Acces PDF Byod Mobile Security Crowd Research Partners

If you ally obsession such a referred **Byod Mobile Security Crowd Research Partners** book that will give you worth, get the no question best seller from us currently from several preferred authors. If you desire to witty books, lots of novels, tale, jokes, and more fictions collections are also launched, from best seller to one of the most current released.

You may not be perplexed to enjoy every book collections Byod Mobile Security Crowd Research Partners that we will categorically offer. It is not approaching the costs. Its approximately what you dependence currently. This Byod Mobile Security Crowd Research Partners, as one of the most working sellers here will certainly be accompanied by the best options to review.

8U31RW - SANTIAGO CHAVEZ

The first comprehensive guide to the design and implementation of security in 5G wireless networks and devices Security models for 3G and 4G networks based on Universal SIM cards worked very well. But they are not fully applicable to the unique security requirements of 5G networks. 5G will face additional challenges due to increased user privacy concerns, new trust and service models and requirements to support IoT and mission-critical applications. While multiple books already exist on 5G, this is the first to focus exclusively on security for the emerging 5G ecosystem. 5G networks are not only expected to be faster, but provide a backbone for many new services, such as IoT and the Industrial Internet. Those services will provide connectivity for everything from autonomous cars and UAVs to remote health monitoring through body-attached sensors, smart logistics through item tracking to remote diagnostics and preventive maintenance of equipment. Most services will be integrated with Cloud computing and novel concepts, such as mobile edge computing, which will require smooth and transparent communications between user devices, data centers and operator networks. Featuring contributions from an international team of experts at the forefront of 5G system design and security, this book: Provides priceless insights into the current and future threats to mobile networks and mechanisms to protect it Covers critical lifecycle functions and stages of 5G security and how to build an effective security architecture for 5G based mobile networks Addresses mobile network security based on network-centricity, device-centricity, information-centricity and people-centricity views Explores security considerations for all relative stakeholders of mobile networks, including mobile network operators, mobile network virtual operators, mobile users, wireless users, Internet-of things, and cybersecurity experts Providing a comprehensive guide to state-of-the-art in 5G security theory and practice, A Comprehensive Guide to 5G Security is an important working resource for researchers, engineers and business professionals working on 5G development and deployment.

Proven security tactics for today's mobile apps, devices, and networks "A great overview of the new threats created by mobile devices. ...The authors have heaps of experience in the topics and bring that to every chapter." -- Slashdot Hacking Exposed Mobile continues in the great tradition of the Hacking Exposed series, arming business leaders and technology practitioners with an in-depth understanding of the latest attacks and countermeasures--so they can leverage the power of mobile platforms while ensuring that security risks are contained." -- Jamil Farshchi, Senior Business Leader of Strategic Planning and Initiatives, VISA Identify and evade key threats across the expanding mobile risk landscape. Hacking Exposed Mobile: Security Secrets & Solutions covers the wide range of attacks to your mobile deployment alongside ready-to-use countermeasures. Find out how attackers compromise networks and devices, attack mobile services, and subvert mobile apps. Learn how to encrypt mobile data, fortify mobile platforms, and eradicate malware. This cutting-edge guide reveals secure mobile development guidelines, how to leverage mobile OS features and MDM to isolate apps and data, and the techniques the pros use to secure mobile payment systems. Tour the mobile risk ecosystem with expert guides to both attack and defense Learn how cellular network attacks compromise devices over-the-air See the latest Android and iOS attacks in action, and learn how to stop them Delve into mobile malware at the code level to understand how to write resilient apps Defend against server-side mobile attacks, including SQL and XML injection Discover mobile web attacks, including abuse of custom URI schemes and JavaScript bridges Develop stronger mobile authentication routines using OAuth and SAML Get comprehensive mobile app development security guidance covering everything from threat modeling to iOS- and Android-specific tips Get started quickly using our mobile pen testing and consumer security checklists

The pace of technological change is accelerating, hyper competition is growing, opportunities for business model disruption are exploding, and comprehensive cloud delivery is readily available. These factors challenge every aspect of business technology strategy. The Innovator’s Imperative: Rapid Technology Adoption for Digital Transformation prepares twenty-first century businesses leaders for competing and leading in this disruptive digital environment. Five years of research conducted by the authors suggests that leading companies have all but abandoned the requirements analysis and modeling best practices of the twentieth century. Accordingly, the authors put forth the innovator’s imperative that contends: All companies wanting to be competitive should adopt emerging and disruptive technologies as quickly as possible, and in many cases, immediately. Technology is driving business strategy, and companies are rethinking their technology strategy, especially the governance that determines how and why technology investments are made. Based on their research the authors have developed a five-step framework for digital transformation: Model and simulate Identify high-leverage opportunities Prioritize transformational targets Identify digital opportunities Find courageous leaders The book explains each of these steps to guide business leaders in architecting digital transformation projects according to their organization’s market positions, budgets, objectives, and corporate culture. Hyper-competitive, disruptive companies are jumping across technology adoption phases without regard to any phasing whatsoever. Companies focused on digital transformation often adopt emerging technologies immediately. They have become early adopters of technologies that can impact existing—and create whole new—business models and processes. This book examines this jump into new technologies, processes, and business models to prepare twen-

ty-first century business leaders to make that leap.

Researchers and practitioners alike often overlook the vital relationship between trust and social media. ... Authors Joanna Paliszkiewicz and Alex Koohang charted a course to explore this abyss with a view to answering the question how does trust influence the use of social media. [i]Dr. John P. Girard, Peyton Anderson Endowed Chair in Information Technology, Middle Georgia State University[/i] The authors have done an excellent job in explaining how trust plays a significant role in social media. The book begins with a thorough overview of social media to its applications in learning, business, and an analysis of social media and trust. The second part of the book uses data from four different countries to answer multiple valid and vital research questions dealing with social media and trust, including an instrument that measures trust variables. This book presents some meaningful work on how the integration of social media and trust can best be developed. The authors apply their backgrounds in information technology, knowledge management, trust, and business to generate some provocative and instructive guidance to the readers on how to best leverage knowledge internally and externally to meet the organizational strategic goals. [i]-Dr. Jay Liebowitz, Distinguished Chair of Applied Business and Finance, Harrisburg University of Science and Technology

Mobile communication has dramatically changed over the past decade with the diffusion of smartphones. Unlike the basic 2G mobile phones, which "merely" facilitated communication between individuals on the move, smartphones allow individuals to communicate, to entertain and inform themselves, to transact, to navigate, to take photos, and countless other things. Mobile communication has thus transformed society by allowing new forms of coordination, communication, consumption, social interaction, and access to news/entertainment. All of this is regardless of the space in which users are immersed. Set in the context of the developed and the developing world, The Oxford Handbook of Mobile Communication and Society updates current scholarship surrounding mobile media and communication. The 43 chapters in this handbook examine mobile communication and its evolving impact on individuals, institutions, groups, societies, and businesses. Contributors examine the communal benefits, social consequences, theoretical perspectives, organizational potential, and future consequences of mobile communication. Topics covered include, among many other things, trends in the Global South, location-based services, and the "appification" of mobile communication and society.

MAT 20 years Topic-wise Solved Papers (1997-2016) consists of detailed solutions of the past 20 years of MAT question papers distributed in 55 topics. The book is divided into 5 sections MATHEMATICAL SKILLS, LANGUAGE COMPREHENSION, DATA ANALYSIS AND SUFFICIENCY, INTELLIGENCE AND CRITICAL REASONING and INDIAN AND GLOBAL ENVIRONMENT. These 5 sections are further divided into 55 chapters. The book is also helpful for other exams like CMAT, NMAT, ATMA, IRMA, SNAP, Bank PO, Bank Clerk, SSC, Railways, etc. To summarise, the book is aimed to serve as one stop solution for all major Competitive Exams. The book contains 5800+ Milestone problems for the major Competitive Exams. The book is fully solved and provides detailed explanation to each and every question. The layout of the book is so simple that a student can prepare/ revise a topic and then solve the previous year questions of that topic from this book.

Explore the game-changing technology that allows mobile learningto effectively reach K-12 students Mobile Learning: A Handbook for Developers, Educators andLearners provides research-based foundations for developing,evaluating, and integrating effective mobile learning pedagogy.Twenty-first century students require twenty-first centurytechnology, and mobile devices provide new and effective ways toeducate children. But with new technologies come new challenges—therefore,this handbook presents a comprehensive look at mobile learning bysynthesizing relevant theories and drawing practical conclusionsfor developers, educators, and students. Mobile devices—in ways that the laptop, the personalcomputer, and netbook computers have not—present theopportunity to make learning more engaging, interactive, andavailable in both traditional classroom settings and informallearning environments. From theory to practice, MobileLearning explores how mobile devices are different than theirtechnological predecessors, makes the case for developers,teachers, and parents to invest in the technology, and illustratesthe many ways in which it is innovative, exciting, and effective ineducating K-12 students. Explores how mobile devices can support the needs ofstudents Provides examples, screenshots, graphics, and visualizations toenhance the material presented in the book Provides developers with the background necessary to create theapps their audience requires Presents the case for mobile learning in and out of classroomsas early as preschool Discusses how mobile learning enables better educationalopportunities for the visually impaired, students with Autism, andadult learners. If you're a school administrator, teacher, app developer, orparent, this topical book provides a theoretical, well-researcheddiscussion of the pedagogical theory and mobile learning, as wellas practical advice in setting up a mobile learning strategy.

The book presents the best contributions from the international scientific conference “Growth Poles of the Global Economy: Emergence, Changes and Future,” which was organized by the Institute of Scientific Communications (Volgograd, Russia) together with the universities of Kyrgyzstan and various other cities in Russia. The 143 papers selected, focus on spatial and sectorial structures of the modern global economy according to the theory of growth poles. It is intended for representatives of the academic community: university and college staff developing study guides on socio-humanitarian disciplines in connection with the theory of growth poles, researchers, and undergraduates, masters, and postgraduates who are interested in the recent inventions and developments in the field. It is also a valuable resource for expert practitioners managing entrepreneurial structures in the existing and prospective growth poles of the global economy as well as those at international institutes that regulate growth poles. The first part of the book investigates the factors and conditions affecting the emergence of the growth poles of the modern global economy. The second part then discusses transformation processes in the traditional growth poles of the global economy under the influence of the technological progress. The third part examines how social factors affect the formation of new growth poles of the modern global economy. Lastly, the fourth part offers perspectives on the future growth of the global economy on the basis of the digital economy and Industry 4.0.

This book constitutes the refereed proceedings of the 8th International Conference on Grid and Pervasive Computing, GPC 2013, held in Seoul, Korea, in May 2013 and the following colocated workshops: International Workshop on Ubiquitous and Multimedia Application Systems, UMAS 2013; International Workshop DATICS-GPC 2013: Design, Analysis and Tools for Integrated Circuits and Systems; and International Workshop on Future Science Technologies and Applications, FSTA 2013. The 111 revised papers were carefully reviewed and selected from numerous submissions. They have

been organized in the following topical sections: cloud, cluster and grid; middleware resource management; mobile peer--to-peer and pervasive computing; multi--core and high-performance computing; parallel and distributed systems; security and privacy; ubiquitous communications, sensor networking, and RFID; ubiquitous and multimedia application systems; design, analysis and tools for integrated circuits and systems; future science technologies and applications; and green and human information technology.

The fast-food worker finds refuge in a bathroom stall to respond to her boyfriend's fifth message in an hour. The human resources manager sees a colleague sending a stream of text messages during a meeting and quickly grabs her mobile to make sure she's also multitasking. These scenarios are common, but unique to the 21st century. Until the early 2000s, workplaces provided most of the computers and portable devices that employees used to perform their jobs and communicate with others. Today, people bring their own mobile devices to work and create new norms for how communication occurs in the workplace. Managers and organizations respond by setting and enforcing new policies that are intended to help them navigate the ever-changing mobile-communication environment. In Negotiating Control: Organizations and Mobile Communication, Keri K. Stephens responds to the struggles of employees, organizations, and even friends and family, as they try to understand new norms for connectedness in the workplace. Drawing on over two decades of her own research and fieldwork, , representing people in over 35 different types of jobs, Stephens claims that though people assume mobile communication is a uniform practice, there are underlying -- and often hidden -- issues of control and power at play, which shape how people are permitted and expected to use mobiles to communicate while working. The accounts Stephens offers reveal the many ways that these portable tools are actually used across work environments today, integrating information, communication, and data, and connecting people in expected and often conflicting ways.

Written by an industry expert, Wireless and Mobile Device Security explores the evolution of wired networks to wireless networking and its impact on the corporate world.

This document provides info. to organizations on the security capabilities of Bluetooth and provide recommendations to organizations employing Bluetooth technologies on securing them effectively. It discusses Bluetooth technologies and security capabilities in technical detail. This document assumes that the readers have at least some operating system, wireless networking, and security knowledge. Because of the constantly changing nature of the wireless security industry and the threats and vulnerabilities to the technologies, readers are strongly encouraged to take advantage of other resources (including those listed in this document) for more current and detailed information. Illustrations.

There can be no doubt that mobile technologies are here to stay. Global mobile traffic grew 74 percent in 2015 alone, with 563 million devices and connections added -- most of them tablets and Smartphones. This growth has been 4000-fold in the past 10 years and 400 million-fold in the past 15 years (Cisco, 2016). Mobile technologies permeate the lives of 21st century citizens as mainstays of organizational and institutional day-to-day operations, commerce, and communication and as tools used to support individuals' personal, social, and career responsibilities. In both the corporate and educational worlds, e- and m-learning and marketing with mobile technologies are moving forward at breakneck speed with, in many cases, a blurring of traditional sector boundaries. As neither the technology nor the uses are static, exploring practices and policies that underpin this quickly shifting mobile technology context is crucial for ensuring its intelligent, purposeful, and equitable use. This edited book provides a venue for researchers to share their work on mobile learning with a focus on uses for mobiles in informal settings and PK-20 classrooms, language learning, mobile gaming, leadership and policy issues, and what mobile learning in the future may be. It assists researchers and educators to consider and answer questions such as: What is "mobile learning" today? How can mobiles be used to enable learning? How is mobile learning crossing or connecting economic, social, and/or cultural sectors? How do specific cultural practices with media influence mobile learning (e.g., youth practices, educator practices, parent practices, community practices)? What are policy and leadership implications in supporting mobile learning? What policies, practices, and/or pedagogical approaches are necessary to move forward with mobiles in schools or universities? In what ways is mobile learning impacting education; including how students learn and teachers teach? What will/ should/might mobile learning look like in the future?

Bring Your Own Device (BYOD) to Work examines the emerging BYOD (Bring Your Own Device to work) trend in corporate IT. BYOD is the practice of employees bringing personally-owned mobile devices (e.g., smartphones, tablets, laptops) to the workplace, and using those devices to access company resources such as email, file servers, and databases. BYOD presents unique challenges in data privacy, confidentiality, security, productivity, and acceptable use that must be met proactively by information security professionals. This report provides solid background on the practice, original research on its pros and cons, and actionable recommendations for implementing a BYOD program. Successful programs are cross-functional efforts including information technology, human resources, finance, legal, security, and business operating teams. This report is a valuable resource to any security professional considering a BYOD program. Bring Your Own Device (BYOD) to Work is a part of Elsevier's Security Executive Council Risk Management Portfolio, a collection of real world solutions and "how-to" guidelines that equip executives, practitioners, and educators with proven information for successful security and risk management programs. Presents research data associated with BYOD and productivity in the workplace Describes BYOD challenges, risks, and liabilities Makes recommendations for the components a clearly communicated BYOD program should contain

Personalized Learning: A Guide for Engaging Students with Technology is designed to help educators make sense of the shifting landscape in modern education. While changes may pose significant challenges, they also offer countless opportunities to engage students in meaningful ways to improve their learning outcomes. Personalized learning is the key to engaging students, as teachers are leading the way toward making learning as relevant, rigorous, and meaningful inside school as outside and what kids do outside school: connecting and sharing online, and engaging in virtual communities of their own Renowned author of the Heck: Where the Bad Kids Go series, Dale Basye, and award winning educator Peggy Grant, provide a go-to tool available to every teacher today—technology as a way to 'personalize' the education experience for every student, enabling students to learn at their various paces and in the way most appropriate to their learning styles.

Since agriculture is one of the key parameters in assessing the gross domestic product (GDP) of any country, it has become crucial to transition from traditional agricultural practices to smart agriculture. New agricultural technologies provide numerous opportunities to maximize crop yield by recognizing and analyzing diseases and

other natural variables that may affect it. Therefore, it is necessary to understand how computer-assisted technologies can best be utilized and adopted in the conversion to smart agriculture. Modern Techniques for Agricultural Disease Management and Crop Yield Prediction is an essential publication that widens the spectrum of computational methods that can aid in agriculture disease management, weed detection, and crop yield prediction. Featuring coverage on a wide range of topics such as soil and crop sensors, swarm robotics, and weed detection, this book is ideally designed for environmentalists, farmers, botanists, agricultural engineers, computer engineers, scientists, researchers, practitioners, and students seeking current research on technology and techniques for agricultural diseases and predictive trends.

Security is a major consideration in the way that business and information technology systems are designed, built, operated, and managed. The need to be able to integrate security into those systems and the discussions with business functions and operations exists more than ever. This IBM® Redbooks® publication explores concerns that characterize security requirements of, and threats to, business and information technology (IT) systems. This book identifies many business drivers that illustrate these concerns, including managing risk and cost, and compliance to business policies and external regulations. This book shows how these drivers can be translated into capabilities and security needs that can be represented in frameworks, such as the IBM Security Blueprint, to better enable enterprise security. To help organizations with their security challenges, IBM created a bridge to address the communication gap between the business and technical perspectives of security to enable simplification of thought and process. The IBM Security Framework can help you translate the business view, and the IBM Security Blueprint describes the technology landscape view. Together, they can help bring together the experiences that we gained from working with many clients to build a comprehensive view of security capabilities and needs. This book is intended to be a valuable resource for business leaders, security officers, and consultants who want to understand and implement enterprise security by considering a set of core security capabilities and services.

This book contains the latest research work presented at the International Conference on Computing and Communication Systems (I3CS 2020) held at North-Eastern Hill University (NEHU), Shillong, India. The book presents original research results, new ideas and practical development experiences which concentrate on both theory and practices. It includes papers from all areas of information technology, computer science, electronics and communication engineering written by researchers, scientists, engineers and scholar students and experts from India and abroad.

Fully updated: The complete guide to Cisco Identity Services Engine solutions Using Cisco Secure Access Architecture and Cisco Identity Services Engine, you can secure and gain control of access to your networks in a Bring Your Own Device (BYOD) world. This second edition of Cisco ISE for BYOD and Secure Unified Accesscontains more than eight brand-new chapters as well as extensively updated coverage of all the previous topics in the first edition book to reflect the latest technologies, features, and best practices of the ISE solution. It begins by reviewing today's business case for identity solutions. Next, you walk through ISE foundational topics and ISE design. Then you explore how to build an access security policy using the building blocks of ISE. Next are the in-depth and advanced ISE configuration sections, followed by the troubleshooting and monitoring chapters. Finally, we go in depth on the new TACACS+ device administration solution that is new to ISE and to this second edition. With this book, you will gain an understanding of ISE configuration, such as identifying users, devices, and security posture; learn about Cisco Secure Access solutions; and master advanced techniques for securing access to networks, from dynamic segmentation to guest access and everything in between. Drawing on their cutting-edge experience supporting Cisco enterprise customers, the authors offer in-depth coverage of the complete lifecycle for all relevant ISE solutions, making this book a cornerstone resource whether you're an architect, engineer, operator, or IT manager. - Review evolving security challenges associated with borderless networks, ubiquitous mobility, and consumerized IT - Understand Cisco Secure Access, the Identity Services Engine (ISE), and the building blocks of complete solutions - Design an ISE-enabled network, plan/distribute ISE functions, and prepare for rollout - Build context-aware security policies for network access, devices, accounting, and audit - Configure device profiles, visibility, endpoint posture assessments, and guest services - Implement secure guest lifecycle management, from WebAuth to sponsored guest access - Configure ISE, network access devices, and supplicants, step by step - Apply best practices to avoid the pitfalls of BYOD secure access - Set up efficient distributed ISE deployments - Provide remote access VPNs with ASA and Cisco ISE - Simplify administration with self-service onboarding and registration - Deploy security group access with Cisco TrustSec - Prepare for high availability and disaster scenarios - Implement passive identities via ISE-PIC and EZ Connect - Implement TACACS+ using ISE - Monitor, maintain, and troubleshoot ISE and your entire Secure Access system - Administer device AAA with Cisco IOS, WLC, and Nexus Normal 0 false false false EN-US X-NONE X-NONE

Where end-users once queued up to ask the IT department for permission to buy a new computer or a new version of software, they are now bypassing IT altogether and buying it on their own. From laptops and smartphones to iPads and virtually unlimited software apps, end-users have tasted their freedom and love it. IT will simply never be the same.Bri

Mobile Cloud Computing: Models, Implementation, and Security provides a comprehensive introduction to mobile cloud computing, including key concepts, models, and relevant applications. The book focuses on novel and advanced algorithms, as well as mobile app development. The book begins with an overview of mobile cloud computing concepts, models, and service deployments, as well as specific cloud service models. It continues with the basic mechanisms and principles of mobile computing, as well as virtualization techniques. The book also introduces mobile cloud computing architecture, design, key techniques, and challenges. The second part of the book covers optimizations of data processing and storage in mobile clouds, including performance and green clouds. The crucial optimization algorithm in mobile cloud computing is also explored, along with big data and service computing. Security issues in mobile cloud computing are covered in-depth, including a brief introduction to security and privacy issues and threats, as well as privacy protection techniques in mobile systems. The last part of the book features the integration of service-oriented architecture with mobile cloud computing. It discusses web service specifications related to implementations of mobile cloud computing. The book not only presents critical concepts in mobile cloud systems, but also drives readers to deeper research, through open discussion questions. Practical case studies are also included. Suitable for graduate students and professionals, this book provides a detailed and timely overview of mobile cloud computing for a broad range of readers.

Effective Research Data Management (RDM) is a key component of research integrity and reproducible research, and its importance is increasingly emphasised by funding bodies, governments, and research institutions around the world. However, many researchers are unfamiliar with RDM best practices, and research support staff are faced with the difficult task of delivering support to researchers across different disciplines and career stages. What strategies can institutions use to solve these problems? Engaging Researchers with Data Management is an invaluable collection of 24 case studies, drawn from institutions across the globe, that demonstrate clearly and practically how to engage the research community with RDM. These case studies together illustrate the variety of innovative strategies research institutions have developed to engage with their researchers about managing research data. Each study is presented concisely and clearly, highlighting the essential ingredients that led to its success and challenges encountered along the way. By interviewing key staff about their experiences and the organisational context, the authors of this book have created an essential resource for organisations looking to increase engagement with their research communities. This handbook is a collaboration by research institutions, for research institutions. It aims not only to inspire and engage, but also to help drive cultural change towards better data management. It has been written for anyone interested in RDM, or simply, good research practice.

You may regard cloud computing as an ideal way for your company to control IT costs, but do you know how private and secure this service really is? Not many people do. With Cloud Security and Privacy, you'll learn what's at stake when you trust your data to the cloud, and what you can do to keep your virtual infrastructure and web applications secure. Ideal for IT staffers, information security and privacy practitioners, business managers, service providers, and investors alike, this book offers you sound advice from three well--known authorities in the tech security world. You'll learn detailed information on cloud computing security that-until now-has been sorely lacking. Review the current state of data security and storage in the cloud, including confidentiality, integrity, and availability Learn about the identity and access management (IAM) practice for authentication, authorization, and auditing of the users accessing cloud services Discover which security management frameworks and standards are relevant for the cloud Understand the privacy aspects you need to consider in the cloud, including how they compare with traditional computing models Learn the importance of audit and compliance functions within the cloud, and the various standards and frameworks to consider Examine security delivered as a service-a different facet of cloud security

Creating Business Agility: How Convergence of Cloud, Social, Mobile, Video, and Big Data Enables Competitive Advantage provides a game plan for integrating technology to build a smarter, more customer--centric business. Using a series of case studies as examples throughout, the book describes the agility that comes from collaborative commerce, and provides key decision makers the implementation roadmap they need to build a successful business ecosystem. The focus is on Business Agility Readiness in terms of the five major changes affecting the information technology landscape, and how data-driven delivery platforms and decision-making processes are being reinvented using digital relationships with a social business model as the consumer world of technology drives innovation and collaboration. Cloud computing, social media, next-gen mobility, streaming video, and big data with predictive analytics are major forces now for a competitive advantage, and Creating Business Agility provides leaders with a roadmap for readiness. Business leaders tasked with innovation and strategy will find that Creating Business Agility provides important insight from an informed perspective.

Surveys the online social habits of American teens and analyzes the role technology and social media plays in their lives, examining common misconceptions about such topics as identity, privacy, danger, and bullying.

Order your instructor's e-inspection copy on VitalSource. Using secondary data offers unique opportunities and challenges. This practical book will guide you through finding, managing and analysing qualitative secondary data in an error-free way. Perfect for those doing dissertations and research projects, it provides an accessible introduction to the theory of secondary research and sets out the advantages and limitations of using this kind of research. Drawing on years of teaching and research experience, the authors · Offer step-by-step advice on how to use qualitative secondary data · Walk you through each stage of the research process · Provide practical, ethical tools to help you with your project · Show you how to avoid the potential pitfalls of using secondary data. Clear and easy to understand, this book is a ready-made toolkit for successfully using qualitative secondary data. From beginner level and beyond, this no-nonsense guide takes the confusion and worry out of doing a secondary research project.

This book introduces several cybersecurity and privacy research challenges and how they are being addressed in the scope of 15 European research projects.Each chapter is dedicated to a different funded European Research project, which aims to cope with digital security and privacy aspects, risks, threats and cybersecurity issues.

Plan and deploy identity-based secure access for BYOD and borderless networks Using Cisco Secure Unified Access Architecture and Cisco Identity Services Engine, you can secure and regain control of borderless networks in a Bring Your Own Device (BYOD) world. This book covers the complete lifecycle of protecting a modern borderless network using these advanced solutions, from planning an architecture through deployment, management, and troubleshooting. Cisco ISE for BYOD and Secure Unified Access begins by reviewing the business case for an identity solution. Next, you'll walk through identifying users, devices, and security posture; gain a deep understanding of Cisco's Secure Unified Access solution; and master powerful techniques for securing borderless networks, from device isolation to protocol-independent network segmentation. You'll find in--depth coverage of all relevant technologies and techniques, including 802.1X, profiling, device onboarding, guest lifecycle management, network admission control, RADIUS, and Security Group Access. Drawing on their cutting-edge experience supporting Cisco enterprise customers, the authors present detailed sample configurations to help you plan your own integrated identity solution. Whether you're a technical professional or an IT manager, this guide will help you provide reliable secure access for BYOD, CYOD (Choose Your Own Device), or any IT model you choose. Review the new security challenges associated with borderless networks, ubiquitous mobility, and consumerized IT Understand the building blocks of an Identity Services Engine (ISE) solution Design an ISE-Enabled network, plan/distribute ISE functions, and prepare for rollout Build context-aware security policies Configure device profiling, endpoint posture assessments, and guest services Implement secure guest lifecycle management, from WebAuth to sponsored guest access Configure ISE, network access devices, and supplicants, step-by-step Walk through a phased deployment that en-

sures zero downtime Apply best practices to avoid the pitfalls of BYOD secure access Simplify administration with self-service onboarding and registration Deploy Security Group Access, Cisco’s tagging enforcement solution Add Layer 2 encryption to secure traffic flows Use Network Edge Access Topology to extend secure access beyond the wiring closet Monitor, maintain, and troubleshoot ISE and your entire Secure Unified Access system

Adaptive Mobile Computing: Advances in Processing Mobile Data Sets explores the latest advancements in producing, processing and securing mobile data sets. The book provides the elements needed to deepen understanding of this trend which, over the last decade, has seen exponential growth in the number and capabilities of mobile devices. The pervasiveness, sensing capabilities and computational power of mobile devices have turned them into a fundamental instrument in everyday life for a large part of the human population. This fact makes mobile devices an incredibly rich source of data about the dynamics of human behavior, a pervasive wireless sensors network with substantial computational power and an extremely appealing target for a new generation of threats. Offers a coherent and realistic image of today’s architectures, techniques, protocols, components, orchestration, choreography and development related to mobile computing Explains state-of-the-art technological solutions for the main issues hindering the development of next-generation pervasive systems including: supporting components for collecting data intelligently, handling resource and data management, accounting for fault tolerance, security, monitoring and control, addressing the relation with the Internet of Things and Big Data and depicting applications for pervasive context-aware processing Presents the benefits of mobile computing and the development process of scientific and commercial applications and platforms to support them Familiarizes readers with the concepts and technologies that are successfully used in the implementation of pervasive/ubiquitous systems

Due to changes in the learning and research environment, changes in the behavior of library users, and unique global disruptions such as the COVID-19 pandemic, libraries have had to adapt and evolve to remain up-to-date and responsive to their users. Thus, libraries are adding new, digital resources and services while maintaining most of the old, traditional resources and services. New areas of research and inquiry in the field of library and information science explore the applications of machine learning, artificial intelligence, and other technologies to better serve and expand the library community. The Handbook of Research on Knowledge and Organization Systems in Library and Information Science examines new technologies and systems and their application and adoption within libraries. This handbook provides a global perspective on current and future trends concerning library and information science. Covering topics such as machine learning, library management, ICTs, blockchain technology, social media, and augmented reality, this book is essential for librarians, library directors, library technicians, media specialists, data specialists, catalogers, information resource officers, administrators, IT consultants and specialists, academicians, and students.

Corporate Security Management provides practical advice on efficiently and effectively protecting an organization's processes, tangible and intangible assets, and people. The book merges business and security perspectives to help transform this often conflicted relationship into a successful and sustainable partnership. It combines security doctrine, business priorities, and best practices to uniquely answer the Who, What, Where, Why, When and How of corporate security. Corporate Security Management explores the diverse structures of security organizations in different industries. It shows the crucial corporate security competencies needed and demonstrates how they blend with the competencies of the entire organization. This book shows how to identify, understand, evaluate and anticipate the specific risks that threaten enterprises and how to design successful protection strategies against them. It guides readers in developing a systematic approach to assessing, analyzing, planning, quantifying, administrating, and measuring the security function. Addresses the often opposing objectives between the security department and the rest of the business concerning risk, protection, outsourcing, and more Shows security managers how to develop business acumen in a corporate security environment Analyzes the management and communication skills needed for the corporate security manager Focuses on simplicity, logic and creativity instead of security technology Shows the true challenges of performing security in a profit-oriented environment, suggesting ways to successfully overcome them Illustrates the numerous security approaches and requirements in a wide variety of industries Includes case studies, glossary, chapter objectives, discussion questions and exercises

Market research has never been more important. As organizations become increasingly sophisticated, the need to profile customers, deliver customer satisfaction, target certain audiences, develop their brands, optimize prices and more has grown. Lively and accessible, Market Research in Practice is a practical introduction to market research tools, approaches and issues. Providing a clear, step-by-step guide to the whole process - from planning and executing a project through to analyzing and presenting the findings - it explains how to use tools and methods effectively to obtain reliable results. This fully updated third edition of Market Research in Practice has been revised to reflect the most recent trends in the industry. Ten new chapters cover topical issues such as ethics in market research and qualitative and quantitative research, plus key concepts such as international research, how to design and scope a survey, how to create a questionnaire, how to choose a sample and how to carry out interviews are covered in detail. Tips, and advice from the authors' own extensive experiences are included throughout to ground the concepts in business reality. Accompanied by a range of online tools, templates, surveys and guides, this is an invaluable guide for students of research methods, researchers, marketers and users of market research. Online resources include a range of tools, templates, surveys and guides.

The prominence and growing dependency on information communication technologies in nearly every aspect of life has opened the door to threats in cyberspace. Criminal elements inside and outside organizations gain access to information that can cause financial and reputational damage. Criminals also target individuals daily with personal devices like smartphones and home security systems who are often unaware of the dangers and the privacy threats around them. The Handbook of Research on Information and Cyber Security in the Fourth Industrial Revolution is a critical scholarly resource that creates awareness of the severity of cyber information threats on personal, business, governmental, and societal levels. The book explores topics such as social engineering in information security, threats to cloud computing, and cybersecurity resilience during the time of the Fourth Industrial Revolution. As a source that builds on available literature and expertise in the field of information technology and security, this publication proves useful for academicians, educationalists, policy makers, government officials, students, researchers, and business leaders and managers.

Winner of the AECT Division of Distance Learning (DDL) Distance Education Book

Award! This handbook provides a comprehensive compendium of research in all aspects of mobile learning, one of the most significant ongoing global developments in the entire field of education. Rather than focus on specific technologies, expert authors discuss how best to utilize technology in the service of improving teaching and learning. For more than a decade, researchers and practitioners have been exploring this area of study as the growing popularity of smartphones, tablets, and other such devices, as well as the increasingly sophisticated applications for these devices, has allowed educators to accommodate and support an increasingly mobile society. This handbook provides the first authoritative account of the theory and research that underlies mobile learning, while also exemplifying models of current and future practice.

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

ucts to market faster. The 6 irrefutable laws of information security should be on a stone plaque on the desk of every security professional." Steven Proctor, VP, Audit & Risk Management, Flextronics

Cybersecurity and Privacy in Cyber-Physical Systems collects and reports on recent high-quality research that addresses different problems related to cybersecurity and privacy in cyber-physical systems (CPSs). It Presents high-quality contributions addressing related theoretical and practical aspects Improves the reader's awareness of cybersecurity and privacy in CPSs Analyzes and presents the state of the art of CPSs, cybersecurity, and related technologies and methodologies Highlights and discusses recent developments and emerging trends in cybersecurity and privacy in CPSs Proposes new models, practical solutions, and technological advances related to cybersecurity and privacy in CPSs Discusses new cybersecurity and privacy models, prototypes, and protocols for CPSs This comprehensive book promotes high--quality research by bringing together researchers and experts in CPS security and privacy from around the world to share their knowledge of the different aspects of CPS security. Cybersecurity and Privacy in Cyber-Physical Systems is ideally suited for policymakers, industrial engineers, researchers, academics, and professionals seeking a thorough understanding of the principles of cybersecurity and privacy in CPSs. They will learn about promising solutions to these research problems and identify unresolved and challenging problems for their own research. Readers will also have an overview of CPS cybersecurity and privacy design.

Strategy is a much-discussed, much-misunderstood topic among managers. In this new edition of The Strategic Manager, Harry Sminia continues to focus on how strategy works in practice, questioning readers' existing expectations that strategy is a matter of strategic planning in order to help them to move into practicing strategy as an everyday activity. The book is based around six different strategy theories, individually presented and supplemented with useful lists of questions that encourage readers to become competent strategic thinkers. Bridging theory and practice, a range of real life case studies open a window into the real world of strategic management. Essential reading for postgraduate students and those in executive education, this text will also be a useful tool for managers trying to develop a better understanding of this easily confused subject.

The perimeter defenses guarding your network perhaps are not as secure as you think. Hosts behind the firewall have no defenses of their own, so when a host in the "trusted" zone is breached, access to your data center is not far behind. That's an all--too-familiar scenario today. With this practical book, you'll learn the principles behind zero trust architecture, along with details necessary to implement it. The Zero Trust Model treats all hosts as if they're internet-facing, and considers the entire network to be compromised and hostile. By taking this approach, you'll focus on building strong authentication, authorization, and encryption throughout, while providing compartmentalized access and better operational agility. Understand how perimeter-based defenses have evolved to become the broken model we use today Explore two case studies of zero trust in production networks on the client side (Google) and on the server side (PagerDuty) Get example configuration for open source tools that you can use to build a zero trust network Learn how to migrate from a perimeter-based network to a zero trust network in production

The five-volume set LNCS 9155-9159 constitutes the refereed proceedings of the 15th International Conference on Computational Science and Its Applications, ICCSA 2015, held in Banff, AB, Canada, in June 2015. The 232 revised full papers presented in 22 workshops and a general track were carefully reviewed and selected from 780 initial submissions for inclusion in this volume. They cover various areas in computational science ranging from computational science technologies to specific areas of computational science such as computational geometry and security.

"Information Systems for Business and Beyond introduces the concept of information systems, their use in business, and the larger impact they are having on our world."--BC Campus website.