Cyber Liability Insurance Managing The Risks Of Intangible Assets Commercial Lines

Managing Risk and Information Security - Malcolm Harkins 2013-03-21
Managing Risk and Information Security: Protect to Enable, an ApressOpen title, describes the changing risk environment and why a fresh approach to information security is needed. Because almost every aspect of an enterprise is now dependent on technology, the focus of IT security must shift from locking down assets to enabling the business while managing and surviving risk. This compact book discusses business risk from a broader perspective, including privacy and regulatory considerations. It describes the increasing number of threats and vulnerabilities, but also offers strategies for developing solutions. These include discussions of how enterprises can take advantage of new and emerging technologies—such as social media and the huge proliferation of Internet-enabled devices—while minimizing risk. With ApressOpen, content is freely available through multiple online distribution channels and electronic formats with the goal of disseminating professionally edited and technically reviewed content to the worldwide community. Here are some of the responses from reviewers of this exceptional work: “Managing Risk and Information Security is a perceptive, balanced, and often thought-provoking exploration of evolving information risk and security challenges within a business context. Harkins clearly connects the needed, but often-overlooked linkage and dialog between the business and technical worlds and offers actionable strategies. The book contains eye-opening security insights that are easily understood, even by the curious layman.” Fred Wettling, Bechtel Fellow, IS&T Ethics & Compliance Officer, Bechtel “As disruptive technology innovations and escalating cyber threats continue to create enormous information security challenges, Managing Risk and Information Security: Protect to Enable provides a much-needed perspective. This book compels information security professionals to think differently about concepts of risk management in order to be more effective. The specific and practical guidance offers a fast-track formula for developing information security strategies which are lock-step with business priorities.” Laura Robinson, Principal, Robinson Insight Chair, Security for Business Innovation Council (SBIC) Program Director, Executive Security Action Forum (ESAF) “The mandate of the information security function is being completely rewritten. Unfortunately most heads of security haven’t picked up on the change, impeding their companies’ agility and ability to innovate. This book makes the case for why security needs to change, and shows how to get started. It will be regarded as marking the turning point in information security for years to come.” Dr. Jeremy Bergsman, Practice Manager, CEB “The world we are responsible to protect is changing dramatically and at an accelerating pace. Technology is pervasive in virtually every aspect of our lives. Clouds, virtualization and mobile are redefining computing – and they are just the beginning of what is to come. Your security perimeter is defined by wherever your information and people happen to be. We are attacked by professional adversaries who are better funded than we will ever be. We in the information security profession must change as dramatically as the environment we protect. We need new skills and new strategies to do our jobs effectively. We literally need to change the way we think. Written by one of the best in the business, Managing Risk and Information Security challenges traditional security theory with clear examples of the need for change. It also provides expert advice on how to dramatically increase the success of your security strategy and methods – from dealing with the misperception of risk to how to become a Z-shaped CISO. Managing Risk and Information Security is the ultimate treatise on how to deliver effective security to the world we live in for the next 10 years. It is absolute must reading for anyone in our profession – and should be on the desk of every CISO in the world.” Dave Cullinane, CISSP CEO Security Starfish, LLC “In this overview, Malcolm Harkins delivers an insightful survey of the trends, threats, and tactics shaping information risk and security. From regulatory compliance to psychology to the changing threat context, this work provides a compelling introduction to an important topic and trains helpful attention on the effects of changing technology and management practices.” Dr. Mariano-Florentino Cuéllar Professor, Stanford Law School Co-Director, Stanford Center for International Security and Cooperation (CISAC), Stanford University “Malcolm Harkins gets it. In his new book Malcolm outlines the major forces changing the information security risk landscape from a big picture perspective, and then goes on to offer effective methods of managing that risk from a practitioner's viewpoint. The combination makes this book unique and a must read for anyone interested in IT risk." Dennis Devlin AVP, Information Security and Compliance, The George Washington University “Managing Risk and Information Security is the first-to-read, must-read book on information security for C-Suite executives. It is accessible, understandable and actionable. No sky-is-falling scare tactics, no techno-babble – just straight talk about a critically important subject. There is no better primer on the economics, ergonomics and psycho-behaviourals of security than this.” Thornton May, Futurist, Executive Director & Dean, IT Leadership Academy “Managing Risk and Information Security is a wake-up call for information security executives and a ray of light for business leaders. It equips organizations with the knowledge required to transform their security programs from a “culture of no” to one focused on agility, value and competitiveness. Unlike other publications, Malcolm provides clear and immediately applicable solutions to optimally balance the frequently opposing needs of risk reduction and business growth. This book should be required reading for anyone currently serving in, or seeking to achieve, the role of Chief Information Security Officer.” Jamil Farshchi, Senior Business Leader of Strategic Planning and Initiatives, VISA “For too many years, business and security – either real or imagined – were at odds. In Managing Risk and Information Security: Protect to Enable, you get what you expect – real life practical ways to break logjams, have security actually enable business, and marries security architecture and business architecture. Why this book? It's written by a practitioner, and not just any practitioner, one of the leading minds in Security today.” John Stewart, Chief Security Officer, Cisco “This book is an invaluable guide to help security professionals address risk in new ways in this alarmingly fast changing environment. Packed with examples which makes it a pleasure to read, the book captures practical ways a forward thinking CISO can turn information security into a competitive advantage for their business. This book provides a new framework for managing risk in an entertaining and thought provoking way. This will change the way security professionals work with their business leaders, and help get products to market faster. The 6 irrefutable laws of information security should be on a stone plaque on the desk of every security professional.” Steven Proctor, VP, Audit & Risk Management, Flextronics

New Realities in Foreign Affairs - Volker Stanzel 2019-07-08
Moderne Diplomatie wirkt heute in viele Bereiche des modernen Lebens hinein. Sie ist zugleich selbst neuen Einflüssen ausgesetzt. Faktoren, die unsere Gesellschaften verändern, verändern auch unser Regierungshandeln, auch in der Außenpolitik, seien es Digitalisierung, emotionalisierte Sensibilitäten unserer Öffentlichkeiten oder nicht-staatliche internationale Akteure. Derartige Entwicklungen müssen von

der Diplomatie aufgenommen werden, damit sie weiter als Instrument einer Regierung funktionieren kann. Regierungen sollten Wege finden, zwischen den neuen Bedürfnissen der Gesellschaft und den Notwendigkeiten legitimen Regierungshandelns zu vermitteln. Das Ziel sollte sein, als souveräner Staat handeln zu können und zugleich das Potential der tiefgreifenden gesellschaftlichen Veränderungen zu nutzen. Mit Beiträgen von Volker Stanzel, Sascha Lohmann, Andrew Cooper, Christer Jönsson, Corneliu Bjola, Emillie V. de Keulenaar, Jan Melissen, Karsten D. Voigt, Kim B. Olsen, Hanns W. Maull und R. S. Zaharna

Adversarial Risk Analysis - David L. Banks 2015-06-30

Winner of the 2017 De Groot Prize awarded by the International Society for Bayesian Analysis (ISBA)A relatively new area of research, adversarial risk analysis (ARA) informs decision making when there are intelligent opponents and uncertain outcomes. Adversarial Risk Analysis develops methods for allocating defensive or offensive resources against

The Tools and Techniques of Insurance Planning and Risk Management, 4th Edition - Stephan R. Leimberg 2018-10-04

This is the fourth edition of our popular professional resource specifically tailored for non-insurance professionals, newly revised with an increased emphasis on techniques that can be used for personal and business clients. Financial planners, tax advisors, and estate planners have all found this book to be invaluable in their practices because it provides the insights, understanding and tools to guide clients as they seek to manage risk and properly plan insurance coverage. The Tools & Techniques of Insurance Planning and Risk Management, 4th Edition, provides expert guidance on all key personal and business-related policies, including life, health, disability, social insurance, commercial property insurance, workers compensation, business umbrella, directors and officers liability, cyber liability, and much more. In this fully revised and updated edition, respected authors Stephan R. Leimberg, CEO of Leimberg and LeClair, Inc.; Kenneth W. Price; and Jesus M. Pedre provide proven, practical guidance you can apply immediately. Each chapter breaks down complex insurance information so that non-insurance professionals can understand the intricacies of the coverage offered by each product line, allowing planners to insure that their clients have the right type and amount of insurance for their risk profiles This edition delivers: Thirty-two newly updated chapters divided into five sections on the principles of risk and insurance; insurance company operations; personal and commercial insurance lines; life and health insurance planning needs; and commercial property & liability A new chapter on cyber insurance provides information on the most common types of cyber threats faced by businesses today, as well as coverage information about cyber insurance policies to help businesses decide which potential risks can be insured against A new section on commercial flood insurance details the options for how businesses can obtain flood coverage on the private market to protect against ever-more-common flood risks Newly updated materials on the National Flood Insurance Program (NFIP) for homeowners Updated content on personal and business auto policies, including coverage for ride-sharing activities Updated coverage information for managing healthcare cost risks for individuals and businesses, including ACA mandates, disability, and long-term care policies Additionally, the risk management techniques in this book are integrated with up-to-date tax and government insurance information so that planners can incorporate that information into their clients' insurance planning activities to avoid duplicate coverage and take advantage of potential tax savings that are available to individuals and businesses.

Cyber Mayday and the Day After - Daniel Lohrmann 2021-11-16

Successfully lead your company through the worst crises with this first-hand look at emergency leadership Cyber security failures made for splashy headlines in recent years, giving us some of the most spectacular stories of the year. From the Solar Winds hack to the Colonial Pipeline ransomware event, these incidents highlighted the centrality of competent crisis leadership. Cyber Mayday and the Day After offers readers a roadmap to leading organizations through dramatic emergencies by mining the wisdom of C-level executives from around the globe. It’s loaded with interviews with managers and leaders who've been through the crucible and survived to tell the tale. From former FBI agents to Chief Information Security Officers, these leaders led their companies and agencies through the worst of times and share their hands-on wisdom. In this book, you’ll find out: What leaders wish they'd known before an emergency and how they've created a crisis game plan for future situations How executive-level media responses can maintain – or shatter – consumer and public trust in your firm How to use communication, coordination, teamwork, and partnerships with vendors and law enforcement to implement your crisis response Cyber Mayday and the Day After is a must-read experience that offers managers, executives, and other current or aspiring leaders a first-hand look at how to lead others through rapidly evolving crises.

Cyber-Risk Management - Atle Refsdal 2015-10-01

This book provides a brief and general introduction to cybersecurity and cyber-risk assessment. Not limited to a specific approach or technique, its focus is highly pragmatic and is based on established international standards (including ISO 31000) as well as industrial best practices. It explains how cyber-risk assessment should be conducted, which techniques should be used when, what the typical challenges and problems are, and how they should be addressed. The content is divided into three parts. First, part I provides a conceptual introduction to the topic of risk management in general and to cybersecurity and cyber-risk management in particular. Next, part II presents the main stages of cyber-risk assessment from context establishment to risk treatment and acceptance, each illustrated by a running example. Finally, part III details four important challenges and how to reasonably deal with them in practice: risk measurement, risk scales, uncertainty, and low-frequency risks with high consequence. The target audience is mainly practitioners and students who are interested in the fundamentals and basic principles and techniques of security risk assessment, as well as lecturers seeking teaching material. The book provides an overview of the cyber-risk assessment process, the tasks involved, and how to complete them in practice.

Cyber Risk, Market Failures, and Financial Stability - Emanuel Kopp 2017-08-07

Cyber-attacks on financial institutions and financial market infrastructures are becoming more common and more sophisticated. Risk awareness has been increasing, firms actively manage cyber risk and invest in cybersecurity, and to some extent transfer and pool their risks through cyber liability insurance policies. This paper considers the properties of cyber risk, discusses why the private market can fail to provide the socially optimal level of cybersecurity, and explore how systemic cyber risk interacts with other financial stability risks. Furthermore, this study examines the current regulatory frameworks and supervisory approaches, and identifies information asymmetries and other inefficiencies that hamper the detection and management of systemic cyber risk. The paper concludes discussing policy measures that can increase the resilience of the financial system to systemic cyber risk.

The Cyber Risk Handbook - Domenic Antonucci 2017-05-01

Actionable guidance and expert perspective for real-world cybersecurity The Cyber Risk Handbook is the practitioner's guide to implementing, measuring and improving the counter-cyber capabilities of the modern enterprise. The first resource of its kind, this book provides authoritative guidance for real-world situations, and cross-functional solutions for enterprise-wide improvement. Beginning with an overview of counter-cyber evolution, the discussion quickly turns practical with design and implementation guidance for the range of capabilities expected of a robust cyber risk management system that is integrated with the enterprise risk management (ERM) system. Expert contributors from around the globe weigh in on specialized topics with tools and techniques to help any type or size of organization create a robust system tailored to its needs. Chapter summaries of required capabilities are aggregated to provide a new cyber risk maturity model used to benchmark capabilities and to road-map gap-improvement. Cyber risk is a fast-growing enterprise risk, not just an IT risk. Yet seldom is guidance provided as to what this means. This book is the first to tackle in detail those enterprise-wide capabilities expected by Board, CEO and Internal Audit, of the diverse executive management functions that need to team up with the Information Security function in order to provide integrated solutions. Learn how cyber risk management can be integrated to better protect your enterprise Design and benchmark new and improved practical counter-cyber capabilities Examine planning and implementation approaches, models, methods, and more Adopt a new cyber risk maturity model tailored to your enterprise needs The need to manage cyber risk across the enterprise—inclusive of the IT operations—is a growing concern as massive data breaches make the news on an alarmingly frequent basis. With a cyber risk management system now a business-necessary requirement, practitioners need to assess the effectiveness of their current system, and measure its gap-improvement over time in response to a dynamic and fast-moving threat landscape. The Cyber Risk

Handbook brings the world's best thinking to bear on aligning that system to the enterprise and vice-a-versa. Every functional head of any organization must have a copy at-hand to understand their role in achieving that alignment.

Cyber Risks, Social Media and Insurance: A Guide to Risk Assessment and Management - Carrie E. Cope 2021-07-30

This 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.

FISMA and the Risk Management Framework - Stephen D. Gantz 2012-12-31

FISMA and the Risk Management Framework: The New Practice of Federal Cyber Security deals with the Federal Information Security Management Act (FISMA), a law that provides the framework for securing information systems and managing risk associated with information resources in federal government agencies. Comprised of 17 chapters, the book explains the FISMA legislation and its provisions, strengths and limitations, as well as the expectations and obligations of federal agencies subject to FISMA. It also discusses the processes and activities necessary to implement effective information security management following the passage of FISMA, and it describes the National Institute of Standards and Technology's Risk Management Framework. The book looks at how information assurance, risk management, and information systems security is practiced in federal government agencies; the three primary documents that make up the security authorization package: system security plan, security assessment report, and plan of action and milestones; and federal information security-management requirements and initiatives not explicitly covered by FISMA. This book will be helpful to security officers, risk managers, system owners, IT managers, contractors, consultants, service providers, and others involved in securing, managing, or overseeing federal information systems, as well as the mission functions and business processes supported by those systems. Learn how to build a robust, near real-time risk management system and comply with FISMA Discover the changes to FISMA compliance and beyond Gain your systems the authorization they need

Cybersecurity: A Business Solution - Rob Arnold 2017-09-26

As a business leader, you might think you have cybersecurity under control because you have a great IT team. But managing cyber risk requires more than firewalls and good passwords. Cash flow, insurance, relationships, and legal affairs for an organization all play major roles in managing cyber risk. Treating cybersecurity as “just an IT problem” leaves an organization exposed and unprepared. Therefore, executives must take charge of the big picture. Cybersecurity: A Business Solution is a concise guide to managing cybersecurity from a business perspective, written specifically for the leaders of small and medium businesses. In this book you will find a step-by-step approach to managing the financial impact of cybersecurity. The strategy provides the knowledge you need to steer technical experts toward solutions that fit your organization’s business mission. The book also covers common pitfalls that lead to a false sense of security. And, to help offset the cost of higher security, it explains how you can leverage investments in cybersecurity to capture market share and realize more profits. The book’s companion material also includes an executive guide to The National Institute of Standards and Technology (NIST) Cybersecurity Framework. It offers a business level overview of the following key terms and concepts, which are central to managing its adoption. - Tiers - Profiles - Functions - Informative References

Understand, Manage, and Measure Cyber Risk - Ryan Leirvik 2021-12-22

When it comes to managing cybersecurity in an organization, most organizations tussle with basic foundational components. This practitioner’s guide lays down those foundational components, with real client examples and pitfalls to avoid. A plethora of cybersecurity management resources are available—many with sound advice, management approaches, and technical solutions—but few with one common theme that pulls together management and technology, with a focus on executive oversight. Author Ryan Leirvik helps solve these common problems by providing a clear, easy-to-understand, and easy-to-deploy foundational cyber risk management approach applicable to your entire organization. The book provides tools and methods in a straight-forward practical manner to guide the management of your cybersecurity program and helps practitioners pull cyber from a “technical” problem to a “business risk management” problem, equipping you with a simple approach to understand, manage, and measure cyber risk for your enterprise. What You Will Learn Educate the executives/board on what you are doing to reduce risk Communicate the value of cybersecurity programs and investments through insightful risk-informative metrics Know your key performance indicators (KPIs), key risk indicators (KRIs), and/or objectives and key results Prioritize appropriate resources through identifying program-related gaps Lay down the foundational components of a program based on real examples, including pitfalls to avoid Who This Book Is For CISOs, CROs, CIOs, directors of risk management, and anyone struggling to pull together frameworks or basic metrics to quantify uncertainty and address risk

Enhancing the Role of Insurance in Cyber Risk Management - Oecd 2017-10-11

- Foreword - Executive summary - Growing cyber risk and the contribution of insurance to cyber risk management - Types of cyber incidents and losses - The cyber insurance market - Cyber insurance market challenges - Addressing challenges to cyber insurability - Supporting the cyber insurance market through better policies and regulation

Digital Transformation of the Economy: Challenges, Trends and New Opportunities - Svetlana Ashmarina 2019-02-05

This book gathers the best contributions from the conference “Digital Transformation of the Economy: Challenges, Trends and New Opportunities”, which took place in Samara, Russian Federation, on May 29–31, 2018. Organized by Samara State University of Economics (Samara), Russia, the conference was devoted to issues of the digital economy.Presenting international research on the impact of digitalization on economic development, it includes topics such as the transformation of the institutional environment under the influence of informatization, the comparative analysis of the digitalization development in different countries, and modeling the dependence of the rate of change in the economy on the level of the digitalization penetration into various spheres of human activity. It also covers business-process transformation in the context of digitalization and changes in the structure of employment and personnel training for the digital economy. Lastly, it addresses the issue of ensuring information security and dealing with information risks for both individual enterprises and national economies as a whole. The book appeals to both students and researchers whose interests include the development of the digital economy, as well as to managers and professionals who integrate digital solutions into real-world business practice.

Enterprise Cybersecurity in Digital Business - Ariel Evans 2021-12-22

Enterprise Cybersecurity in Digital Business: Building a Cyber Resilient Organization provides a clear guide for companies to understand cyber from a business perspective rather than a technical perspective, and to build resilience for their business.

Insurance Decision-making and Market Behavior - Howard Kunreuther 2006

Considerable evidence suggests that many people for whom insurance is worth purchasing do not have coverage and others who appear not to need financial protection against certain events actually have purchased coverage. There are certain types of events for which one might expect to see insurance widely marketed are now viewed today by insurers as uninsurable and there are other policies one might not expect to be successfully marketed that exist on a relatively large scale. In addition, evidence suggests that cost-effective preventive measures are sometimes rewarded by insurers in ways that could change their clients' behavior. These examples reveal that insurance purchasing and marketing activities do not always produce results that are in the best interest of individuals at risk. Insurance Decision Making and Market Behavior discusses such behavior with the intent of categorizing these insurance "anomalies." It represents a first step in constructing a theory of insurance decision making to explain behavior that does not conform to standard economic models of choice and decision-making. Finally, the authors propose a set of prescriptive solutions for improving insurance decision-making.

Cyberinsurance Policy - Josephine Wolff 2022-08-30

Why cyberinsurance has not improved cybersecurity and what governments can do to make it a more effective tool for cyber risk management. As cybersecurity incidents—ranging from data breaches and denial-of-service attacks to computer fraud and ransomware—become more common, a cyberinsurance industry has emerged to provide coverage for any resulting liability, business interruption, extortion payments, regulatory fines, or repairs. In this book, Josephine Wolff offers the first comprehensive history of cyberinsurance, from the early “Internet Security Liability” policies in the late 1990s to the expansive coverage offered today. Drawing on legal records, government reports, cyberinsurance policies, and interviews with regulators and insurers, Wolff finds that cyberinsurance has not improved cybersecurity or reduced cyber risks. Wolff examines the development of cyberinsurance, comparing it to other insurance sectors, including car and flood insurance; explores legal disputes between insurers and policyholders about whether cyber-related losses were covered under policies designed for liability, crime, or property and casualty losses; and traces the trend toward standalone cyberinsurance policies and government efforts to regulate and promote the industry. Cyberinsurance, she argues, is ineffective at curbing cybersecurity losses because it normalizes the payment of online ransoms, whereas the goal of cybersecurity is the opposite—to disincentivize such payments to make ransomware less profitable. An industry built on modeling risk has found itself confronted by new technologies before the risks posed by those technologies can be fully understood.

Enhancing the Role of Insurance in Cyber Risk Management - OECD 2017-12-08

This report provides an overview of the financial impact of cyber incidents, the coverage of cyber risk available in the insurance market, the challenges to market development and initiatives to address those challenges.

Damage Control - Joseph Brunsman 2020-03-12

Cyber insurance and compliance for the general business community.

Cyber Risk Management - Christopher Hodson 2019

Learn how to prioritize threats, implement a cyber security programme and effectively communicate risks

Corporate Compliance Answer Book - Christopher A. Myers 2018-11

Representing the combined work of more than forty leading compliance attorneys, Corporate Compliance Answer Book helps you develop, implement, and enforce compliance programs that detect and prevent wrongdoing. You'll learn how to: Use risk assessment to pinpoint and reduce your company's areas of legal exposureApply gap analysis to detect and eliminate flaws in your compliance programConduct internal investigations that prevent legal problems from becoming major crisesDevelop records management programs that prepare you for the e-discovery involved in investigations and litigationSatisfy labor and employment mandates, environmental rules, lobbying and campaign finance laws, export control regulations, and FCPA anti-bribery standardsMake voluntary disclosures and cooperate with government agencies in ways that mitigate the legal, financial and reputational damages caused by violationsFeaturing dozens of real-world case studies, charts, tables, compliance checklists, and best practice tips, Corporate Compliance Answer Book pays for itself over and over again by helping you avoid major legal and financial burdens.

The Psychology of Information Security - Leron Zinatullin 2016-01-26

The Psychology of Information Security – Resolving conflicts between security compliance and human behaviour considers information security from the seemingly opposing viewpoints of security professionals and end users to find the balance between security and productivity. It provides recommendations on aligning a security programme with wider organisational objectives, successfully managing change and improving security culture.

Cyber Security And Supply Chain Management: Risks, Challenges, And Solutions - Steven Carnovale 2021-05-25

What are the cyber vulnerabilities in supply chain management? How can firms manage cyber risk and cyber security challenges in procurement, manufacturing, and logistics?Today it is clear that supply chain is often the core area of a firm's cyber security vulnerability, and its first line of defense. This book brings together several experts from both industry and academia to shine light on this problem, and advocate solutions for firms operating in this new technological landscape.Specific topics addressed in this book include: defining the world of cyber space, understanding the connection between supply chain management and cyber security, the implications of cyber security and supply chain risk management, the 'human factor' in supply chain cyber security, the executive view of cyber security, cyber security considerations in procurement, logistics, and manufacturing among other areas.

Navigating New Cyber Risks - Ganna Pogrebna 2019-06-10

This book is a means to diagnose, anticipate and address new cyber risks and vulnerabilities while building a secure digital environment inside and around businesses. It empowers decision makers to apply a human-centred vision and a behavioral approach to cyber security problems in order to detect risks and effectively communicate them. The authors bring together leading experts in the field to build a step-by-step toolkit on how to embed human values into the design of safe human-cyber spaces in the new digital economy. They artfully translate cutting-edge behavioral science and artificial intelligence research into practical insights for business. As well as providing executives, risk assessment analysts and practitioners with practical guidance on navigating cyber risks within their organizations, this book will help policy makers better understand the complexity of business decision-making in the digital age. Step by step, Pogrebna and Skilton show you how to anticipate and diagnose new threats to your business from advanced and AI-driven cyber-attacks.

Confronting Cyber Risk - Gregory J. Falco 2022

"Confronting Cyber Risk: An Embedded Endurance Strategy for Cybersecurity is a practical leadership handbook defining a new strategy for improving cybersecurity and mitigating cyber risk. Written by two leading experts with extensive professional experience in cybersecurity, the book provides CEOs and cyber newcomers alike with novel, concrete guidance on how to implement a cutting-edge strategy to mitigate an organization's overall risk to malicious cyberattacks. Using short, real-world case studies, the book highlights the need to address attack prevention and the resilience of each digital asset while also accounting for an incident's potential impact on overall operations. In a world of hackers, artificial intelligence, and persistent ransomware attacks, the Embedded Endurance strategy embraces the reality of interdependent digital assets and provides an approach that addresses cyber risk at both the micro-(people, networks, systems and data) and macro-(organizational) levels. Most books about cybersecurity focus entirely on technology; the Embedded Endurance strategy recognizes the need for sophisticated thinking with preventative and resilience measures engaged systematically a cross your organization"--

Cyber Liability and Insurance - T. R. Franklin 2009

This book is designed to provide information and guidance to employees of all levels looking for ways to best handle the ever-changing and emerging world of intellectual property, its related issues, and associated risk management concerns. *Information on identifying, managing, and controlling e-risk, including cybercrime and e-discovery *Includes executive's guide for protecting electronically stored information

Managing Cyber Risk in the Financial Sector - Ruth Taplin 2016-01-22

Cyber risk has become increasingly reported as a major problem for financial sector businesses. It takes many forms including fraud for purely monetary gain, hacking by people hostile to a company causing business interruption or damage to reputation, theft by criminals or malicious individuals of the very large amounts of customer information (“big data”) held by many companies, misuse including accidental misuse or lack of use of such data, loss of key intellectual property, and the theft of health and medical data which can have a profound effect on the insurance sector. This book assesses the major cyber risks to businesses and discusses how they can be managed and the risks reduced. It includes case studies of the situation in different financial sectors and countries in relation to East Asia, Europe and the United States. It takes an interdisciplinary approach assessing cyber risks and management solutions from an economic, management risk, legal, security intelligence, insurance, banking and cultural perspective.

Solving Cyber Risk - Andrew Coburn 2018-12-18

The non-technical handbook for cyber security risk management Solving Cyber Risk distills a decade of research into a practical framework for cyber security. Blending statistical data and cost information with research into the culture, psychology, and business models of the hacker community, this book provides business executives, policy-makers, and individuals with a deeper understanding of existing future threats, and an action plan for safeguarding their organizations. Key Risk Indicators reveal vulnerabilities based on organization type, IT infrastructure and existing security measures, while expert discussion from leading cyber risk specialists details practical, real-world methods of risk reduction and mitigation. By the nature of the business, your organization’s customer database is packed with highly sensitive information that is essentially hacker-bait, and even a minor flaw in security protocol could spell disaster. This book takes you deep into the cyber threat landscape to show you how to keep your data secure. Understand who is carrying out cyber-attacks, and why Identify your organization’s risk of attack and vulnerability to damage Learn the most cost-effective risk reduction measures Adopt a new cyber risk assessment and quantification framework based on techniques used by the insurance industry By applying risk management principles to cyber security, non-technical leadership gains a greater understanding of the types of threat, level of threat, and level of investment needed to fortify the organization against attack. Just because you have not been hit does not mean your data is safe, and hackers rely on their targets’ complacence to help maximize their haul. Solving Cyber Risk gives you a concrete action plan for implementing top-notch preventative measures before you’re forced to implement damage control.

Handbook of System Safety and Security - Edward Griffor 2016-10-02

Handbook of System Safety and Security: Cyber Risk and Risk Management, Cyber Security, Adversary Modeling, Threat Analysis, Business of Safety, Functional Safety, Software Systems, and Cyber Physical Systems presents an update on the world's increasing adoption of computer-enabled products and the essential services they provide to our daily lives. The tailoring of these products and services to our personal preferences is expected and made possible by intelligence that is enabled by communication between them. Ensuring that the systems of these connected products operate safely, without creating hazards to us and those around us, is the focus of this book, which presents the central topics of current research and practice in systems safety and security as it relates to applications within transportation, energy, and the medical sciences. Each chapter is authored by one of the leading contributors to the current research and development on the topic. The perspective of this book is unique, as it takes the two topics, systems safety and systems security, as inextricably intertwined. Each is driven by concern about the hazards associated with a system’s performance. Presents the most current and leading edge research on system safety and security, featuring a panel of top experts in the field Includes several research advancements published for the first time, including the use of ‘goal structured notation’ together with a ‘judgment calculus’ and their automation as a ‘rule set’ to facilitate systems safety and systems security process execution in compliance with existing standards Presents for the first time the latest research in the field with the unique perspective that systems safety and systems security are inextricably intertwined Includes coverage of systems architecture, cyber physical systems, tradeoffs between safety, security, and performance, as well as the current methodologies and technologies and implantation practices for system safety and security

Cyberinsurance Policy - Josephine Wolff 2022-08-30

Why cyberinsurance has not improved cybersecurity and what governments can do to make it a more effective tool for cyber risk management. As cybersecurity incidents—ranging from data breaches and denial-of-service attacks to computer fraud and ransomware—become more common, a cyberinsurance industry has emerged to provide coverage for any resulting liability, business interruption, extortion payments, regulatory fines, or repairs. In this book, Josephine Wolff offers the first comprehensive history of cyberinsurance, from the early “Internet Security Liability” policies in the late 1990s to the expansive coverage offered today. Drawing on legal records, government reports, cyberinsurance policies, and interviews with regulators and insurers, Wolff finds that cyberinsurance has not improved cybersecurity or reduced cyber risks. Wolff examines the development of cyberinsurance, comparing it to other insurance sectors, including car and flood insurance; explores legal disputes between insurers and policyholders about whether cyber-related losses were covered under policies designed for liability, crime, or property and casualty losses; and traces the trend toward standalone cyberinsurance policies and government efforts to regulate and promote the industry. Cyberinsurance, she argues, is ineffective at curbing cybersecurity losses because it normalizes the payment of online ransoms, whereas the goal of cybersecurity is the opposite—to disincentivize such payments to make ransomware less profitable. An industry built on modeling risk has found itself confronted by new technologies before the risks posed by those technologies can be fully understood.

Cyber Risk for the Financial Sector: A Framework for Quantitative Assessment - Antoine Bouveret 2018-06-22

Cyber risk has emerged as a key threat to financial stability, following recent attacks on financial institutions. This paper presents a novel documentation of cyber risk around the world for financial institutions by analyzing the different types of cyber incidents (data breaches, fraud and business disruption) and identifying patterns using a variety of datasets. The other novel contribution that is outlined is a quantitative framework to assess cyber risk for the financial sector. The framework draws on a standard VaR type framework used to assess various types of stability risk and can be easily applied at the individual country level. The framework is applied in this paper to the available cross-country data and yields illustrative aggregated losses for the financial sector in the sample across a variety of scenarios ranging from 10 to 30 percent of net income.

Enterprise Security Risk Management - Brian Allen, Esq., CISSP, CISM, CPP, CFE 2017-11-29

As a security professional, have you found that you and others in your company do not always define “security” the same way? Perhaps security interests and business interests have become misaligned. Brian Allen and Rachelle Loyear offer a new approach: Enterprise Security Risk Management (ESRM). By viewing security through a risk management lens, ESRM can help make you and your security program successful. In their long-awaited book, based on years of practical experience and research, Brian Allen and Rachelle Loyear show you step-by-step how Enterprise Security Risk Management (ESRM) applies fundamental risk principles to manage all security risks. Whether the risks are informational, cyber, physical security, asset management, or business continuity, all are included in the holistic, all-encompassing ESRM approach which will move you from task-based to risk-based security. How is ESRM familiar? As a security professional, you may already practice some of the components of ESRM. Many of the concepts – such as risk identification, risk transfer and acceptance, crisis management, and incident response – will be well known to you. How is ESRM new? While many of the principles are familiar, the authors have identified few organizations that apply them in the comprehensive, holistic way that ESRM represents – and even fewer that communicate these principles effectively to key decision-makers. How is ESRM practical? ESRM offers you a straightforward, realistic, actionable approach to deal effectively with all the distinct types of security risks facing you as a security practitioner. ESRM is performed in a life cycle of risk management including: Asset assessment and prioritization. Risk assessment and prioritization. Risk treatment (mitigation). Continuous improvement. Throughout Enterprise Security Risk Management: Concepts and Applications, the authors give you the tools and materials that will help you advance you in the security field, no matter if you are a student, a newcomer, or a seasoned professional. Included are realistic case studies, questions to help you assess your own security program, thought-provoking discussion questions, useful figures and tables, and references for your further reading. By redefining how everyone thinks about the role of security in the enterprise, your security organization can focus on working in partnership with business leaders and other key stakeholders to identify and mitigate security risks. As you begin to use ESRM, following the instructions in this book, you will experience greater personal and professional satisfaction as a security professional – and you’ll become a recognized and trusted partner in the business-critical effort of protecting your enterprise and all its assets.

Global Cyber Security Labor Shortage and International Business Risk - Christiansen, Bryan 2018-10-05

Global events involving cybersecurity breaches have highlighted the ever-growing dependence on interconnected online systems in international business. The increasing societal dependence on information technology has pushed cybersecurity to the forefront as one of the most urgent challenges facing the global community today. Poor cybersecurity is the primary reason hackers are able to penetrate safeguards in business computers and other networks, and the growing global skills gap in cybersecurity simply exacerbates the problem. Global Cyber Security Labor Shortage and International Business Risk provides emerging research exploring the theoretical and practical aspects of protecting computer systems against online threats as well as transformative business models to ensure sustainability and longevity. Featuring coverage on a broad range of topics such as cybercrime, technology security training, and labor market understanding, this book is ideally designed for professionals, managers, IT consultants, programmers, academicians, and students seeking current research on cyber security’s influence on business, education, and social networks.

Cyber Security Management - Peter Trim 2016-05-13

Cyber Security Management: A Governance, Risk and Compliance Framework by Peter Trim and Yang-Im Lee has been written for a wide audience. Derived from research, it places security management in a holistic context and outlines how the strategic marketing approach can be used to underpin cyber security in partnership arrangements. The book is unique because it integrates material that is of a highly specialized nature but which can be interpreted by those with a non-specialist background in the area. Indeed, those with a limited knowledge of cyber security will be able to develop a comprehensive understanding of the subject and will be guided into devising and implementing relevant policy, systems and procedures that make the organization better able to withstand the increasingly sophisticated forms of cyber attack. The book includes a sequence-of-events model; an organizational governance framework; a business continuity management planning framework; a multi-cultural communication model; a cyber security management model and strategic management framework; an integrated governance mechanism; an integrated resilience management model; an integrated management model and system; a communication risk management strategy; and recommendations for counteracting a range of cyber threats. Cyber Security Management: A Governance, Risk and Compliance Framework simplifies complex material and provides a multi-disciplinary perspective and an explanation and interpretation of how managers can manage cyber threats in a pro-active manner and work towards counteracting cyber threats both now and in the future.

Cyber Strategy - Carol A. Siegel 2020-04-13

Cyber Strategy: Risk-Driven Security and Resiliency provides a process and roadmap for any company to develop its unified Cybersecurity and Cyber Resiliency strategies. It demonstrates a methodology for companies to combine their disassociated efforts into one corporate plan with buy-in from senior management that will efficiently utilize resources, target high risk threats, and evaluate risk assessment methodologies and the efficacy of resultant risk mitigations. The book discusses all the steps required from conception of the plan from preplanning (mission/vision, principles, strategic objectives, new initiatives derivation), project management directives, cyber threat and vulnerability analysis, cyber risk and controls assessment to reporting and measurement techniques for plan success and overall strategic plan performance. In addition, a methodology is presented to aid in new initiative selection for the following year by identifying all relevant inputs. Tools utilized include: Key Risk Indicators (KRI) and Key Performance Indicators (KPI) National Institute of Standards and Technology (NIST) Cyber Security Framework (CSF) Target State Maturity interval mapping per initiative Comparisons of current and target state business goals and critical success factors A quantitative NIST-based risk assessment of initiative technology components Responsible, Accountable, Consulted, Informed (RACI) diagrams for Cyber Steering Committee tasks and Governance Boards' approval processes Swimlanes, timelines, data flow diagrams (inputs, resources, outputs), progress report templates, and Gantt charts for project management The last chapter provides downloadable checklists, tables, data flow diagrams, figures, and assessment tools to help develop your company's cybersecurity and cyber resiliency strategic plan.

Security Risk Models for Cyber Insurance - David Rios Insua 2020-12-21

Tackling the cybersecurity challenge is a matter of survival for society at large. Cyber attacks are rapidly increasing in sophistication and magnitude—and in their destructive potential. New threats emerge regularly, the last few years having seen a ransomware boom and distributed denial-of-service attacks leveraging the Internet of Things. For organisations, the use of cybersecurity risk management is essential in order to manage these threats. Yet current frameworks have drawbacks which can lead to the suboptimal allocation of cybersecurity resources. Cyber insurance has been touted as part of the solution – based on the idea that insurers can incentivize companies to improve their cybersecurity by offering premium discounts – but cyber insurance levels remain limited. This is because companies have difficulty determining which cyber insurance products to purchase, and insurance companies struggle to accurately assess cyber risk and thus develop cyber insurance products. To deal with these challenges, this volume presents new models for cybersecurity risk management, partly based on the use of cyber insurance. It contains: A set of mathematical models for cybersecurity risk management, including (i) a model to assist companies in determining their optimal budget allocation between security products and cyber insurance and (ii) a model to assist insurers in designing cyber insurance products. The models use adversarial risk analysis to account for the behavior of threat actors (as well as the behavior of companies and insurers). To inform these models, we draw on psychological and behavioural economics studies of decision-making by individuals regarding cybersecurity and cyber insurance. We also draw on organizational decision-making studies involving cybersecurity and cyber insurance. Its theoretical and methodological findings will appeal to researchers across a wide range of cybersecurity-related disciplines including risk and decision analysis, analytics, technology management, actuarial sciences, behavioural sciences, and economics. The practical findings will help cybersecurity professionals and insurers enhance cybersecurity and cyber insurance, thus benefiting society as a whole. This book grew out of a two-year European Union-funded project under Horizons 2020, called CYBECO (Supporting Cyber Insurance from a Behavioral Choice Perspective).

Managing Cyber Risk - Ariel Evans 2019-03-28

Cyber risk is the second highest perceived business risk according to U.S. risk managers and corporate insurance experts. Digital assets now represent over 85% of an organization's value. In a survey of Fortune 1000 organizations, 83% surveyed described cyber risk as an organizationally complex topic, with most using only qualitative metrics that provide little, if any insight into an effective cyber strategy. Written by one of the foremost cyber risk experts in the world and with contributions from other senior professionals in the field, Managing Cyber Risk provides corporate cyber stakeholders – managers, executives, and directors – with context and tools to accomplish several strategic objectives. These include enabling managers to understand and have proper governance oversight of this crucial area and ensuring improved cyber resilience. Managing Cyber Risk helps businesses to understand cyber risk quantification in business terms that lead risk owners to determine how much cyber insurance they should buy based on the size and the scope of policy, the cyber budget required, and how to prioritize risk remediation based on reputational, operational, legal, and financial impacts. Directors are held to standards of fiduciary duty, loyalty, and care. These insights provide the ability to demonstrate that directors have appropriately discharged their duties, which often dictates the ability to successfully rebut claims made against such individuals. Cyber is a strategic business issue that requires quantitative metrics to ensure cyber resiliency. This handbook acts as a roadmap for executives to understand how to increase cyber resiliency and is unique since it quantifies exposures at the digital asset level.

Measuring and Managing Information Risk - Jack Freund 2014-08-23

Using the factor analysis of information risk (FAIR) methodology developed over ten years and adopted by corporations worldwide, Measuring and Managing Information Risk provides a proven and credible framework for understanding, measuring, and analyzing information risk of any size or complexity. Intended for organizations that need to either build a risk management program from the ground up or strengthen an existing one, this book provides a unique and fresh perspective on how to do a basic quantitative risk analysis. Covering such key areas as risk theory, risk calculation, scenario modeling, and communicating risk within the organization, Measuring and Managing Information Risk helps managers make better business decisions by understanding their organizational risk. Uses factor analysis of information risk (FAIR) as a methodology for measuring and managing risk in any organization. Carefully balances theory with practical applicability and relevant stories of successful implementation. Includes examples from a wide variety of businesses and situations presented in an accessible writing style.

Cyber Threat! - MacDonnell Ulsch 2014-07-14

Conquering cyber attacks requires a multi-sector, multi-modal approach Cyber Threat! How to Manage the Growing Risk of Cyber Attacks is an in-depth examination of the very real cyber security risks facing all facets of government and industry, and the various factors that must align to maintain information integrity. Written by one of the nation's most highly respected cyber risk analysts, the book describes how businesses and government agencies must protect their most valuable assets to avoid potentially catastrophic consequences. Much more than just cyber security, the necessary solutions require government and industry to work cooperatively and intelligently. This resource reveals the extent of the problem, and provides a plan to change course and better manage and protect critical information. Recent news surrounding cyber hacking operations show how intellectual property theft is now a matter of national security, as well as economic and commercial security. Consequences are far-reaching, and can have enormous effects on national economies and international relations. Aggressive cyber forces in China, Russia, Eastern Europe and elsewhere, the rise of global organized criminal networks, and inattention to vulnerabilities throughout critical infrastructures converge to represent an abundantly clear threat. Managing the threat and keeping information safe is now a top priority for global businesses and government agencies. Cyber Threat! breaks the issue down into real terms, and proposes an approach to effective defense. Topics include: The information at risk The true extent of the threat The potential consequences across sectors The multifaceted approach to defense The growing cyber threat is fundamentally changing the nation's economic, diplomatic, military, and intelligence operations, and will extend into future technological, scientific, and geopolitical influence. The only effective solution will be expansive and complex, encompassing every facet of government and industry. Cyber Threat! details the situation at hand, and provides the information that can help keep the nation safe.

Managing Cyber Risk - Ariel Evans 2019

Cyber risk is the second highest perceived business risk according to U.S. risk managers and corporate insurance experts. Digital assets now represent over 85% of an organization's value. In a survey of Fortune 1000 organizations, 83% surveyed described cyber risk as an organizationally complex topic, with most using only qualitative metrics that provide little, if any insight into an effective cyber strategy. Written by one of the foremost cyber risk experts in the world and with contributions from other senior professionals in the field, Managing Cyber Risk provides corporate cyber stakeholders - managers, executives, and directors - with context and tools to accomplish several strategic objectives. These include enabling managers to understand and have proper governance oversight of this crucial area and ensuring improved cyber resilience. Managing Cyber Risk helps businesses to understand cyber risk quantification in business terms that lead risk owners to determine how much cyber insurance they should buy based on the size and the scope of policy, the cyber budget required, and how to prioritize risk remediation based on reputational, operational, legal, and financial impacts. Directors are held to standards of fiduciary duty, loyalty, and care. These insights provide the ability to demonstrate that directors have appropriately discharged their duties, which often dictates the ability to successfully rebut claims made against such individuals. Cyber is a strategic business issue that requires quantitative metrics to ensure cyber resiliency. This handbook acts as a roadmap for executives to understand how to increase cyber resiliency and is unique since it quantifies exposures at the digital asset level. s terms that lead risk owners to determine how much cyber insurance they should buy based on the size and the scope of policy, the cyber budget required, and how to prioritize risk remediation based on reputational, operational, legal, and financial impacts. Directors are held to standards of fiduciary duty, loyalty, and care. These insights provide the ability to demonstrate that directors have appropriately discharged their duties, which often dictates the ability to successfully rebut claims made against such individuals. Cyber is a strategic business issue that requires quantitative metrics to ensure cyber resiliency. This handbook acts as a roadmap for executives to understand how to increase cyber resiliency and is unique since it quantifies exposures at the digital asset level.