Marriott Data Breach Case Study

Cybersecurity
FinTech
Trafficking Data
Data Ethics and Challenges
Management Information Systems
EBK: Services Marketing: Integrating Customer Service Across the Firm 4e
What is Online Research?
Cyber Litigation: The Legal Principles
Database Administration
Corporate Frauds
Why Don't We Defend Better?
Health Providers in India
Cybersecurity Law Fundamentals
Crimes Committed by Terrorist Groups
Big Data for Better Tourism Policy, Management, and Sustainable Recovery from COVID-19
How to Measure Anything in Cybersecurity Risk
Survivability
China Internet Development Report 2017
Internal Communication and Employee Engagement
Privacy Concerns Surrounding Personal Information Sharing on Health and Fitness Mobile Apps
Security Policies and Implementation Issues
Strategic Management in Sport
Music, Business and Peacebuilding
ECCWS 2017 16th European Conference on Cyber Warfare and Security
Cybersecurity and Third-Party Risk
The Cambridge Handbook of Compliance
Breach (2005-2006) #9
Plunder of the Commons
Surveillance State
Information Technology for Management
Strategic Management for Hospitality and Tourism
Strategy, Leadership, and AI in the Cyber Ecosystem
Digital Transformation in Aviation, Tourism and Hospitality in Southeast Asia
Handbook of Research on Theory and Practice of Financial Crimes
Big Breaches
Converge
Security and Risk Assessment for Facility and Event Managers
Cloud Computing Solutions
Information is Beautiful

HICKS ROBINSON

Cybersecurity Addison-Wesley
Black money and financial crime are emerging global phenomena. During the last few decades, corrupt financial practices were increasingly being monitored in many countries around the globe. Among a large number of problems is a lack of general awareness about all these issues among various stakeholders including researchers and practitioners. The Handbook of Research on Theory and Practice of Financial Crimes is a critical scholarly research publication that provides comprehensive research on all aspects of black money and financial crime in individual, organizational, and societal experiences. The book further examines the implications of white-collar crime and practices to enhance forensic audits on financial fraud and the effects on tax enforcement. Featuring a wide range of topics such as ethical leadership, cybercrime, and blockchain, this book is ideal for policymakers, academicians, business professionals, managers, IT specialists, researchers, and students.
FinTech Edward Elgar Publishing
"Trafficking Data argues that the movement of human data across borders for political and financial gain is disenfranchising consumers, eroding national autonomy, and destabilizing sovereignty. Focusing on the United States and China, it traces how US government leadership failures, Silicon Valley's disruption fetish, and Wall Street's addiction to growth have yielded an unprecedented opportunity for Chinese firms to gather data in the United States and quietly send it back to China, and by extension, the Chinese government. Such "data trafficking," as the book names this insidious phenomenon, is enabled by the competing governance models of the world's two largest economies: mass government data aggregation in China and impenetrable corporate data management policies in the United States. China is stepping up its data trafficking efforts through national regulations, soft power persuasion, and tech investment, extending the scope of state control over domestic and international data and tech infrastructure, and thereby expanding its global influence. The United States, by contrast, is retreating from participation in foreign alliances, international organizations, and the systemic regulation of the tech industry-practices with the potential to counter data trafficking. Confronting data trafficking as the defining international competition of the twenty-first century, this book ultimately advocates for an alternative future of data stabilization. To stem data trafficking and stabilize data flows, it shows, policymakers can synthesize tools from across the private sector, public sector, multi-national organizations, and consumers to protect users, secure national sovereignty, and establish valuable international standards"--
Trafficking Data Springer Nature
This volume has articles contributed by health researchers, practitioners, policy advocates, programme managers and a journalist, and poems by renowned poet–physician Gieve Patel. Each presents a distinctive view of a particular group of frontline health providers, based on field research or on the authors' respective experiences of working with or as providers. The health providers addressed in this volume include doctors (working in the public and private sectors), nurses, public health workers, counsellors, traditional practitioners and homecare providers. Different groups of health providers face struggles at diverse frontiers — social, professional and systemic. In the context of reforming health systems, government health workers must constantly negotiate the vagaries of changing working environments and policy vacillations. For traditional and homecare providers, formal health systems and structures often only reject and exclude their contributions. Medical doctors, conversely, face difficult challenges of introspection, as they tread the line between personal gain and public service. The ideas and themes that emerge in this collection not only contribute to the understanding of providers' roles as actors in the health systems and societies of contemporary India, but re-examines preconceptions about this critical occupational group. This volume advances the case for a deeper appreciation of India's complex landscape of healthcare provision, and of the potential roles of frontline health providers as central figures in development.
Data Ethics and Challenges Routledge
Compliance has become key to our contemporary markets, societies, and modes of governance across a variety of public and private domains. While this has stimulated a rich body of empirical and practical expertise on compliance, thus far, there has been no comprehensive understanding of what compliance is or how it influences various fields and sectors. The academic knowledge of compliance has remained siloed along different disciplinary domains, regulatory and legal spheres, and mechanisms and interventions. This handbook bridges these divides to provide the first one-stop overview of what compliance is, how we can best study it, and the core mechanisms that shape it. Written by leading experts, chapters offer perspectives from across law, regulatory studies, management science, criminology, economics, sociology, and psychology. This volume is the definitive and comprehensive account of compliance.
Management Information Systems DIANE Publishing
Move beyond the checklist and fully protect yourself from third-party cybersecurity risk Over the last decade, there have been hundreds of big-name organizations in every sector that have experienced a public breach due to a vendor. While the media tends to focus on high-profile breaches like those that hit Target in 2013 and Equifax in 2017, 2020 has ushered in a huge wave of cybersecurity attacks, a near 800% increase in cyberattack activity as millions of workers shifted to working remotely in the wake of a global pandemic. The 2020 SolarWinds supply-chain attack illustrates that lasting impact of this dramatic increase in cyberattacks. Using a technique known as Advanced Persistent Threat (APT), a sophisticated hacker leveraged APT to steal information from multiple organizations from Microsoft to the Department of Homeland Security not by attacking targets directly, but by attacking a trusted partner or vendor. In addition to exposing third-party risk vulnerabilities for other hackers to exploit, the damage from this one attack alone will continue for years, and there are no signs that cyber breaches are slowing. Cybersecurity and Third-Party Risk delivers proven, active, and predictive risk reduction strategies and tactics designed to keep you and your organization safe. Cybersecurity and IT expert and author Gregory Rasner shows you how to transform third-party risk from an exercise in checklist completion to a proactive and effective process of risk mitigation. Understand the basics of third-party risk management Conduct due diligence on third parties connected to your network Keep your data and sensitive information current and reliable Incorporate third-party data requirements for offshoring, fourth-party hosting, and data security arrangements into your vendor contracts Learn valuable lessons from devasting breaches suffered by other companies like Home Depot, GM, and Equifax The time to talk cybersecurity with your data partners is now. Cybersecurity and Third-Party Risk is a must-read resource for business leaders and security professionals looking for a practical roadmap to avoiding the massive reputational and financial losses that come with third-party security breaches.
EBK: Services Marketing: Integrating Customer Service Across the Firm 4e St. Martin's Press
The wave of data breaches raises two pressing questions: Why don't we defend our networks better? And, what practical incentives can we create to improve our defenses? Why Don't We Defend Better?: Data Breaches, Risk Management, and Public Policy answers those questions. It distinguishes three technical sources of data breaches corresponding to three types of vulnerabilities: software, human, and network. It discusses two risk management goals: business and consumer. The authors propose mandatory anonymous reporting of information as an essential step toward better defense, as well as a general reporting requirement. They also provide a systematic overview of data breach defense, combining technological and public policy considerations. Features Explains why data breach defense is currently often ineffective Shows how to respond to the increasing frequency of data breaches Combines the issues of technology, business and risk management, and legal liability Discusses the

different issues faced by large versus small and medium-sized businesses (SMBs) Provides a practical framework in which public policy issues about data breaches can be effectively addressed
What is Online Research? John Wiley & Sons
Business schools are placing more emphasis on the role of business in society. Top business school accreditors are shifting to mandating that schools teach their students about the social impact of business, including AACSB standards to require the incorporation of business impact on society into all elements of accredited institutions. Researchers are also increasingly focused on issues related to sustainability, but in particular to business and peace as a field. A strong strain of scholarship argues that ethics is nurtured by emotions and through aesthetic quests for moral excellence. The arts (and music as shown specifically in this book) can be a resource to nudge positive emotions in the direction toward ethical behavior and, logically, then toward peace. Business provides a model for positive interactions that not only foster long-term successful business but also incrementally influences society. This book provides an opportunity for integration and recognition of how music (and other art forms) can further encourage business toward the direction of peace while business provides a platform for the dissemination and modeling of the positive capabilities of music toward the aims of peace in the world today. The primary market for this book is the academic audience. Unlike many other academic books, however, the interdisciplinary nature of the book allows for multiple academic audiences. Thus, this book reaches into schools of music, business, political science, film studies, sports and society studies, the humanities, ethics and, of course, peace studies.
Cyber Litigation: The Legal Principles Taylor & Francis
Technological advances and the drive to digitalize business processes in aviation, tourism, and hospitality have forced the industries to go along with the digital movement. The results are often mixed. This book brings together contributions from leading scholars in the field and explores the digital transformation in these industries in Southeast Asia. The book looks at the impact of digital transformation on the region and the issues and challenges brought about by this transformation. It also addresses trends in the industries from blockchain technology, AI, biometric and mobile technology applications to in-flight catering. It examines the impact of COVID-19 on the industries and how the pandemic has led to businesses adopting new business models. Through the case studies of digital adoptions in the region, readers will gain insights on how the countries have leveraged new technologies and the implementation processes to drive digital transformation. The book aims to help scholars and policy makers understand the digital advances in the industries to better formulate responses in research and policy making and deliver effective digital transformation.
Database Administration CRC Press
Security and Risk Assessment for Facility and Event Managers introduces a risk assessment framework that helps readers identify and plan for potential security threats, develop countermeasures and emergency response strategies, and implement training programs to prepare staff.
Corporate Frauds Routledge
CLOUD COMPUTING SOLUTIONS The main purpose of this book is to include all the cloud-related technologies in a single platform, so that researchers, academicians, postgraduate students, and those in the industry can easily understand the cloud-based ecosystems. This book discusses the evolution of cloud computing through grid computing and cluster computing. It will help researchers and practitioners to understand grid and distributed computing cloud infrastructure, virtual machines, virtualization, live migration, scheduling techniques, auditing concept, security and privacy, business models, and case studies through the state-of-the-art cloud computing countermeasures. This book covers the spectrum of cloud computing-related technologies and the wide-ranging contents will differentiate this book from others. The topics treated in the book include: The evolution of cloud computing from grid computing, cluster computing, and distributed systems; Covers cloud computing and virtualization environments; Discusses live migration, database, auditing, and applications as part of the materials related to cloud computing; Provides concepts of cloud storage, cloud strategy planning, and management, cloud security, and privacy issues; Explains complex concepts clearly and covers information for advanced users and beginners. Audience The primary audience for the book includes IT, computer science specialists, researchers, graduate students, designers, experts, and engineers who are occupied with research.
Why Don't We Defend Better? Jones & Bartlett Learning
'One of the most important books I've read in years' Brian Eno We are losing the commons. Austerity and neoliberal policies have depleted our shared wealth; our national utilities have been sold off to foreign conglomerates, social housing is almost non-existent, our parks are cordoned off for private events and our national art galleries are sponsored by banks and oil companies. This plunder deprives us all of our common rights, recognized as far back as the Magna Carta and the Charter of the Forest of 1217, to share fairly and equitably in our public wealth. Guy Standing leads us through a new appraisal of the commons, stemming from the medieval concept of common land reserved in ancient law from marauding barons, to his modern reappraisal of the resources we all hold in common - a brilliant new synthesis that crystallises quite how much public wealth has been redirected to the 1% in recent decades through the state-approved exploitation of everything from our land to our state housing, health and benefit systems, to our justice system, schools, newspapers and even the air we breathe. Plunder of the Commons proposes a charter for a new form of commoning, of remembering, guarding and sharing that which belongs to us all, to slash inequality and soothe our current political instability.
Health Providers in India Springer
What is Online Research? is a straightforward, accessible introduction to social research online. The book covers the key issues and concerns, with sections on design,ethics and good practice.It will be key reading for social scientists of all levels.
Cybersecurity Law Fundamentals Academic Press
Big data is already being used to measure, monitor, and manage tourism development, but its potential remains to be fully exploited. This report discusses the trends, opportunities, and challenges in using big data and digitalization in the tourism sector. It highlights how big data is being leveraged for COVID-19 recovery and examines its relationship with statistical frameworks to better measure the economic, social, and environmental impact of tourism. Case studies of partnerships in Asia and the Pacific between the public and private sector demonstrate ways to tap big data.
Crimes Committed by Terrorist Groups SAGE Publishing India
Where is the line between digital utopia and digital police state? Surveillance State tells the gripping, startling, and detailed story of how China's Communist Party is building a new kind of political control: shaping the will of the people through the sophisticated—and often brutal—harnessing of data. It is a story born in Silicon Valley and America's "War on Terror," and now playing out in alarming ways on China's remote Central Asian frontier. As a minority separatist movement strains against Party control, China's leaders have built a dystopian police state that keeps millions under the constant gaze of security forces armed with AI. But across the country in the city of Hangzhou, the government is weaving a digital utopia, where technology helps optimize everything from traffic patterns to food safety to emergency response. Award-winning journalists Josh Chin and Liza Lin take readers on a journey through the new world China is building within its borders, and beyond. Telling harrowing stories of the people and families affected by the Party's ambitions, Surveillance State reveals a future that is already underway—a new society engineered around the power of digital surveillance.
Big Data for Better Tourism Policy, Management, and Sustainable Recovery from COVID-19 John Wiley & Sons
Cyber Litigation: The Legal Principles brings together the existing legal principles in this rapidly developing area of law whilst at the same time considering the latest challenges facing practitioners and corporate advisers. The authors have surveyed the legal landscape to identify bespoke approaches to the issues involved. The book looks at the most common causes of action in cyber litigation, including 'cybercrime', IP, data protection breaches, and conflict of laws considerations. It analyses the situations where cyber-related litigation requires a new approach and looks at the remedies available. It covers cyber litigation and regulatory enforcement action, as well as alternatives to litigation such as the NCA Prevent scheme, Deferred Prosecution Agreements and Civil Recovery. It describes situations where arbitration or mediation are mandated, as well as online dispute resolution and technology powered alternatives to traditional determination. Readers will benefit from the use of flowcharts, tables, checklists and case studies to provide a clear understanding of the processes involved, as well as legal analysis of significant cases, an insight into what constitutes 'data', and legal analysis and commentary on potential legal arguments that may arise in cyber litigation. Cyber Litigation: The Legal Principles is an essential title for all practitioners involved in commercial disputes, information technology professionals, data protection officers, compliance staff and technologists with a legal interest.
How to Measure Anything in Cybersecurity Risk Bloomsbury Publishing
An expose on what unethical businesses are prepared to do to enhance profits and reputation.
Survivability HarperCollins UK
Today, safeguarding nation-states, organizations, and citizens has less to do with security (cyber and non-cyber) but has everything to do with Survivability. We are now in the 'Era of the Unprecedented': since 2010, Geo-Poli-Cyber™ warfare has been increasing in intensity. The motivation of its perpetrators is often driven by political, ideological, 'religious' and extremist objectives, rather than financial gain. Many top decision makers and citizens are unaware of this reality or the implications it has on their sovereignties, businesses, lives and livelihoods, and most do not know how to mitigate it. This trend has seen governments and businesses constantly breached by high-impact cyberattacks, confirming the ineptitude of best in class cyber security strategies, solutions, policies and procedures. Yet, they continue implementing what they know is failing and ineffective. The 2020 pandemic revealed a fundamental flaw in many Western democratic nations; their failure to appropriately prepare for a threat they knew was coming and the cost of this in human lives. This pandemic has shed light on the weaknesses of the current international order and economic, political, legal and democratic models and structures that enable it. It has also called into question the capacity of existing cyber security protocols and designs to protect nations, companies and citizens. The question remains: are governments ready for cyber terrorism, election meddling, fake news and the malicious use of artificial intelligence and quantum computing? How about them all happening at the same time? Survivability provides potential answers to this and other pressing concerns.
China Internet Development Report 2017 Pearson Educación
A start-to-finish guide for realistically measuring cybersecurity risk In the newly revised How to Measure Anything in Cybersecurity Risk, Second Edition, a pioneering information security professional and a leader in quantitative analysis methods delivers yet another eye-opening text applying the quantitative language of risk analysis to cybersecurity. In the book, the authors demonstrate how to quantify uncertainty and shed light on how to measure seemingly intangible goals. It's a practical guide to improving risk assessment with a straightforward and simple framework. Advanced methods and detailed advice for a variety of use cases round out the book, which also includes: A new "Rapid Risk Audit" for a first quick quantitative risk assessment. New research on the real impact of reputation damage New Bayesian examples for assessing risk with little data New material on simple measurement and estimation, pseudo-random number generators, and advice on combining expert opinion Dispelling long-held beliefs and myths about information security, How to Measure Anything in Cybersecurity Risk is an essential roadmap for IT security managers, CFOs, risk and compliance professionals, and even statisticians looking for novel new ways to apply quantitative techniques to cybersecurity.
Internal Communication and Employee Engagement Penguin UK
This book gives a thorough and systematic introduction to Data, Data Sources, Dimensions of Data, Privacy, and Security Challenges associated with Data, Ethics, Laws, IPR Copyright, and Technology Law. This book will help students, scholars, and practitioners to understand the challenges while dealing with data and its ethical and legal aspects. The book focuses on emerging issues while working with the Data.
Privacy Concerns Surrounding Personal Information Sharing on Health and Fitness Mobile Apps IGI Global
Database Administration, Second Edition, is the definitive, technology-independent guide to the modern discipline of database administration. Packed with best practices and proven solutions for any database platform or environment, this text fully reflects the field's latest realities and challenges. Drawing on more than thirty years of database experience, Mullins focuses on problems that today's DBAs actually face, and skills and knowledge they simply must have. Mullins presents realistic, thorough, and up-to-date coverage of every DBA task, including creating database environments, data modeling, normalization, design, performance, data integrity, compliance, governance, security, backup/recovery, disaster planning, data and storage management, data movement/distribution, data warehousing, connectivity, metadata, tools, and more. This edition adds new coverage of "Big Data," database appliances, cloud computing, and NoSQL. Mullins includes an entirely new chapter on the DBA's role in regulatory compliance, with substantial new material on data breaches, auditing, encryption, retention, and metadata management. You'll also find an all-new glossary, plus up-to-the-minute DBA rules of thumb.

Related with Marriott Data Breach Case Study:
© Marriott Data Breach Case Study Anatomy Of An Elk
© Marriott Data Breach Case Study Anatomy Of Constitution Answer Key
© Marriott Data Breach Case Study Anatomy Of A Pew