Cyber Risks In Consumer Business Be Secure Vigilant And

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. TiersProfilesFunctionsInformative References

"This research book is a repository for academicians, researchers, and industry practitioners to share and exchange their research ideas, theories, and practical experiences, discuss challenges and opportunities, and present tools and techniques in all aspects of e-business

development and management in the digital economy"--Provided by publisher.

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.

The asymmetry of responsibilities between management and

corporate governance both for day-to-day operations and the board's monthly or quarterly review and evaluation remains an unresolved challenge. Expertise in the area of risk management is a fundamental requirement for effective corporate governance, if not by all, certainly by some board members. This means that along with board committees such as "compensation", "audit", "strategy" and several others, "risk management" committees must be established to monitor the likelihood of certain events that may cause the collapse of the firm. Risk Management and Corporate Governance allows academics and practitioners to assess the state of international research in risk management and corporate governance. The chapters overlay the areas of risk management and corporate governance on both financial and operating decisions of a firm while treating legal and political environments as externalities to decisions undertaken.

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.

Today's financial sector faces multiple challenges stemming from ecological, societal, and technological risks such as climate change, political extremism, and cyber-attacks. However, these non-traditional risks are yet to be fully identified and measured, in order to ensure their successful management. This edited collection sheds light on the topic by examining the unique measurement and modelling challenges associated with each of these risks, and their interaction with finance. Offering a comprehensive analysis of non-traditional finance risks, the authors provide the basis for developing appropriate risk management techniques. With new approaches to protect against emerging threats to the financial sector, this edited collection will appeal to academics researching sustainability, development finance, and risk

management, as well as policy-makers and practitioners within the banking sector.

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.

For anyone thinking about starting an online business, this resource provides all the steps needed to take an idea and turn it into reality. Wiley Pathways E-Business begins by discussing the legal considerations involved in launching the business as well as tips for acquiring the necessary financing. It also delves into the techniques to follow for operating the e-business, including selecting the right products, managing inventory, creating a marketing plan, and more. The book then covers how to create a secure Web site that can track customer data.

This book has a two-fold mission: to explain and facilitate digital transition in business organizations using information and communications technology and to address the associated growing threat of cyber crime and the challenge of creating and maintaining effective cyber protection. The book begins with a section on Digital Business Transformation, which includes chapters on tools for

integrated marketing communications, human resource workplace digitalization, the integration of the Internet of Things in the workplace, Big Data, and more. The technologies discussed aim to help businesses and entrepreneurs transform themselves to align with today's modern digital climate. The Evolution of Business in the Cyber Age: Digital Transformation, Threats, and Security provides a wealth of information for those involved in the development and management of conducting business online as well as for those responsible for cyber protection and security. Faculty and students, researchers, and industry professionals will find much of value in this volume.

Cybersecurity threats are on the rise. As a leader, you need to be prepared to keep your organization safe. Companies are investing an unprecedented amount of money to keep their data and assets safe, yet cyberattacks are on the rise--and the problem is worsening. No amount of technology, resources, or policies will reverse this trend. Only sound governance, originating with the board, can turn the tide. Protection against cyberattacks can't be treated as a problem solely belonging to an IT or cybersecurity department. It needs to cast a wide and impenetrable net that covers everything an organization does--from its business operations, models, and strategies to its products and intellectual property. And boards are in the best

position to oversee the needed changes to strategy and hold their companies accountable. Not surprisingly, many boards aren't prepared to assume this responsibility. In A Leader's Guide to Cybersecurity, Thomas Parenty and Jack Domet, who have spent over three decades in the field, present a timely, clear-eyed, and actionable framework that will empower senior executives and board members to become stewards of their companies' cybersecurity activities. This includes: Understanding cyber risks and how best to control them Planning and preparing for a crisis--and leading in its aftermath Making cybersecurity a companywide initiative and responsibility Drawing attention to the nontechnical dynamics that influence the effectiveness of cybersecurity measures Aligning the board, executive leadership, and cybersecurity teams on priorities Filled with tools, best practices, and strategies, A Leader's Guide to Cybersecurity will help boards navigate this seemingly daunting but extremely necessary transition.

The historic European Union Directive on Data Protection will take effect in October 1998. A key provision will prohibit transfer of personal information from Europe to other countries if they lack “adequate” protection of privacy. If enforced as written, the Directive could create enormous obstacles to commerce between Europe and other countries, such as the United States, that do not

have comprehensive privacy statutes. In this book, Peter Swire and Robert Litan provide the first detailed analysis of the sector-by-sector effects of the Directive. They examine such topics as the text of the Directive, the tension between privacy laws and modern information technologies, issues affecting a wide range of businesses and other organizations, effects on the financial services sector, and effects on other prominent sectors with large transborder data flows. In light of the many and significant effects of the Directive as written, the book concludes with detailed policy recommendations on how to avoid a coming trade war with Europe. The book will be of interest to the wide range of individuals and organizations affected by the important new European privacy laws. More generally, the privacy clash discussed in the book will prove a major precedent for how electronic commerce and world data flows will be governed in the Internet Age.

BUSINESS FINANCE presents finance from a business point of view. This text, written specifically for high school students, covers finance fundamentals, long-term and short-term funding sources, business risk management, use of technology, and international finance. Business Finance combines fundamental concepts with a strong lesson-based instructional design, weaving in interesting real-world features, creative methods of

assessment, research opportunities, financial calculations, case studies, and academic connections. Whether your course is offered at an Academy of Finance, within a Finance Career Cluster Concentration, or as part of a business curriculum, Business Finance provides you with complete coverage. The comprehensive package of print and technology resources reaches students with a variety of learning styles, skills, and educational backgrounds. Students examine the financial side of running a business, keeping records, protecting against loss, offering credit, and making strategic decisions. Important Notice: Media content referenced within the product description or the product text may not be available in the ebook version.

Digital transformation and cyber insecurity are two global trends that converged in 2020. The COVID-19 pandemic has accelerated these global challenges into paradigm-changing realities that threaten to destroy every company, government, network, and individual. But what can be done to embrace the accelerating digital disruption and at the same time manage the explosion of vulnerabilities, cyber threats, and business risks? What strategies are enabling technology leaders to thrive in this fast-changing landscape and stay calm in the midst of a world filled with ransomware, online deception, and nation-state hackers? Cyber Mayday and the Day

After is a business book, a communication toolkit offering stories, strategies, tactics, and outlook with key extracts and lessons learned from top C-executive leaders around the world. Some of these insights come from former FBIs, NASA agents, government CISOs, and high profile CxOs, offering practical examples and workable solutions for leaders to succeed in the 21st century. This book unpacks key learnings on leadership and nfluence. It equips readers with the mastery of th r stakeholders and explores how to effect a cultural change within organizations.

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

A ground shaking exposé on the failure of popular

cyber risk management methods How to Measure Anything in Cybersecurity Risk exposes the shortcomings of current "risk management" practices, and offers a series of improvement techniques that help you fill the holes and ramp up security. In his bestselling book How to Measure Anything, author Douglas W. Hubbard opened the business world's eyes to the critical need for better measurement. This book expands upon that premise and draws from The Failure of Risk Management to sound the alarm in the cybersecurity realm. Some of the field's premier risk management approaches actually create more risk than they mitigate, and questionable methods have been duplicated across industries and embedded in the products accepted as gospel. This book sheds light on these blatant risks, and provides alternate techniques that can help improve your current situation. You'll also learn which approaches are too risky to save, and are actually more damaging than a total lack of any security. Dangerous risk management methods abound; there is no industry more critically in need of solutions than cybersecurity. This book provides solutions where they exist, and advises when to change tracks entirely. Discover the shortcomings of cybersecurity's "best practices" Learn which risk management approaches actually create risk Improve your current practices with practical alterations Learn which methods are beyond saving,

and worse than doing nothing Insightful and enlightening, this book will inspire a closer examination of your company's own risk management practices in the context of cybersecurity. The end goal is airtight data protection, so finding cracks in the vault is a positive thing—as long as you get there before the bad guys do. How to Measure Anything in Cybersecurity Risk is your guide to more robust protection through better quantitative processes, approaches, and techniques.

A large part of academic literature, business literature as well as practices in real life are resting on the assumption that uncertainty and risk does not exist. We all know that this is not true, yet, a whole variety of methods, tools and practices are not attuned to the fact that the future is uncertain and that risks are all around us. However, despite risk management entering the agenda some decades ago, it has introduced risks on its own as illustrated by the financial crisis. Here is a book that goes beyond risk management as it is today and tries to discuss what needs to be improved further. The book also offers some cases.

Welcome to the all-new second edition of Navigating the Digital Age. This edition brings together more than 50 leaders and visionaries from business, science, technology, government, aca¬demia, cybersecurity, and law enforce¬ment. Each has

contributed an exclusive chapter designed to make us think in depth about the ramifications of this digital world we are creating. Our purpose is to shed light on the vast possibilities that digital technologies present for us, with an emphasis on solving the existential challenge of cybersecurity. An important focus of the book is centered on doing business in the Digital Age-par¬ticularly around the need to foster a mu¬tual understanding between technical and non-technical executives when it comes to the existential issues surrounding cybersecurity. This book has come together in three parts. In Part 1, we focus on the future of threat and risks. Part 2 emphasizes lessons from today's world, and Part 3 is designed to help you ensure you are covered today. Each part has its own flavor and personal¬ity, reflective of its goals and purpose. Part 1 is a bit more futuristic, Part 2 a bit more experiential, and Part 3 a bit more practical. How we work together, learn from our mistakes, deliver a secure and safe digital future-those are the elements that make up the core thinking behind this book. We cannot afford to be complacent. Whether you are a leader in business, government, or education, you should be knowledgeable, diligent, and action-oriented. It is our sincerest hope that this book provides answers, ideas, and inspiration.If we fail on the cybersecurity front, we put all of our hopes and aspirations at risk. So we start this book with a simple proposition:

When it comes to cybersecurity, we must succeed. The convenience of online shopping has driven consumers to turn to the internet to purchase everything from clothing to housewares and even groceries. The ubiquity of online retail stores and availability of hard-to-find products in the digital marketplace has been a catalyst for a heighted interest in research on the best methods, techniques, and strategies for remaining competitive in the era of e-commerce. The Encyclopedia of E-Commerce Development, Implementation, and Management is an authoritative reference source highlighting crucial topics relating to effective business models, managerial strategies, promotional initiatives, development methodologies, and end-user considerations in the online commerce sphere. Emphasizing emerging research on up-and-coming topics such as social commerce, the Internet of Things, online gaming, digital products, and mobile services, this multi-volume encyclopedia is an essential addition to the reference collection of both academic and corporate libraries and caters to the research needs of graduate-level students, researchers, IT developers, and business professionals. .

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).

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.

Financial technology (fintech) is emerging as an innovative way to achieve financial inclusion and the broader objective of inclusive growth. Thus far, fintech in the MENAP and CCA remains below potential with limited impact on financial inclusion. This paper reviews the fintech landscape in the MENAP and CCA regions, identifies the constraints to the growth of fintech and its contribution to inclusive growth and considers policy options to unlock the potential.

The cost and frequency of cybersecurity incidents are on the rise, is your enterprise keeping pace? The numbers of threats, risk scenarios and vulnerabilities have grown exponentially. Cybersecurity has evolved as a new field of interest, gaining political and societal attention. Given this magnitude, the future tasks and responsibilities associated with

cybersecurity will be essential to organizational survival and profitability. This publication applies the COBIT 5 framework and its component publications to transforming cybersecurity in a systemic way. First, the impacts of cybercrime and cyberwarfare on business and society are illustrated and put in context. This section shows the rise in cost and frequency of security incidents, including APT attacks and other threats with a critical impact and high intensity. Second, the transformation addresses security governance, security management and security assurance. In accordance with the lens concept within COBIT 5, these sections cover all elements of the systemic transformation and cybersecurity improvements.

Most organizations are undergoing a digital transformation of some sort and are looking to embrace innovative technology, but new ways of doing business inevitably lead to new threats which can cause irreparable financial, operational and reputational damage. In an increasingly punitive regulatory climate, organizations are also under pressure to be more accountable and compliant. Cyber Risk Management clearly explains the importance of implementing a cyber security strategy and provides practical guidance for those responsible for managing threat events, vulnerabilities and controls, including malware, data leakage, insider threat and Denial-of-Service.

Examples and use cases including Yahoo, Facebook and TalkTalk, add context throughout and emphasize the importance of communicating security and risk effectively, while implementation review checklists bring together key points at the end of each chapter. Cyber Risk Management analyzes the innate human factors around risk and how they affect cyber awareness and employee training, along with the need to assess the risks posed by third parties. Including an introduction to threat modelling, this book presents a data-centric approach to cyber risk management based on business impact assessments, data classification, data flow modelling and assessing return on investment. It covers pressing developments in artificial intelligence, machine learning, big data and cloud mobility, and includes advice on responding to risks which are applicable for the environment and not just based on media sensationalism.

Traditional marketing techniques have become outdated by the emergence of the internet, and for companies to survive in the new technological marketplace, they must adopt digital marketing and business analytics practices. Unfortunately, with the benefits of improved storage and flow of information comes the risk of cyber-attack. Business Analytics and Cyber Security Management in Organizations compiles innovative research from international professionals discussing the opportunities and

challenges of the new era of online business. Outlining updated discourse for business analytics techniques, strategies for data storage, and encryption in emerging markets, this book is ideal for business professionals, practicing managers, and students of business.

No data is completely safe. Cyberattacks on companies and individuals are on the rise and growing not only in number but also in ferocity. And while you may think your company has taken all the precautionary steps to prevent an attack, no individual, company, or country is safe. Cybersecurity can no longer be left exclusively to IT specialists. Improving and increasing data security practices and identifying suspicious activity is everyone's responsibility, from the boardroom to the break room. Cybersecurity: The Insights You Need from Harvard Business Review brings you today's most essential thinking on cybersecurity, from outlining the challenges to exploring the solutions, and provides you with the critical information you need to prepare your company for the inevitable hack. The lessons in this book will help you get everyone in your organization on the same page when it comes to protecting your most valuable assets. Business is changing. Will you adapt or be left behind? Get up to speed and deepen your understanding of the topics that are shaping your company's future with the Insights You Need from

Harvard Business Review series. Featuring HBR's smartest thinking on fast-moving issues--blockchain, cybersecurity, AI, and more--each book provides the foundational introduction and practical case studies your organization needs to compete today and collects the best research, interviews, and analysis to get it ready for tomorrow. You can't afford to ignore how these issues will transform the landscape of business and society. The Insights You Need series will help you grasp these critical ideas--and prepare you and your company for the future.

A definitive guide to cybersecurity law Expanding on the author's experience as a cybersecurity lawyer and law professor, Cybersecurity Law is the definitive guide to cybersecurity law, with an in-depth analysis of U.S. and international laws that apply to data security, data breaches, sensitive information safeguarding, law enforcement surveillance, cybercriminal combat, privacy, and many other cybersecurity issues. Written in an accessible manner, the book provides real-world examples and case studies to help readers understand the practical applications of the presented material. The book begins by outlining the legal requirements for data security, which synthesizes the Federal Trade Commission's cybersecurity cases in order to provide the background of the FTC's views on data security. The book also examines data security requirements imposed by a growing number of state

legislatures and private litigation arising from data breaches. Anti-hacking laws, such as the federal Computer Fraud and Abuse Act, Economic Espionage Act, and the Digital Millennium Copyright Act, and how companies are able to fight cybercriminals while ensuring compliance with the U.S. Constitution and statutes are discussed thoroughly. Featuring an overview of the laws that allow coordination between the public and private sectors as well as the tools that regulators have developed to allow a limited amount of collaboration, this book also: • Addresses current U.S. and international laws, regulations, and court opinions that define the field of cybersecurity including the security of sensitive information, such as financial data and health information • Discusses the cybersecurity requirements of the largest U.S. trading partners in Europe, Asia, and Latin America, and specifically addresses how these requirements are similar to (and differ from) those in the U.S. • Provides a compilation of many of the most important cybersecurity statutes and regulations • Emphasizes the compliance obligations of companies with in-depth analysis of crucial U.S. and international laws that apply to cybersecurity issues • Examines government surveillance laws and privacy laws that affect cybersecurity as well as each of the data breach notification laws in 47 states and the District of Columbia • Includes numerous case

studies and examples throughout to aid in classroom use and to help readers better understand the presented material • Supplemented with a companion website that features in-class discussion questions and timely and recent updates on recent legislative developments as well as information on interesting cases on relevant and significant topics Cybersecurity Law is appropriate as a textbook for undergraduate and graduate-level courses in cybersecurity, cybersecurity law, cyber operations, management-oriented information technology (IT), and computer science. This book is also an ideal reference for lawyers, IT professionals, government personnel, business managers, IT management personnel, auditors, and cybersecurity insurance providers. JEFF KOSSEFF is Assistant Professor of Cybersecurity Law at the United States Naval Academy in Annapolis, Maryland. He frequently speaks and writes about cybersecurity and was a journalist covering technology and politics at The Oregonian, a finalist for the Pulitzer Prize, and a recipient of the George Polk Award for national reporting.

This book adopts an international perspective to examine how the online sale of insurance challenges the insurance regulation and the insurance contract, with a focus on insurance sales, consumer protection, cyber risks and privacy, as well as dispute resolution. Today insurers, policyholders,

intermediaries and regulators interact in an increasingly online world with profound implications for what has up to now been a traditionally operating industry. While the growing threats to consumer and business data from cyber attacks constitute major sources of risk for insurers, at the same time cyber insurance has become the fastest growing commercial insurance product in many jurisdictions. Scholars and practitioners from Europe, the United States and Asia review these topics from the viewpoints of insurers, policyholders and insurance intermediaries. In some cases, existing insurance regulations appear readily adaptable to the online world, such as prohibitions on deceptive marketing of insurance products and unfair commercial practices, which can be applied to advertising through social media, such as Facebook and Twitter, as well as to traditional written material. In other areas, current regulatory and business practices are proving to be inadequate to the task and new ones are emerging. For example, the insurance industry and insurance supervisors are exploring how to review, utilize, profit from and regulate the explosive growth of data mining and predictive analytics (“big data”), which threaten long-standing privacy protection and insurance risk classification laws. This book’s ambitious international scope matches its topics. The online insurance market is cross-territorial and cross-jurisdictional with insurers often

operating internationally and as part of larger financial-services holding companies. The authors' exploration of these issues from the vantage points of some of the world's largest insurance markets – the U.S., Europe and Japan – provides a comparative framework, which is necessary for the understanding of online insurance.

Over the last decade, electronically stored data has become both an indispensable asset and emergent liability for companies that transact business online. Almost weekly, data breaches and computer crimes make national headlines, compounding the public's demand for adequate protection of sensitive consumer information. Increasingly, entities doing business in the information age find that traditional commercial general liability insurance policies do not cover the loss or theft of electronic data, leaving those entities with a sizable gap in insurance coverage in the event of a data breach. In response to this coverage gap, insurers have begun underwriting cyber-risk insurance policies to specifically address the perils of e-commerce. These policies range from coverage for losses and fines associated with data breach notification statutes, to comprehensive indemnity from consumer class action suits, infrastructure remediation costs and credit monitoring for affected individuals. Similar to more established types of insurance, however, cyber-risk coverage is not immune from the traditional

vulnerabilities of the insurance marketplace, including moral hazard and adverse selection. This Article seeks to provide insurers and policymakers with a suggestion for mitigating moral hazard in the cyber-risk insurance market. Through an analysis of information security regulation and public policy considerations, this Article proposes an information exchange that insurers and regulators may use to share loss data, claim costs, and compliance audits of insureds, in an effort to more effectively price cyber-risk coverage and thereby reduce the moral hazard presented by insureds that possess insufficient information security infrastructure. Admission to this information exchange is predicated on two conditions: First, an insurer must pledge to discount premiums for entities that employ information security infrastructure that sufficiently protects consumer custodial data as matter of public policy; and second, insurers writing cyber-risk coverage must contribute their own loss data to this information exchange. The result of this proposal is a recommendation for an information-sharing platform, which encourages insurers to pool loss data and differentiate premiums for preferred risks. Because cyber-risk insurance is neither a market-driven private enterprise engaged in the unrestrained pursuit of profit, nor a tightly regulated, monopolistic public utility, this Article seeks to balance the autonomy of insurers with the public's need for

adequately secured personal information to create a system that simultaneously mitigates moral hazard for insurers while encouraging the adequate protection of consumer data.

This dissertation research studied how different degrees of knowledge of online security risks affect B2C (business-to-consumer) e-commerce consumer decision making. Online information security risks, such as identity theft, have increasingly become a major factor inhibiting the potential growth of e-commerce. On the other hand, e-commerce consumers lack knowledge and awareness of security risks in the online shopping environment and make decisions under conditions where precise probabilities of risks are not available. Based on research in the decision theory field, a person's knowledge of a risk is assumed to fall under one of four states: known certainty, known uncertainty, unknown uncertainty, and unknowable uncertainty. A theoretical model was developed in this study, and based on the model explicit hypotheses were stated which relate a consumer's degree of risk knowledge and the consumer's online security risk evaluation and purchase decision making. This research used an experimental approach to study the effect of different levels of consumers' knowledge of a typical online security risk on their purchase behavior. Following a pilot experiment to test and refine the experimental design, a between-subjects experiment was conducted with the four knowledge states as treatments among 160 subjects. Results indicated that the consumers' willingness to pay to avoid risks and their intention to purchase online vary

systematically under different knowledge conditions. Results suggested that people can distinguish between risk and uncertainty and will pay a premium to avoid uncertainty. This research used an experimental approach to study the effect of different levels of consumers' knowledge of a typical online security risk on their purchase behavior. Following a pilot experiment to test and refine the experimental design, a between-subjects experiment was conducted with the four knowledge states as treatments among 160 subjects. Results indicated that the consumers' willingness to pay to avoid risks and their intention to purchase online vary systematically under different knowledge conditions. Results suggested that people can distinguish between risk and uncertainty and will pay a premium to avoid uncertainty.

The latest edition features a new chapter on implementation and operation of an integrated smart grid with updates to multiple chapters throughout the text. New sections on Internet of things, and how they relate to smart grids and smart cities, have also been added to the book. It describes the impetus for change in the electric utility industry and discusses the business drivers, benefits, and market outlook of the smart grid initiative. The book identifies the technical framework of enabling technologies and smart solutions and describes the role of technology developments and coordinated standards in smart grid, including various initiatives and organizations helping to drive the smart grid effort. With chapters written by leading experts in the field, the text explains how to plan, integrate, implement, and operate

a smart grid.

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.

This is a general guide to the origins of cyber risks and to developing suitable strategies for their management. It provides a breakdown of the main risks involved and shows you how to manage them. Covering the relevant legislation on information security and data protection, the author combines his legal expertise with a solid, practical grasp of the latest developments in IT to offer a comprehensive overview of a highly complex subject.

"This book offers comprehensive explanations of topics in computer system security in order to combat the growing risk associated with technology"--Provided by publisher.