Cisa 2015

Right here, we have countless books **Cisa 2015** and collections to check out. We additionally come up with the money for variant types and furthermore type of the books to browse. The agreeable book, fiction, history, novel, scientific research, as capably as various new sorts of books are readily easily reached here.

As this Cisa 2015, it ends taking place bodily one of the favored ebook Cisa 2015 collections that we have. This is why you remain in the best website to look the incredible book to have.

Cisa 2015 ***2021-04-25***

MACK JAYCE

China's New Sources of Economic Growth: Vol. 1 CRC Press Threat intelligence is a surprisingly complex topic that goes far beyond the obvious technical challenges of collecting, modelling and sharing technical indicators. Most books in this area focus mainly on technical measures to harden a system based on threat intel data and limit their scope to single organizations only. This book provides a unique angle on the topic of national cyber threat intelligence and security information sharing. It also provides a clear view on ongoing works in research laboratories world-wide in order to address current security concerns at national level. It allows practitioners to learn about upcoming trends, researchers to share current results, and decision makers to prepare for future developments.

Foundations of Homeland Security Emerald Group Publishing Like most aspects of modern existence, more and more of our financial lives have migrated to the digital realm. With the benefits of ease that our Internet allows us, that transition also raises numerous – and dangerous – threats to national security, our money, and the systems we use to store and transfer it. In TheUnhackable Internet, financial services and technology expert Thomas P. Vartanian exposes the vulnerabilities of the many networks that we rely on today as well as the threats facing the integrity of our national security and financial services sector. From cyberattacks by foreign adversaries like China and Russia, the explosion of cryptocurrency, the advancement of ransomware, phishing, surveillance apps, spying software, and logic bombs, along with the increasing savvy and daring shown by Internet hackers, the next financial panic is likely to be delivered to us through use or abuse of technology. The Unhackable Internet describes how society can remake an Internet that was never conceived as a secure environment and badly tainted by the original sin of substandard coding. Vartanian argues for increasing the use of private and offline network infrastructures, controlling the ownership of Internet infrastructure, and imposing enhanced authentication,

governance, and enforcement standards. This online universe would look more like our analog lives, authenticating all digital traffic to a real person and removing any virtual traveler that violated the new rules of the road. The Unhackable Internet poses a challenge to America: take the lead and create a coalition of democratic nations to implement financial cyber strategies or be left with no counterweight short of military power to respond to those who weaponize technology. This comprehensive and compelling book makes it clear that nothing less than the control of global economies is up for grabs, and that how we use technology is our choice.

Industry Perspectives on the President's Cybersecurity Information-sharing Proposal Rowman & Littlefield

The book contains several new concepts, techniques, applications and case studies for cyber securities in parallel and distributed computing The main objective of this book is to explore the concept of cybersecurity in parallel and distributed computing along with recent research developments in the field. Also included are various real-time/offline applications and case studies in the fields of engineering and computer science and the modern tools and technologies used. Information concerning various topics relating to cybersecurity technologies is organized within the sixteen chapters of this book. Some of the important topics covered include: Research and solutions for the problem of hidden image detection Security aspects of data mining and possible solution techniques A comparative analysis of various methods used in e-commerce security and how to perform secure payment transactions in an efficient manner Blockchain technology and how it is crucial to the security industry Security for the Internet of Things Security issues and challenges in distributed computing security such as heterogeneous computing, cloud computing, fog computing, etc. Demonstrates the administration task issue in unified cloud situations as a multi-target enhancement issue in light of security Explores the concepts of cybercrime and cybersecurity and presents the statistical impact it is having on organizations Security policies and mechanisms, various categories of attacks (e.g., denial-of-service), global security architecture, along with distribution of security mechanisms Security issues in the healthcare sector with existing solutions and emerging threats.

European Criminal Law University of California Press

Cybercrime and Information Technology: Theory and Practice—The Computer Network Infostructure and Computer Security, Cybersecurity Laws, Internet of Things (IoT), and Mobile Devices is an introductory text addressing current technology, trends, and security issues. While many books on the market cover investigations, forensic recovery, and presentation of evidence, and others explain computer and network security, this book explores both, explaining the essential principles governing computers, wireless and mobile devices, the Internet of Things, cloud systems, and their significant vulnerabilities. Only with this knowledge can students truly appreciate the security challenges and opportunities for cybercrime that cannot be uncovered, investigated, and adjudicated unless they are understood. The legal portion of the book is an overview of the legal system in the United States, including cyberlaw standards, and regulations affecting cybercrime. This section includes cases in progress that are shaping and developing legal precedents. As is often the

case, new technologies require new statues and regulations—something the law is often slow to move on given the current speed in which technology advances. Key Features: Provides a strong foundation of cybercrime knowledge along with the core concepts of networking, computer security, Internet of Things (IoTs), and mobile devices. Addresses legal statutes and precedents fundamental to understanding investigative and forensic issues relative to evidence collection and preservation. Identifies the new security challenges of emerging technologies including mobile devices, cloud computing, Software-as-a-Service (SaaS), VMware, and the Internet of Things. Strengthens student understanding of the fundamentals of computer and network security, concepts that are often glossed over in many textbooks, and includes the study of cybercrime as critical forward-looking cybersecurity challenges. Cybercrime and Information Technology is a welcome addition to the literature, particularly for those professors seeking a more hands-on, forward-looking approach to technology and trends. Coverage is applicable to all forensic science courses in computer science and forensic programs, particularly those housed in criminal justice departments emphasizing digital evidence and investigation processes. The textbook is appropriate for courses in the Computer Forensics and Criminal Justice curriculum, and is relevant to those studying Security Administration, Public Administrations, Police Studies, Business Administration, Computer Science, and Information Systems. An Instructor's Manual with Test Bank and chapter PowerPoint slides is available to qualified professors for use in classroom instruction.

The Oxford Handbook of Cyber Security FriesenPress

Building an Effective Security Program for Distributed Energy Resources and Systems Build a critical and effective security program for DERs Building an Effective Security Program for Distributed Energy Resources and Systems requires a unified approach to establishing a critical security program for DER systems and Smart Grid applications. The methodology provided integrates systems security engineering principles, techniques, standards, and best practices. This publication introduces engineers on the design, implementation, and maintenance of a security program for distributed energy resources (DERs), smart grid, and industrial control systems. It provides security professionals with understanding the specific requirements of industrial control systems and real-time constrained applications for power systems. This book: Describes the cybersecurity needs for DERs and power grid as critical infrastructure Introduces the information security principles to assess and manage the security and privacy risks of the emerging Smart Grid technologies Outlines the functions of the security program as well as the scope and differences between traditional IT system security requirements and those required for industrial control systems such as SCADA systems Offers a full array of resources—cybersecurity concepts, frameworks, and emerging trends Security Professionals and Engineers can use Building an Effective Security Program for Distributed Energy Resources and Systems as a reliable resource that is dedicated to the essential topic of security for distributed energy resources and power grids. They will find standards, guidelines, and recommendations from standards organizations, such as ISO, IEC, NIST, IEEE, ENISA, ISA, ISACA, and ISF, conveniently included for reference within

chapters.
The Digital Supply Chain Rowman & Littlefield
Security studies, also known as international security studies, is an academic subfield within the wider discipline of international relations that examines organized violence, military conflict, and national security. Meant to serve as an introduction to the field of security studies, Contextualizing Security is a collection of original essays, primary source lectures, and previously published material in the overlapping fields of security studies, political science, sociology, journalism, and philosophy. It offers both graduate and undergraduate students a grasp on both foundational issues and more contemporary debates in security studies. Nineteen chapters cover security studies in the context of homeland security and liberty, U.S. foreign policy, lessons from the Cold War, science and technology policy, drones, cybersecurity, the War on Terror, migration, study-abroad programs, the surveillance state, Africa, and China. CONTRIBUTORS: Amelia Ayers, James E. Baker, Roy D. Blunt, Mark Boulton, Naji Bsisu, Robert E. Burnett, Daniel Egbe, Laila Farooq, Lisa Fein, Anna Holyan, Jeh C. Johnson, Richard Ledgett, David L. McDermott, James McRae, Amanda Murdie, Bernie Sanders, Jeremy Scahill, Kristan Stoddart, Jeremy Brooke Straughn, J. R. Swanegan, and Kali Wright-Smith
Politics and Technology in the Post-Truth Era Rowman & Littlefield
In this introductory volume, readers will learn about the vital role that the various Critical Infrastructure (CI) sectors play in America, in the context of homeland security. The protection, maintenance, and monitoring of these interdependent CI assets is a shared responsibility of governments, private sector owner/operators, first responders, and all those involved in homeland security and emergency management. As this foundational learning resource demonstrates, rapidly advancing technologies combined with exponential growth in demand on the aging infrastructure of America's power grid is setting the stage for a potentially catastrophic collapse that would paralyze each and every facet of civilian life and military operations. This meticulously researched primer will guide readers through the known world of power failures and cyber-attacks to the emerging threat from a High-altitude Electromagnetic Pulse (HEMP). A HEMP would cause cascading failures in the power grid, communications, water treatment facilities, oil refineries, pipelines, banking, supply chain management, food production, air traffic control, and all forms of transportation. Each chapter in America's Greatest Existential Threat (Vol. 1) begins with learning objectives and ends with a series of review questions to assess take-up of the chapter material. Similarly, subsequent volumes will explore HEMP and emerging issues in closer detail with current research and analysis now in development.
Transforming Government Organizations CRC Press
Since their creation, the European Union and the Council of Europe have worked to harmonise the justice systems of their member states. This project has been met with a series of challenges. European Criminal Law offers a compelling insight into the development and functions of European criminal law. It tracks the historical development of European criminal law, offering a detailed critical analysis of the criminal justice systems responsible for its implementation. While the rapid expansion and

transnationalisation of criminal law is a necessary response to the growing numbers of free movement of persons and goods, it has serious implications for the rights of European citizens and needs to be balanced with rights protections. With its close analysis of secondary legislation and reliance on a wide variety of original sources, this book provides a thorough understanding of European Criminal Law and the institutions involved.

The Unhackable Internet Elsevier

Prepare for success on the IAPP CIPP/US exam and further your career in privacy with this effective study guide - now includes a downloadable supplement to get you up to date on the 2022 CIPP exam! Information privacy has become a critical and central concern for small and large businesses across the United States. At the same time, the demand for talented professionals able to navigate the increasingly complex web of legislation and regulation regarding privacy continues to increase. Written from the ground up to prepare you for the United States version of the Certified Information Privacy Professional (CIPP) exam, Sybex's IAPP CIPP/US Certified Information Privacy Professional Study Guide also readies you for success in the rapidly growing privacy field. You'll efficiently and effectively prepare for the exam with online practice tests and flashcards as well as a digital glossary. The concise and easy-to-follow instruction contained in the IAPP/CIPP Study Guide covers every aspect of the CIPP/US exam, including the legal environment, regulatory enforcement, information management, private sector data collection, law enforcement and national security, workplace privacy and state privacy law, and international privacy regulation. Provides the information you need to gain a unique and sought-after certification that allows you to fully understand the privacy framework in the US Fully updated to prepare you to advise organizations on the current legal limits of public and private sector data collection and use Includes access to the Sybex online learning center, with chapter review questions, full-length practice exams, hundreds of electronic flashcards, and a glossary of key terms Perfect for anyone considering a career in privacy or preparing to tackle the challenging IAPP CIPP exam as the next step to advance an existing privacy role, the IAPP CIPP/US Certified Information Privacy Professional Study Guide offers you an invaluable head start for success on the exam and in your career as an in-demand privacy professional.

Building an Effective Security Program for Distributed Energy Resources and Systems John Wiley & Sons

Cyber security is concerned with the identification, avoidance, management and mitigation of risk in, or from, cyber space. The risk concerns harm and damage that might occur as the result of everything from individual carelessness, to organised criminality, to industrial and national security espionage and, at the extreme end of the scale, to disabling attacks against a country's critical national infrastructure. However, there is much more to cyber space than vulnerability, risk, and threat. Cyber space security is an issue of strategy, both commercial and technological, and whose breadth spans the international, regional, national, and personal. It is a matter of hazard and vulnerability, as much as an opportunity for social, economic and cultural growth. Consistent with this outlook, The Oxford Handbook of Cyber Security takes a comprehensive and rounded approach to the still evolving topic of cyber security. The structure of the Handbook is intended to

demonstrate how the scope of cyber security is beyond threat, vulnerability, and conflict and how it manifests on many levels of human interaction. An understanding of cyber security requires us to think not just in terms of policy and strategy, but also in terms of technology, economy, sociology, criminology, trade, and morality. Accordingly, contributors to the Handbook include experts in cyber security from around the world, offering a wide range of perspectives: former government officials, private sector executives, technologists, political scientists, strategists, lawyers, criminologists, ethicists, security consultants, and policy analysts.
US National Cybersecurity Createspace Independent Publishing Platform
The Cybersecurity Information Sharing Act of 2015 (CISA) encourages private companies to voluntarily share information about cyber threats with each other and the Government. CISA broadly authorizes the Federal Government to share Unclassified cyber threat indicators (CTI) and defensive measures (DM) technical data that indicates how networks have been attacked, and how such attacks have been successfully detected, prevented, or mitigated. The law accounts for its impacts on privacy and civil liberties by requiring that companies scrub personal information before sharing cyber threats. CISA also addresses the risks of misuse by the Federal Government or the private sector by only extending liability protections for companies and entities who participate in cybersecurity information sharing if that information sharing is done in accordance with CISA requirements. CISA is not a silver-bullet solution to cybersecurity challenges, but increasing the speed and quality of bilateral information flows of CTIs and DMs is essential for developing a holistic approach to cyber defense.
U.S. Critical Infrastructure John Wiley & Sons
Atmospheric reactive nitrogen (N) emissions, as an important component of global N cycle, have been significantly altered by anthropogenic activities, and consequently have had a global impact on air pollution and ecosystem services. Due to rapid agricultural, industrial, and urban development, China has been experiencing an increase in reactive N emissions and deposition since the late 1970s. Based on a literature review, this book summarizes recent research on: 1) atmospheric reactive N in China from a global perspective (Chapter 1); 2) atmospheric reactive N emissions, deposition and budget in China (Chapters 2-5); 3) the contribution of atmospheric reactive N to air pollution (e.g., haze, surface O3, and acid deposition) (Chapters 6-8); 4) the impacts of N deposition on sensitive ecosystems (e.g., forests, grasslands, deserts and lakes) (Chapters 9-12); and 5) the regulatory strategies for mitigation of atmospheric reactive N pollution from agricultural and non-agricultural sectors in China (Chapters 13-14). As such it offers graduate students, researchers, educators in agricultural, ecological and environmental sciences, and policy makers a glimpse of the environmental issues related to reactive N in China .
Mitigating Mass Violence and Managing Threats in Contemporary Society Page Publishing Inc
In a decade that has seen the rise of far-right extremism, Western countries still face myriad threats of mass violence, including terrorism. Of particular concern is the phenomenon of “lone-wolf terrorism,” whereby acts of political violence are committed by individuals who are operating independently of any

organized terrorist group, something which makes them inherently more difficult to identify in advance of an attack. Now there is a need for research that profiles these perpetrators, explores the incidents that occur, and analyzes the shifting changes in mass violence, technology, and terrorist behavior in modern times. Mitigating Mass Violence and Managing Threats in Contemporary Society explores the shifting definitions and implications of mass violence and covers important areas focused on the individuals who partake in these acts as well as weapon choice and the influence of weapon accessibility, how the attention-seeking behavior and promotion of violent actions is evolving, and how technology is used such as disseminating a manifesto prior to the incidents or using live streaming to broadcast incidents of mass violence as they transpire. The book also examines ways to prevent these incidents before they occur, which is a proven challenge with no single accurate profile for offenders, and whether perpetrators of mass violence share similar goals and motivations for their sprees, as well as commonalities in warning behaviors. This comprehensive research work is essential for law enforcement, military officials, defense specialists, national security experts, criminologists, psychologists, government officials, policymakers, lawmakers, professionals, practitioners, academicians, students, and researchers working in the fields of conflict analysis and resolution, crisis management, law enforcement, mental health, education, psychology, sociology, criminology, criminal justice, terrorism, and other social sciences.

ECCWS 2017 16th European Conference on Cyber Warfare and Security Springer Nature

Terrorism Inside America's Borders examines the history, trends, and different features of terrorism, and how the media, law enforcement, and other social institutions have responded to the violence. A variety of theoretical, methodological and analytical strategies are used to explore these issues.

Contextualizing Security John Wiley & Sons

On December 18, 2015, Congress passed and President Obama signed into law the Cybersecurity Act of 2015. Title I of the Cybersecurity Act, entitled the Cybersecurity Information Sharing Act (CISA or the Act), provides increased authority for cybersecurity information sharing between and among the private sector; state, local, tribal, and territorial governments; and the Federal Government. Section 105(a)(4) of the Act directed the Attorney General and the Secretary of the Department of Homeland Security (DHS) to jointly develop guidance to promote sharing of cyber threat indicators with federal entities pursuant to CISA no later than 60 days after CISA was enacted. That guidance was published on February 16, 2016, as required by statute. Unlike other guidance documents that CISA required the federal government to produce, the guidance for sharing cyber threat indicators with federal entities did not direct the publication of an updated version. However, feedback elicited from non-federal entities after the release of the original guidance on sharing with federal entities counseled in favor of releasing a revised version, as permitted under section 105(a)(4)(B)(iii). Accordingly, this document clarifies and updates the original guidance to further assist non-federal entities who elect to share cyber threat indicators with the Federal Government to do so in accordance with the Act. It also assists

non-federal entities to identify defensive measures and explains how to share them with federal entities as provided by CISA. Lastly, it describes the protections non-federal entities receive under CISA for sharing cyber threat indicators and defensive measures in accordance with the Act, including targeted liability protection and other statutory protections.

Oversight of the Cybersecurity Act of 2015 Routledge

As industries are rapidly being digitalized and information is being more heavily stored and transmitted online, the security of information has become a top priority in securing the use of online networks as a safe and effective platform. With the vast and diverse potential of artificial intelligence (AI) applications, it has become easier than ever to identify cyber vulnerabilities, potential threats, and the identification of solutions to these unique problems. The latest tools and technologies for AI applications have untapped potential that conventional systems and human security systems cannot meet, leading AI to be a frontrunner in the fight against malware, cyber-attacks, and various security issues. However, even with the tremendous progress AI has made within the sphere of security, it's important to understand the impacts, implications, and critical issues and challenges of AI applications along with the many benefits and emerging trends in this essential field of security-based research. Research Anthology on Artificial Intelligence Applications in Security seeks to address the fundamental advancements and technologies being used in AI applications for the security of digital data and information. The included chapters cover a wide range of topics related to AI in security stemming from the development and design of these applications, the latest tools and technologies, as well as the utilization of AI and what challenges and impacts have been discovered along the way. This resource work is a critical exploration of the latest research on security and an overview of how AI has impacted the field and will continue to advance as an essential tool for security, safety, and privacy online. This book is ideally intended for cyber security analysts, computer engineers, IT specialists, practitioners, stakeholders, researchers, academicians, and students interested in AI applications in the realm of security research.

Atmospheric Reactive Nitrogen in China IGI Global

China's change to a new model of growth, now called the 'new normal', was always going to be hard. Events over the past year show how hard it is. The attempts to moderate the extremes of high investment and low consumption, the correction of overcapacity in the heavy industries that were the mainstays of the old model of growth, the hauling in of the immense debt hangover from the fiscal and monetary expansion that pulled China out of the Great Crash of 2008 would all have been hard at any time. They are harder when changes in economic policy and structure coincide with stagnation in global trade and rising protectionist sentiment in developed countries, extraordinarily rapid demographic change and recognition of the urgency of easing the environmental damage from the old model. China's economy has slowed and there are worries that the authorities will not be able to contain the slowdown within preferred limits. This year's Update explores the challenge of the slowdown in growth and the change in economic structure. Leading experts on China's economy and environment review change within China's

new model of growth, and its interaction with ageing, environmental pressure, new patterns of urbanisation, and debt problems at different levels of government. It illuminates some new developments in China's economy, including the transformational potential of internet banking, and the dynamics of financial market instability. China's economic development since 1978 is full of exciting change, and this year's China Update is again the way to know it as it is happening.

Sardinia 2015. 15th International Waste Management and Landfill Symposium IGI Global

This volume explores the contemporary challenges to US national cybersecurity. Taking stock of the field, it features contributions by leading experts working at the intersection between academia and government and offers a unique overview of some of the latest debates about national cybersecurity. These contributions showcase the diversity of approaches and issues shaping contemporary understandings of cybersecurity in the West, such as deterrence and governance, cyber intelligence and big data, international cooperation, and public–private collaboration. The volume's main contribution lies in its effort to settle the field around three main themes exploring the international politics, concepts, and organization of contemporary cybersecurity from a US perspective. Related to these themes, this volume pinpoints three pressing challenges US decision makers and their allies currently face as they attempt to govern cyberspace: maintaining international order, solving conceptual puzzles to harness the modern information environment, and coordinating the efforts of diverse partners. The volume will be of much interest to students of cybersecurity, defense studies, strategic studies, security studies, and IR in general.

Cybersecurity Routledge

One of the Department of Homeland Security's (DHS) priorities is the protection of Federal employees and private citizens who work within and visit U.S. Government-owned or leased facilities. The Interagency Security Committee (ISC), chaired by DHS, consists of 53 Federal departments and agencies, has as its mission the development of security standards and best practices for nonmilitary Federal facilities in the United States. As Chair of the ISC, I am pleased to introduce the new ISC document titled The Risk Management Process: An Interagency Security Committee Standard (Standard). This ISC Standard defines the criteria and processes that those responsible for the security of a facility should use to determine its facility security level and provides an integrated, single source of physical security countermeasures for all nonmilitary Federal facilities. The Standard also provides guidance for customization of the countermeasures for Federal facilities.

Cybersecurity First Principles: A Reboot of Strategy and Tactics Cambridge Scholars Publishing

Solid Waste Landfilling: Concepts, Processes, Technology provides information on technologies that promote stabilization and minimize environmental impacts in landfills. As the main challenges in waste management are the reduction and proper treatment of waste and the appropriate use of waste streams, the book satisfies the needs of a modern landfill, covering waste pre-treatment, in situ treatment, long-term behavior, closure, aftercare, environmental impact and sustainability. It is written for practitioners who need specific information on landfill

construction and operation, but is also ideal for those concerned about the possible return of these sites to landscapes and their subsequent uses for future generations. Includes input by international contributors from a vast number of disciplines Provides worldwide approaches and technologies Showcases the interdisciplinary nature of the topic Focuses on sustainability, covering the lifecycle of landfills under the concept of minimizing environmental impact Presents knowledge of the legal framework and economic aspects of landfilling