Access Free Secure It Up Cyber Insurance Due Diligence Pdf Free Copy

Managing Cyber Risk Oct 06 2021 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.

Enhancing the Role of Insurance in Cyber Risk Management Feb 22 2023 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.

Secure It Up! Jan 21 2023 Alberto Partida's first book, "itsecuriteers," published in 2010, revealed HOW to create an Information Security team that enables business objectives. "Secure IT Up!," his second book, provides qualitative and quantitative insights that justify WHY the adoption of Information Security measures brings benefits to organisations and facilitates cyber-insurance due diligence processes. In the world we live in, risk management and information risk management are complex fields under continuous development. If you need to justify why applying security to your organisation will provide value to your customers or you are involved in cyber insurance due diligence engagements, "Secure it up!" helps you with a statistically sound quantitative study and a set of reputable literature references. "The recommendations in this book are simple but effective: managers will find them of practical relevance and easy to communicate. They are based on sound empirical research which makes them go beyond consultancy speak." Jean-Noel Ezingeard, Dean and

Professor of Processes and Systems Management at Kingston University, London. "Alberto Partida combines a comprehensive analysis of existing literature and the results of surveys of subject matter experts to make his argument for combining Enterprise Risk Management (ERM) with information security practices." Richard Stiennon, Chief Research Analyst at IT-Harvest, Author of "Surviving Cyberwar,""Cyber Defense: Countering Targeted Attacks," Blogger at forbes.com, Michigan. Alberto is an information security analyst. He blogs at securityandrisk.blogspot.com and tweets as @itsecuriteer.

7 Rules To Become Exceptional At Cyber Security Mar 31 2021 What every current and aspiring cyber security leader and professional needs to know to become truly exceptional. Bridging the gap between business and cyber security. Actionable rules to maximise value from cyber security and address cyber threats. Differentiating skills for professional excellence and massive career success. In a hyperconnected world powered by technology, the importance of cyber security to our collective prosperity and progress has never been greater. Using practical and real-world experiences, this book introduces seven rules for cyber security leaders and professionals to deliver immense value to their organisations while rapidly progressing in their own careers. The book also gives senior executives a view of what good looks like from a cyber security perspective so they can be more effective in accomplishing their objectives and supporting their teams. Moving beyond unnecessary technical jargon, buzzwords, and hype, the book delivers valuable insights into the strategies,

opportunities, and approaches associated with building and running exceptional cyber security programs that truly enable organisations. These insights include: - Tangible ways to adopt a business-aligned mindset, incorporate risk-based approaches and relevant measurements to demonstrate progress, inspire confidence, and optimise investments. - Addressing the critical roles of human factor and culture to the success of cyber security endeavours. - Elements for building and executing fit-for-purpose and comprehensive cyber security strategies. - Mastering differentiating skills and brand building, including writing, storytelling, networking, and communication for continued professional and personal career growth and success.

How Has Ransomware Changed Cyber Insurance? Nov 19 2022 Recent threat reports show that in 2021 the entire globe experienced twenty ransomware attacks every second of every day [1]. That means cybercriminals attempted to infiltrate systems over 1.7 million times a day. Ransomware recovery costs in 2021 were estimated at $4.62 million [2], and this does not include the ransom payment. In 94% of the incidents, a cyber insurance company pays the ransom [3]. Reports and statistics may differ, but all agree that the cyber insurance industry is severely affected by ransomware. With the alarming rate of ransomware attacks, how has cyber insurance changed? This project explores the increase in ransomware attacks and their effect on the cyber insurance industry. These effects include increased premium rates, restrictions in terms/limits, and exclusions to policies. A few companies offering cyber insurance have created cybersecurity scores that will enable them to assess the

cyber risk of policyholders better and offer services with their policies. Similarly, in the way that banks use credit scores to assess the person getting the loan [4]. This project discusses ways that policyholders are using to mitigate their cyber risks, such as using lawyers to lead the investigation and direct them through regulatory requirements before using an incident response team [5]. This project also explores the idea of using the Terrorism Risk Insurance Program (TRIP) via the Terrorism Risk Insurance Act (TRIA) to help the cyber insurance market subsidize data breaches and stabilize the current cyber insurance inflation. The project describes mitigation approaches that cyber insurance companies are using to aid the policyholders in lowering their cyber risks.

Cyber Strategy Feb 27 2021 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.

Guide to Cybersecurity Due Diligence in M&A Transactions Dec 08 2021 "In the digital era, ubiquitous connectivity has spared no enterprise the risks of being hacked from anywhere in the world. The reality of this threat, coupled with the near total dependence of today's businesses on networked digital technology, presents a major risk of catastrophic consequences to most businesses. And acquiring or merging with any business involves taking on that risk. Thus, in any M&A transaction, an evaluation of the target's cybersecurity capabilities and experience is critical. [This book] is designed to assist companies and their counsel in assessing that risk. Detailed and easy-to-read, this comprehensive guide includes discussions on recent cyber

incidents, including Nieman Marcus, Yahoo, Target Corporation, Sony Pictures, and Volkswagen."--

At the Nexus of Cybersecurity and Public Policy Jan 29 2021 We depend on information and information technology (IT) to make many of our day-to-day tasks easier and more convenient. Computers play key roles in transportation, health care, banking, and energy. Businesses use IT for payroll and accounting, inventory and sales, and research and development. Modern military forces use weapons that are increasingly coordinated through computer-based networks. Cybersecurity is vital to protecting all of these functions. Cyberspace is vulnerable to a broad spectrum of hackers, criminals, terrorists, and state actors. Working in cyberspace, these malevolent actors can steal money, intellectual property, or classified information; impersonate law-abiding parties for their own purposes; damage important data; or deny the availability of normally accessible services. Cybersecurity issues arise because of three factors taken together - the presence of malevolent actors in cyberspace, societal reliance on IT for many important functions, and the presence of vulnerabilities in IT systems. What steps can policy makers take to protect our government, businesses, and the public from those would take advantage of system vulnerabilities? At the Nexus of Cybersecurity and Public Policy offers a wealth of information on practical measures, technical and nontechnical challenges, and potential policy responses. According to this report, cybersecurity is a never-ending battle; threats will evolve as adversaries adopt new tools and techniques to compromise security. Cybersecurity is

therefore an ongoing process that needs to evolve as new threats are identified. At the Nexus of Cybersecurity and Public Policy is a call for action to make cybersecurity a public safety priority. For a number of years, the cybersecurity issue has received increasing public attention; however, most policy focus has been on the short-term costs of improving systems. In its explanation of the fundamentals of cybersecurity and the discussion of potential policy responses, this book will be a resource for policy makers, cybersecurity and IT professionals, and anyone who wants to understand threats to cyberspace.

Cyber Risks, Social Media and Insurance: A Guide to Risk Assessment and Management 8/2022-8/2023 Edition Apr 12 2022 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.

Readings & Cases in Information Security: Law & Ethics Oct 26 2020 Readings and Cases in Information Security: Law and Ethics provides a depth of content and analytical viewpoint not found in many other books. Designed for use with any Cengage Learning security text, this resource offers readers a real-life view of information security management, including the ethical and legal issues associated with various on-the-job experiences. Included are a wide selection of foundational readings and scenarios from a variety of experts to give the reader the most realistic perspective of a career in information security. Important Notice: Media content referenced within the product description or the product text may not be available in the ebook version.

Manager Cyber Security Critical Questions Skills

Assessment Jul 03 2021 You want to know how to evaluate the effectiveness of your organizations cybersecurity program. In order to do that, you need the answer to why should cybersecurity and data security risk be on your radar? The problem is what are the physical security and cybersecurity changes that will be required, which makes you feel asking does your organization have a documented cybersecurity policy in place? We believe there is an answer to problems like does the target organization have a cybersecurity incident response plan. We understand you need to assure ourselves that your organizations approach to cybersecurity is effective which is why an answer to 'does your organization have any cybersecurity training or awareness programs?' is important. Here's how you do it with this book: 1. Assure yourselves that your organizations approach to cybersecurity is effective 2. Manage unclear Manager Cyber Security skills requirements 3. Go about comparing Manager Cyber Security skills approaches/solutions So, does your organization have an information and/or cybersecurity policy? This Manager Cyber Security Critical Questions Skills Assessment book puts you in control by letting you ask what's important, and in the meantime, ask yourself; do you have an organized plan for responding to a security breach? So you can stop wondering 'do you have cybersecurity insurance that covers data breaches?' and instead find a solution having the ability to test the security and the performance of a system. This Manager Cyber Security Guide is unlike books you're used to. If you're looking for a textbook, this might not be for you. This book and its included digital components is for you who

understands the importance of asking great questions. This gives you the questions to uncover the Manager Cyber Security challenges you're facing and generate better solutions to solve those problems. INCLUDES all the tools you need to an in-depth Manager Cyber Security Skills Assessment. Featuring new and updated case-based questions, organized into seven core levels of Manager Cyber Security maturity, this Skills Assessment will help you identify areas in which Manager Cyber Security improvements can be made. In using the questions you will be better able to: Diagnose Manager Cyber Security projects, initiatives, organizations, businesses and processes using accepted diagnostic standards and practices. Implement evidence-based best practice strategies aligned with overall goals. Integrate recent advances in Manager Cyber Security and process design strategies into practice according to best practice guidelines. Using the Skills Assessment tool gives you the Manager Cyber Security Scorecard, enabling you to develop a clear picture of which Manager Cyber Security areas need attention. Your purchase includes access to the Manager Cyber Security skills assessment digital components which gives you your dynamically prioritized projects-ready tool that enables you to define, show and lead your organization exactly with what's important.

Building a Cyber Resilient Business Dec 28 2020 Learn how to build a proactive cybersecurity culture together with the rest of your C-suite to effectively manage cyber risks Key Features Enable business acceleration by preparing your organization against cyber risks Discover tips and tricks to

manage cyber risks in your organization and build a cyber resilient business Unpack critical questions for the C-suite to ensure the firm is intentionally building cyber resilience Book Description With cyberattacks on the rise, it has become essential for C-suite executives and board members to step up and collectively recognize cyber risk as a top priority business risk. However, non-cyber executives find it challenging to understand their role in increasing the business's cyber resilience due to its complex nature and the lack of a clear return on investment. This book demystifies the perception that cybersecurity is a technical problem, drawing parallels between the key responsibilities of the C-suite roles to line up with the mission of the Chief Information Security Officer (CISO). The book equips you with all you need to know about cyber risks to run the business effectively. Each chapter provides a holistic overview of the dynamic priorities of the C-suite (from the CFO to the CIO, COO, CRO, and so on), and unpacks how cybersecurity must be embedded in every business function. The book also contains self-assessment questions, which are a helpful tool in evaluating any major cybersecurity initiatives and/or investment required. With this book, you'll have a deeper appreciation of the various ways all executives can contribute to the organization's cyber program, in close collaboration with the CISO and the security team, and achieve a cyber-resilient, profitable, and sustainable business. What you will learn Understand why cybersecurity should matter to the C-suite Explore how different roles contribute to an organization's security Discover how priorities of roles affect an executive's

contribution to security Understand financial losses and business impact caused by cyber risks Come to grips with the role of the board of directors in cybersecurity programs Leverage the recipes to build a strong cybersecurity culture Discover tips on cyber risk quantification and cyber insurance Define a common language that bridges the gap between business and cybersecurity Who this book is for This book is for the C-suite and executives who are not necessarily working in cybersecurity. The guidebook will bridge the gaps between the CISO and the rest of the executives, helping CEOs, CFOs, CIOs, COOs, etc., to understand how they can work together with the CISO and their team to achieve organization-wide cyber resilience for business value preservation and growth.

Cyber-Security in Critical Infrastructures Jul 23 2020 This book presents a compendium of selected game- and decision-theoretic models to achieve and assess the security of critical infrastructures. Given contemporary reports on security incidents of various kinds, we can see a paradigm shift to attacks of an increasingly heterogeneous nature, combining different techniques into what we know as an advanced persistent threat. Security precautions must match these diverse threat patterns in an equally diverse manner; in response, this book provides a wealth of techniques for protection and mitigation. Much traditional security research has a narrow focus on specific attack scenarios or applications, and strives to make an attack “practically impossible.” A more recent approach to security views it as a scenario in which the cost of an attack exceeds the potential reward. This does not rule out the possibility of an attack but

minimizes its likelihood to the least possible risk. The book follows this economic definition of security, offering a management scientific view that seeks a balance between security investments and their resulting benefits. It focuses on optimization of resources in light of threats such as terrorism and advanced persistent threats. Drawing on the authors' experience and inspired by real case studies, the book provides a systematic approach to critical infrastructure security and resilience. Presenting a mixture of theoretical work and practical success stories, the book is chiefly intended for students and practitioners seeking an introduction to game- and decision-theoretic techniques for security. The required mathematical concepts are self-contained, rigorously introduced, and illustrated by case studies. The book also provides software tools that help guide readers in the practical use of the scientific models and computational frameworks.

Global Cyber Security Labor Shortage and International Business Risk Dec 16 2019 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.

Pricing Cyber Security Insurance Mar 11 2022 Cybersecurity breaches may be correlated due to geography, similar infrastructure, or use of a third-party contractor. We show how a copula model may be used to estimate the probability of an attack where breaches may be correlated among firms. Losses arising from cybersecurity breaches have an unknown distribution. We propose the stock price reaction to a breach as an objective measure of the loss in wealth sustained by the firm due to a breach, a loss that can be modeled and that insurers can use to price cyberinsurance products. This loss measure reflects the immediate and long-term effects of a breach, including reputational effects and other intangible impacts that are otherwise more difficult to quantify. We examine stock returns for 258 cybersecurity breach announcements over 2011-2016 in order to obtain the empirical loss distribution. We find a five-day abnormal return of -1.44%. Seventy-one percent of these 258 announcements result in a negative abnormal return, and a gamma distribution provides an excellent fit to these losses. In addition to introducing a

copula model for correlated losses, our study shows that insurers can use either the empirical stock market distribution of losses or the theoretical (gamma) distribution in the pricing of cyberinsurance.

Cyberinsurance Policy Nov 07 2021 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.

Solving Cyber Risk Dec 20 2022 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.

Cyber Insurance Roundtable Readout Report Aug 16 2022 DHS held a series of roundtables on cybersecurity with health industry representatives. The industry representatives, all of them Chief Information Security Officers (CISOs) or risk manager equivalents, hailed from a variety of organizations including an academic medical center and research university, a university hospital system, and a medical vendor that provides health care consumer products, pharmaceuticals, and medical devices/technology. Although each presented very different cyber risk management use cases, they shared many of the same challenges while addressing them. They consequently directed their remarks to three principal topics during the roundtable discussions: (1) making the case for cybersecurity investments to senior leadership; (2) incorporating cost/benefit considerations into their arguments; and (3) negotiating the boundary between risk mitigation efforts and risk transfer/insurance options to promote more effective cyber risk management strategies.

EIOPA Strategy on Cyber Underwriting May 01 2021 EIOPA's strategic priorities take into account the European Commission's Digital Strategy, Cybersecurity Strategy and

FinTech Action Plan and support its ambition for a Digital Single Market . The Digital Single Market is built on 3 pillars: 1. Better access for consumers and businesses to digital goods and services across Europe; 2. Creating the right conditions and a level playing field for digital networks and innovative services to flourish; 3. Maximising the growth potential of the digital economy. A sound cyber insurance market can be a crucial enabler of the digital economy. In particular, a well-developed cyber insurance market can help: › To raise awareness of businesses to the risks and losses that can result from cyber-attacks; › To share knowledge of good cyber security and risk management practices; › To encourage investment in risk reduction and the use of risk-based premiums; › To facilitate responses to and recovery from cyber- attacks. 1 https://ec.europa.eu/digital-single-market/en/cyber-security 2 https://ec.europa.eu/digital-single-market/en/policies/shaping-digital- single-market Appropriate cyber insurance coverages, underwriting practices and sound supervision can make a valuable contribution to managing cyber risk faced by individuals, businesses and organisations and to enhance cyber resilience, ultimately enabling the digital economy. In this context, EIOPA has been developing a number of initiatives and highlighting supervisory concerns, specifically in the area of silent/non-affirmative risks as well as of accumulation of risk. It is now time to further close knowledge and data gaps regarding cyber risks and cyber underwriting in particular.

Cyber Risk for the Financial Sector: A Framework for

Quantitative Assessment Feb 10 2022 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.

Digital Asset Valuation and Cyber Risk Measurement Oct 18 2022 Digital Asset Valuation and Cyber Risk Measurement: Principles of Cybernomics is a book about the future of risk and the future of value. It examines the indispensable role of economic modeling in the future of digitization, thus providing industry professionals with the tools they need to optimize the management of financial risks associated with this megatrend. The book addresses three problem areas: the valuation of digital assets, measurement of risk exposures of digital valuables, and economic modeling for the management of such risks. Employing a pair of novel cyber risk measurement units, bitmort and hekla, the book covers areas of value, risk, control, and return, each of which are viewed from the

perspective of entity (e.g., individual, organization, business), portfolio (e.g., industry sector, nation-state), and global ramifications. Establishing adequate, holistic, and statistically robust data points on the entity, portfolio, and global levels for the development of a cybernomics databank is essential for the resilience of our shared digital future. This book also argues existing economic value theories no longer apply to the digital era due to the unique characteristics of digital assets. It introduces six laws of digital theory of value, with the aim to adapt economic value theories to the digital and machine era. Comprehensive literature review on existing digital asset valuation models, cyber risk management methods, security control frameworks, and economics of information security Discusses the implication of classical economic theories under the context of digitization, as well as the impact of rapid digitization on the future of value Analyzes the fundamental attributes and measurable characteristics of digital assets as economic goods Discusses the scope and measurement of digital economy Highlights cutting-edge risk measurement practices regarding cybersecurity risk management Introduces novel concepts, models, and theories, including opportunity value, Digital Valuation Model, six laws of digital theory of value, Cyber Risk Quadrant, and most importantly, cyber risk measures hekla and bitmort Introduces cybernomics, that is, the integration of cyber risk management and economics to study the requirements of a databank in order to improve risk analytics solutions for (1) the valuation of digital assets, (2) the measurement of risk exposure of digital assets, and (3)

the capital optimization for managing residual cyber risK Provides a case study on cyber insurance

Assessing and Insuring Cybersecurity Risk May 13 2022 Remote workforces using VPNs, Cloud-based infrastructure and critical systems, and a proliferation in phishing attacks and fraudulent websites are all raising the level of risk for every company. It all comes down to just one thing that is at stake: how to gauge a company's level of cyber risk and the tolerance level for this risk. Loosely put, this translates to how much level of uncertainty an organization can tolerate before the uncertainty starts to negatively affect mission critical flows and business processes. Trying to gauge this can be a huge and nebulous task for any IT security team to accomplish. Making this task so difficult are the many frameworks and models that can be utilized. It is very confusing to know which one to utilize in order to achieve a high level of security. Complicating this situation further is that both quantitative and qualitative variables must be taken into consideration and deployed into a cyber risk model. Assessing and Insuring Cybersecurity Risk provides an insight into how to gauge an organization's particular level of cyber risk, and what would be deemed appropriate for the organization's risk tolerance. In addition to computing the level of cyber risk, an IT security team has to determine the appropriate controls that are needed to mitigate cyber risk. Also to be considered are the standards and best practices that the IT security team has to implement for complying with such regulations and mandates as CCPA, GDPR, and HIPAA. To help a security team to comprehensively assess an organization's cyber risk

level and how to insure against it, the book covers: The mechanics of cyber risk Risk controls that need to be put into place The issues and benefits of cybersecurity risk insurance policies GDPR, CCPA, and the CMMC Gauging how much cyber risk and uncertainty an organization can tolerate is a complex and complicated task, and this book helps to make it more understandable and manageable.

Machine Learning for Computer and Cyber Security

Jun 02 2021 While Computer Security is a broader term which incorporates technologies, protocols, standards and policies to ensure the security of the computing systems including the computer hardware, software and the information stored in it, Cyber Security is a specific, growing field to protect computer networks (offline and online) from unauthorized access, botnets, phishing scams, etc. Machine learning is a branch of Computer Science which enables computing machines to adopt new behaviors on the basis of observable and verifiable data and information. It can be applied to ensure the security of the computers and the information by detecting anomalies using data mining and other such techniques. This book will be an invaluable resource to understand the importance of machine learning and data mining in establishing computer and cyber security. It emphasizes important security aspects associated with computer and cyber security along with the analysis of machine learning and data mining based solutions. The book also highlights the future research domains in which these solutions can be applied. Furthermore, it caters to the needs of IT professionals, researchers, faculty members, scientists, graduate students,

research scholars and software developers who seek to carry out research and develop combating solutions in the area of cyber security using machine learning based approaches. It is an extensive source of information for the readers belonging to the field of Computer Science and Engineering, and Cyber Security professionals. Key Features: This book contains examples and illustrations to demonstrate the principles, algorithms, challenges and applications of machine learning and data mining for computer and cyber security. It showcases important security aspects and current trends in the field. It provides an insight of the future research directions in the field. Contents of this book help to prepare the students for exercising better defense in terms of understanding the motivation of the attackers and how to deal with and mitigate the situation using machine learning based approaches in better manner.

Trust, Privacy and Security in Digital Business Oct 14 2019 This book constitutes the refereed proceedings of the 17th International Conference on Trust, Privacy and Security in Digital Business, TrustBus 2020, held in Bratislava, Slovakia, in September 2020. The conference was held virtually due to the COVID-19 pandemic. The 11 full and 4 short papers presented were carefully reviewed and selected from 28 submissions. The papers are organized in the following topical sections: blockchain, cloud security/hardware; economics/privacy; human aspects; privacy; privacy and machine learning; trust.

Decision and Game Theory for Security Sep 24 2020 This book constitutes the refereed proceedings of the Second International Conference on Decision and Game Theory for

Security, GameSec 2011, held in College Park, Maryland, USA, in November 2011. The 16 revised full papers and 2 plenary keynotes presented were carefully reviewed and selected from numerous submissions. The papers are organized in topical sections on attacks, adversaries, and game theory, wireless adhoc and sensor networks, network games, security insurance, security and trust in social networks and security investments.

Data Breach Preparation and Response May 21 2020 Data Breach Preparation and Response: Breaches are Certain, Impact is Not is the first book to provide 360 degree visibility and guidance on how to proactively prepare for and manage a data breach and limit impact. Data breaches are inevitable incidents that can disrupt business operations and carry severe reputational and financial impact, making them one of the largest risks facing organizations today. The effects of a breach can be felt across multiple departments within an organization, who will each play a role in effectively managing the breach. Kevvie Fowler has assembled a team of leading forensics, security, privacy, legal, public relations and cyber insurance experts to create the definitive breach management reference for the whole organization. Discusses the cyber criminals behind data breaches and the underground dark web forums they use to trade and sell stolen data Features never-before published techniques to qualify and discount a suspected breach or to verify and precisely scope a confirmed breach Helps identify your sensitive data, and the commonly overlooked data sets that, if stolen, can result in a material breach Defines breach response plan requirements and describes how to develop a

plan tailored for effectiveness within your organization Explains strategies for proactively self-detecting a breach and simplifying a response Covers critical first-responder steps and breach management practices, including containing a breach and getting the scope right, the first time Shows how to leverage threat intelligence to improve breach response and management effectiveness Offers guidance on how to manage internal and external breach communications, restore trust, and resume business operations after a breach, including the critical steps after the breach to reduce breach-related litigation and regulatory fines Illustrates how to define your cyber-defensible position to improve data protection and demonstrate proper due diligence practices

Cyber Risk & Security for SMEs - Practical Recommendations for the Digital Age Aug 24 2020 The purpose of the thesis is to determine the current level of awareness among SMEs and developing a list of cyber security essentials for SMEs in Switzerland in addition to the design a simplified cyber risk management process. The design will be based on a literature review regarding cyber risk, risk management, cyber security and in addition, on the results of the self-designed survey directed at Swiss SMEs. The research allows the following conclusion to be drawn: the majority of the SMEs underestimates their level of exposure and is not prepared for an incident and lacks the knowledge and the resources to respond appropriately. Currently, due to the rather slow development in the insurance market and thus, lack of transfer options, security investments and the implementation of risk management

measures is considered to be their first line of defence. The implementation of cyber security essentials is vital as approximately the effects of nearly 80% of all cyber attacks can be successfully avoided with basic technological security measures in place.

Data Breaches Sep 05 2021 Protect Your Organization Against Massive Data Breaches and Their Consequences Data breaches can be catastrophic, but they remain mysterious because victims don’t want to talk about them. In Data Breaches, world-renowned cybersecurity expert Sherri Davidoff shines a light on these events, offering practical guidance for reducing risk and mitigating consequences. Reflecting extensive personal experience and lessons from the world’s most damaging breaches, Davidoff identifies proven tactics for reducing damage caused by breaches and avoiding common mistakes that cause them to spiral out of control. You’ll learn how to manage data breaches as the true crises they are; minimize reputational damage and legal exposure; address unique challenges associated with health and payment card data; respond to hacktivism, ransomware, and cyber extortion; and prepare for the emerging battlefront of cloud-based breaches. Understand what you need to know about data breaches, the dark web, and markets for stolen data Limit damage by going beyond conventional incident response Navigate high-risk payment card breaches in the context of PCI DSS Assess and mitigate data breach risks associated with vendors and third-party suppliers Manage compliance requirements associated with healthcare and HIPAA Quickly respond to ransomware and data exposure cases Make better decisions about cyber

insurance and maximize the value of your policy Reduce cloud risks and properly prepare for cloud-based data breaches Data Breaches is indispensable for everyone involved in breach avoidance or response: executives, managers, IT staff, consultants, investigators, students, and more. Read it before a breach happens! Register your book for convenient access to downloads, updates, and/or corrections as they become available. See inside book for details.

The Cyber Risk Handbook Jul 15 2022 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.

Artificial Intelligence for Cyber Security: Methods, Issues and Possible Horizons or Opportunities Nov 26 2020 This book provides stepwise discussion, exhaustive literature review, detailed analysis and discussion, rigorous experimentation results (using several analytics tools), and an application-oriented approach that can be demonstrated with respect to data analytics using artificial intelligence to make systems stronger (i.e., impossible to breach). We can

see many serious cyber breaches on Government databases or public profiles at online social networking in the recent decade. Today artificial intelligence or machine learning is redefining every aspect of cyber security. From improving organizations' ability to anticipate and thwart breaches, protecting the proliferating number of threat surfaces with Zero Trust Security frameworks to making passwords obsolete, AI and machine learning are essential to securing the perimeters of any business. The book is useful for researchers, academics, industry players, data engineers, data scientists, governmental organizations, and non-governmental organizations.

Economics of Grids, Clouds, Systems, and Services Jun 21 2020 This book constitutes the refereed proceedings of the 18th International Conference on Economics of Grids, Clouds, Systems, and Services, GECON 2021, in September 2021. Due to COVID-19 pandemic the conference was held virtually hosted by the Libera Università Maria SS. Assunta (LUMSA), Rome, Italy. The 7 full papers and 2 short papers presented in this book were carefully reviewed and selected from 41 submissions. In addition, this book includes 8 work-in-progress papers and 2 extended abstracts. Chapters "AI Technologies and Motives for AI Adoption by Countries and Firms: A Systematic Literature Review"; "Knowledge Management Framework for Cloud Federation"; "Architecture for Orchestrating Containers in Cloud" and "Towards Software Compliance Specification and Enforcement using TOSCA" are available open access under a Creative Commons Attribution 4.0 International License via link.springer.com.

Proceedings of Fifth International Conference on Soft Computing for Problem Solving Apr 19 2020 The proceedings of SocProS 2015 will serve as an academic bonanza for scientists and researchers working in the field of Soft Computing. This book contains theoretical as well as practical aspects using fuzzy logic, neural networks, evolutionary algorithms, swarm intelligence algorithms, etc., with many applications under the umbrella of 'Soft Computing'. The book will be beneficial for young as well as experienced researchers dealing across complex and intricate real world problems for which finding a solution by traditional methods is a difficult task. The different application areas covered in the proceedings are: Image Processing, Cryptanalysis, Industrial Optimization, Supply Chain Management, Newly Proposed Nature Inspired Algorithms, Signal Processing, Problems related to Medical and Health Care, Networking Optimization Problems, etc.

Cyber Security Guideline Nov 14 2019 Cyber security is the application of technologies, processes and controls to protect systems, networks, programs, devices and data from cyber attacks. It aims to reduce the risk of cyber attacks and protect against the unauthorised exploitation of systems, networks and technologies.

The Manager's Guide to Terrorism, Risk, and Insurance Aug 04 2021 As a manager, you're aware of terrorist acts, are considering the risks, but sense that you need more background. How might terrorism occur? How is it part of risk and threat planning? What insurance strategies might protect your company from financial loss? In a few short chapters, The Manager's Guide to Terrorism, Risk, and

Insurance: Essentials for Today’s Business fills in the blanks for you. What does it take to weigh the likelihood of a terrorism exposure and protect all the assets of your company? The answer to this question involves understanding the nature of terrorists and their behavior, evaluating the risk of potential damage and business interruption, and exploring ways to use insurance – such as programs covered by the US Terrorism Risk Insurance Act – to protect against severe financial harm. Authors of this book, David J. Smith and Mark D. Silinsky, give you the benefit of their decades of professional experience in risk management, insurance, physical and cyber security, and anti-terrorism. Topics covered will help you to better understand: Characteristics that could make your company the target of terrorism. The most costly terrorist acts that have brought about fatalities and insured property loss. . How to anticipate the probability of maximum loss and foreseeable loss from terrorism. . The psychological picture of the typical terrorist – the warning signs and pre-attack indicators. . Tactics used by terrorists, such as bombings, assassination, and kidnapping. . Safety measures to be used by employees in the office and as they travel. . Practical steps for loss reduction from a variety of terrorist-related threats. . Insurance options to protect against financial loss from destructive terrorist acts, kidnap and ransom, and cyber attack and exposure. Case studies and discussion questions are provided to speed your understanding of the material. Importantly, since the book has been extensively researched, the authors provide a wealth of resources that you can consult as you dig deeper into this complex topic.

Cybersecurity Discussion Cases Feb 16 2020 Cybersecurity affects us all, every business, school, and citizen. This book, a collection of discussion case studies, presents in-depth examinations of eleven cybersecurity-related decisions facing managers and researchers. It is organized around the common cybersecurity framework: Identify, Protect, Detect, Respond, and Recover. It also includes two cases that specifically involve education. These cases place the reader in the position of the decision-maker featured in each case. None of them have a “right” answer. Instead, they are specifically designed to: 1. Serve as the basis of discussion, either in an formal educational context and as part of an industry training program 2. Help participants refine their judgment skills, allowing them to make better decisions when encountering similar contexts in their future career

Cyber Insurance Jan 09 2022 Malicious cyber activity poses significant risk to the federal government and the nation’s businesses and critical infrastructure, and it costs the U.S. billions of dollars each year. Threat actors are becoming increasingly capable of carrying out attacks, highlighting the need for a stable cyber insurance market. This report describes (1) key trends in the current market for cyber insurance, and (2) identified challenges faced by the cyber insurance market and options to address them.

Safety, Security and Privacy for Cyber-Physical Systems Jan 17 2020 This book presents an in-depth overview of recent work related to the safety, security, and privacy of cyber-physical systems (CPSs). It brings together contributions from leading researchers in networked control

systems and closely related fields to discuss overarching aspects of safety, security, and privacy; characterization of attacks; and solutions to detecting and mitigating such attacks. The book begins by providing an insightful taxonomy of problems, challenges and techniques related to safety, security, and privacy for CPSs. It then moves through a thorough discussion of various control-based solutions to these challenges, including cooperative fault-tolerant and resilient control and estimation, detection of attacks and security metrics, watermarking and encrypted control, privacy and a novel defense approach based on deception. The book concludes by discussing risk management and cyber-insurance challenges in CPSs, and by presenting the future outlook for this area of research as a whole. Its wide-ranging collection of varied works in the emerging fields of security and privacy in networked control systems makes this book a benefit to both academic researchers and advanced practitioners interested in implementing diverse applications in the fields of IoT, cooperative autonomous vehicles and the smart cities of the future.

Holistic Approach to Quantum Cryptography in Cyber Security Mar 19 2020 This new book discusses the concepts while also highlighting the challenges in the field of quantum cryptography and also covering cryptographic techniques and cyber security techniques, in a single volume. It comprehensively covers important topics in the field of quantum cryptography with applications, including quantum key distribution, position-based quantum cryptography, quantum teleportation, quantum e-commerce, quantum cloning, cyber security techniques' architectures

and design, cyber security techniques management, software-defined networks, and cyber security techniques for 5G communication. The text also discusses the security of practical quantum key distribution systems, applications and algorithms developed for quantum cryptography, as well as cyber security through quantum computing and quantum cryptography. The text will be beneficial for graduate students, academic researchers, and professionals working in the fields of electrical engineering, electronics and communications engineering, computer science, and information technology.

Security Risk Models for Cyber Insurance Jun 14 2022 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).

Cyber Risk, Market Failures, and Financial Stability

Sep 17 2022 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.

- Enhancing The Role Of Insurance In Cyber Risk Management
- Secure It Up
- Solving Cyber Risk
- How Has Ransomware Changed Cyber Insurance
- Digital Asset Valuation And Cyber Risk Measurement
- Cyber Risk Market Failures And Financial Stability
- Cyber Insurance Roundtable Readout Report
- The Cyber Risk Handbook
- Security Risk Models For Cyber Insurance
- Assessing And Insuring Cybersecurity Risk

- Cyber Risks Social Media And Insurance A Guide To Risk Assessment And Management 8 2022 8 2023 Edition
- Pricing Cyber Security Insurance
- Cyber Risk For The Financial Sector A Framework For Quantitative Assessment
- Cyber Insurance
- Guide To Cybersecurity Due Diligence In MA Transactions
- Cyberinsurance Policy
- Managing Cyber Risk
- Data Breaches
- The Managers Guide To Terrorism Risk And Insurance
- Manager Cyber Security Critical Questions Skills Assessment
- Machine Learning For Computer And Cyber Security
- EIOPA Strategy On Cyber Underwriting
- 7 Rules To Become Exceptional At Cyber Security
- Cyber Strategy
- At The Nexus Of Cybersecurity And Public Policy
- Building A Cyber Resilient Business
- Artificial Intelligence For Cyber Security Methods Issues And Possible Horizons Or Opportunities
- Readings Cases In Information Security Law Ethics
- Decision And Game Theory For Security
- Cyber Risk Security For SMEs Practical Recommendations For The Digital Age
- Cyber Security In Critical Infrastructures
- Economics Of Grids Clouds Systems And Services

- Data Breach Preparation And Response
- Proceedings Of Fifth International Conference On Soft Computing For Problem Solving
- Holistic Approach To Quantum Cryptography In Cyber Security
- Cybersecurity Discussion Cases
- Safety Security And Privacy For Cyber Physical Systems
- Global Cyber Security Labor Shortage And International Business Risk
- Cyber Security Guideline
- Trust Privacy And Security In Digital Business