international law as organisational tools of the shipowner for establishing the applicable legal framework in an age of increasing regulatory activity and extraterritorial effect of legislation. It then focuses on sustainability requirements and the liability of shipping companies managing supply chains and ships as waste. The third section considers challenges stemming from times of financial crisis and deals with the cross-border impact of shipping insolvencies, the UNCITRAL Model Law, and the approaches of different jurisdictions. Finally, the fourth section concerns digitalisation and automation, including delivery on the basis of digital release codes, bills of lading based on blockchain technology, the use of web portals and data sharing, and particular aspects of the law relating to autonomous ships, notably in marine insurance and carriage of goods. The book will be a useful resource for academics and practising lawyers working in shipping and maritime law.

With everything on the line… Flood Zone by Dana Mentink Mia Sandoval’s friend is murdered—and the single mother is a suspect. Her only ally is search-and-rescue worker Dallas Black. Working with the secretive Dallas, Mia discovers he’s as complicated as the murder they’re forced to investigate. Yet as a flood ravages their small Colorado town, a killer is determined that Mia, Dallas and their evidence get swept away to a watery grave. To Save Her Child by Margaret Daley When a young boy goes missing from wilderness day camp, Alaskan search-and-rescue worker Josiah Witherspoon is on the case. The former marine promises to find the child and return him to his mother. But Ella Jackson has a secret that could put them all in danger. Ella and Josiah are ready to risk their lives to save her son, but will they risk their hearts? USA TODAY Bestselling Author Margaret Daley Previously published as Flood Zone and To Save Her Child

Critical Information Infrastructure Security

Protocols for Secure Electronic Commerce
Ecological Security
Hearing Before the Military Personnel Subcommittee of the Committee on National Security, House of Representatives, One Hundred Fourth Congress, Second Session, Hearing Held September 17, - War College Series

Enterprise Risk Management
Five Habits to Protect Your Family, Money, and Identity from Cyber Criminals

This book constitutes the thoroughly refereed post-proceedings of the 5th International Workshop on Critical Information Infrastructure Security, CRITIS 2010, held in Athens, Greece in September 2010. The 12 revised full papers and two poster papers presented went through two rounds of reviewing and improvement and were selected from 30 submissions. The papers included address various techniques to realize the security of systems, communications, and data.

Matthew Knight is ex-security services and half-Comanche Native American. He's as rough, tough and dedicated in the field of risk management as they come. Mia Palmieri is an ordinary woman caught up in an extraordinary situation. Matthew is on Mia's case to unearth the truth about her, and his only option is to kidnap her! But while she's held prisoner in his luxury hideaway, she can't resist his hard-muscled handsomeness. And though their lovemaking is hot and savage, Mia's still got a secret mission to fulfill….

Geek girl Mia Connors has to find her missing friend, solve a murder and clear her name. Read the first book in Julie Anne Lindsey's addictive new mystery series! IT manager Mia Connors is up to her tortoiseshell glasses in technical drama when a glitch in the Horseshoe Falls email system disrupts security and sends errant messages to residents of the gated community. The snafu's timing couldn't be worse—Renaissance Faire season is in full swing and Mia's family's business relies on her presence. Mia doesn't have time to hunt down a computer hacker. Her best friend has disappeared, and she finds another of her friends murdered—in her office. When the hunky new head of Horseshoe Falls security identifies Mia as the prime suspect, her anxiety level registers on the Richter scale. Eager to clear her name, Mia moves into action to locate her missing buddy and find out who killed their friend. But her quick tongue gets her into trouble with more than the new head of security. When Mia begins receiving threats, the killer makes it clear that he's closer than she'd ever imagined. 75,000 words

This book constitutes the refereed proceedings of the 21th International Conference on Information and Communications Security, ICICS 2019, held in Beijing, China, in December 2019. The 47 revised full papers were carefully selected from 199 submissions. The papers are organized in topics on malware analysis and detection, IoT and CPS security enterprise network security, software security, system security, authentication, applied cryptograph internet security, machine learning security, machine learning privacy, Web security, steganography and steganalysis.

Breach of Trust (Atlanta Justice Book #3)

POW/MIA Issues: The Korean War
Congressional Record
A Legal Analysis of New Challenges in the Maritime Industry
A Geek Girl's Guide to Murder
From Theory to Applications
Social Vulnerability & Assessment Framework

When she investigates the death of her best friend and coworker, Colleen, and its connections to the murder of another Seattle prosecutor four years earlier, Mia Quinn finds that many people could have wanted Colleen dead.

Volume 2: Risk, Threats, and the New Normal explains the new political and technological developments that created new domestic national security threats against the nation and the people of the United States.

This Volume of the AIDA Europe Research Series on Insurance Law and Regulation explores the key trends in InsurTech and the potential legal and regulatory issues that accompany them. There is a proliferation of ideas and concepts within InsurTech that will fundamentally change the market in the next few years. These innovations have the potential to change the way the insurance industry works and alter the relationships between customers and insurers, resulting in insurance products that are more closely aligned to individual preferences and priced more appropriately to the risk. Increasing use of technology in the insurance sector is having both a disruptive and transformative impact on areas including product development, distribution, modelling, underwriting and claims and administration practice. The result is a new industry, known as InsurTech. But while the insurance market looks to technology for greater efficiency, regulators are beginning to raise concerns about managing potential risks. The first part of the book examines technological innovations relevant for insurance, such as FinTech, InsurTech, Sharing Economy, and the Internet of Things. The second part then gathers contributions on insurance contract law in a digitalized world, while the third part focuses on cyber insurance and robots. Last but not least, the fourth part of the book discusses legal and ethical questions regarding autonomous vehicles and transportation, including the shipping industry, as well as their impact on the insurance sector and civil liability. Written by legal scholars and practitioners, the book offers international, comparative

and European perspectives. The Chapters "FinTech, InsurTech and the Regulators" by Viktoria Chatzara, "Smart Contracts in Insurance. A Law and Futurology Perspective" by Angelo Borselli and "Room for Compulsory Product Liability Insurance in the European Union for Smart Robots?" by Aysegul Bugra are available open access under a CC BY 4.0 license at link.springer.com. All three open access chapters were funded by BIPAR.

This is a curated and comprehensive collection of the most important works covering matters related to national security, diplomacy, defense, war, strategy, and tactics. The collection spans centuries of thought and experience, and includes the latest analysis of international threats, both conventional and asymmetric. It also includes riveting first person accounts of historic battles and wars.Some of the books in this Series are reproductions of historical works preserved by some of the leading libraries in the world. As with any reproduction of a historical artifact, some of these books contain missing or blurred pages, poor pictures, errant marks, etc. We believe these books are essential to this collection and the study of war, and have therefore brought them back into print, despite these imperfections.We hope you enjoy the unmatched breadth and depth of this collection, from the historical to the just-published works.

Cyber-risk and Youth

RocketPrep CompTIA Security+ Concepts 350 Practice Questions and Answers: Dominate Your Certification Exam

Countering Terrorist Recruitment in the Context of Armed Counter-Terrorism Operations

Deadly Risk

6th International Conference, Inscrypt 2010, Shanghai, China, October 20-24, 2010, Revised Selected Papers