Cyber Awareness Training Requirements

This book provides a comprehensive overview of the current and emerging challenges of cyber criminology, victimization and profiling. It is a compilation of the outcomes of the collaboration between researchers and practitioners in the cyber criminology field, IT law and security field. As Governments, corporations, security firms, and individuals look to tomorrow's cyber security challenges, this book provides a reference point for experts and forward-thinking analysts at a time when the debate over how we plan for the cyber-security of the future has become a major concern. Many criminological perspectives define crime in terms of social, cultural and material characteristics, and view crimes as taking place at a specific geographic location. This definition has allowed crime to be characterised, and crime prevention, mapping and measurement methods to be tailored to specific target audiences. However, this characterisation cannot be carried over to cybercrime, because the environment in which such crime is committed cannot be pinpointed to a geographical location, or distinctive social or cultural groups. Due to the rapid changes in technology, cyber criminals' behaviour has become dynamic, making it necessary to reclassify the typology being currently used. Essentially, cyber criminals' behaviour is evolving over time as they learn from their actions and others' experiences, and enhance their skills. The offender signature, which is a repetitive ritualistic behaviour that offenders often display at the crime scene, provides law enforcement agencies an appropriate profiling tool and offers investigators the opportunity to understand the motivations that perpetrate such crimes. This has helped researchers classify the type of perpetrator being sought. This book offers readers insights into the psychology of cyber criminals, and understanding and analysing their motives and the methodologies they adopt. With an understanding of these motives, researchers, governments and practitioners can take effective measures to tackle cybercrime and reduce victimization.

Rogue states and non-state actors have consistently launched cyber-attacks against Department of Defense (DoD) program offices, information systems, networks, and contractor facilities. In response to this, the DoD has made cybersecurity a requirement for all defense acquisition programs. Thus, according to the DoD, cybersecurity must be fully considered and implemented in all phases and aspects of a program's acquisition life cycle. To enforce this obligation on contracting organizations that do business with the DoD, Software Professionals (SPs) from the Defense Contract Management Agency (DCMA) have to be technically proficient to ascertain if the contractors' performance and management systems are in accordance with DoD's cybersecurity requirements. This study will examine, under the FY 18 Air Force Space Command research priority, "Cyber resilience, Cyber Assurance, and the Third Offset," how DCMA can assess the effectiveness of its Cybersecurity Awareness Training (CAT) and will provide recommendations on how to continually improve this training program. As a government agency, DCMA exists to ensure that defense contract requirements are correctly implemented by contractors. Consequently, by failing to address the current cybersecurity knowledge gap of DCMA's Software Professionals, this particular workforce will be unable to positively influence contractor performance, in this case, compliance with governmental cybersecurity requirements, which would ultimately result in mission failure for the Agency.

Over 1,600 total pages ... CONTENTS: AN OPEN SOURCE APPROACH TO SOCIAL MEDIA DATA GATHERING Open Source Intelligence – Doctrine's Neglected Child (Unclassified) Aggregation Techniques to Characterize Social Networks Open Source Intelligence (OSINT): Issues for Congress A BURNING NEED TO KNOW: THE USE OF OPEN SOURCE INTELLIGENCE IN THE FIRE SERVICE Balancing Social Media with Operations Security (OPSEC) in the 21st Century Sailing the Sea of OSINT in the Information Age Social Media: Valuable Tools in Today‘s Operational Environment ENHANCING A WEB CRAWLER WITH ARABIC SEARCH CAPABILITY UTILIZING SOCIAL MEDIA TO FURTHER THE NATIONWIDE SUSPICIOUS ACTIVITY REPORTING INITIATIVE THE WHO, WHAT AND HOW OF SOCIAL MEDIA EXPLOITATION FOR A COMBATANT COMMANDER Open Source Cybersecurity for the 21st Century UNAUTHORIZED DISCLOSURE: CAN BEHAVIORAL INDICATORS HELP PREDICT WHO WILL COMMIT UNAUTHORIZED DISCLOSURE OF CLASSIFIED NATIONAL SECURITY INFORMATION? ATP 2-22.9 Open-Source Intelligence NTTP 3-13.3M OPERATIONS SECURITY (OPSEC) FM 2-22.3 HUMAN INTELLIGENCE COLLECTOR OPERATIONS

This book constitutes the refereed proceedings of the 13th International Conference on Augmented Cognition, AC 2019, held as part of the 21st International Conference on Human-Computer Interaction, HCII 2019, in Orlando, FL, USA in July, 2019. The 1274 full papers and 209 posters presented at the HCII 2019 conferences were carefully reviewed and selected from 5029 submissions. The papers cover the entire field of human-computer interaction, addressing major advances in knowledge and effective use of computers in a variety of applications areas. The papers in this volume are organized in the following topical sections: cognitive modeling, perception, emotion and interaction; human cognition and behavior in complex tasks and environments; brain-computer interfaces and electroencephalography; and augmented learning.

At last, here is a textbook that covers the field of technology and public management in an informative and engaging style. Ever since the National Association of Schools of Public Affairs and Administration required greater infusion of technology into the curriculum, faculty and administrators have struggled with finding the right course materials designed specifically for the public administration environment. Technology is no longer the sole domain of an information technology office, as it has evolved into a growing set of complex tools that influence every area of government. To be effective, every public manager needs to be actively engaged in technology decisions. This textbook is designed for students of public administration at every level who need to know and understand how technology can be applied in today's public management workplace. The book explores the latest trends in public management, policy, and technology and focuses on best practices on governance issues. Finally, this book provides real-life examples about the need for policies and procedures to safeguard our technology infrastructure while providing greater openness, participation, and transparency. Technology and Public Management covers: How information system design relates to democratic theory How and where public policy and technology intersect Skills and tools that are useful in information management, information technology, and systems dedicated for the effective flow of information within organizations Understanding the role of e-government, m-government, and social media in today's society and in public organizations Possibilities and challenges associated with technology applications within public organizations How technology can be managed, through various governance models The latest technology trends and their potential impact on public administration.

If Sun Tzu were alive today, rather than in the fifth century BC, he would be on various stages and his strategies would be all the rage for individuals and organizations alike. In The Art of Cyber Conflict, Henry J. Sienkiewicz brings his strategic and practical experience to bear as he uses the timeless strategies from Sun Tzu's The Art of War in this highly relevant and exceptionally approachable guidebook. From a technology-independent perspective, Henry focuses on knowing and understanding cyber, the cyber environment, the cyber actors, and this constantly evolving form of modern conflict, while concurrently providing direct approaches to recognize, remediate, and resolve the underlying threats. "A thought-provoking and earnest view of the current cyber landscape from the classic construct of Sun Tzu. I anticipate it soon will be a key text for War College students as they explore cyber risk management strategies."

With the immense amount of data that is now available online, security concerns have been an issue from the start, and have grown as new technologies are increasingly integrated in data collection, storage, and transmission. Online cyber threats, cyber terrorism, hacking, and other cybercrimes have begun to take advantage of this information that can be easily accessed if not properly handled. New privacy and security measures have been developed to address this cause for concern and have become an essential area of research within the past few years and into the foreseeable future. The ways in which data is secured and privatized should be discussed in terms of the technologies being used, the methods and models for security that have been developed, and the ways in which risks can be detected, analyzed, and mitigated. The Research Anthology on Privatizing and Securing Data reveals the latest tools and technologies for privatizing and securing data across different technologies and industries. It takes a deeper dive into both risk detection and mitigation, including an analysis of cybercrimes and cyber threats, along with a sharper focus on the technologies and methods being actively implemented and utilized to secure data online. Highlighted topics include information governance and privacy, cybersecurity, data protection, challenges in big data, security threats, and more. This book is essential for data analysts, cybersecurity professionals, data scientists, security analysts, IT specialists, practitioners, researchers, academicians, and students interested in the latest trends and technologies for privatizing and securing data.

As society continues to heavily rely on software and databases, the risks for cyberattacks have increased rapidly. As the dependence on computers has become gradually widespread throughout communities and governments, there is a need for cybersecurity programs that can assist in protecting sizeable networks and significant amounts of data at once. Implementing overarching security policies for software systems is integral to protecting community-wide data from harmful attacks. Establishing Cyber Security Programs Through the Community Cyber Security Maturity Model (CCSMM) is an essential reference source that discusses methods in applying sustainable cybersecurity programs and policies within organizations, governments, and other communities. Featuring research on topics such as community engagement, incident planning methods, and information sharing, this book is ideally designed for cybersecurity professionals, security analysts, managers, researchers, policymakers, students, practitioners, and academicians seeking coverage on novel policies and programs in cybersecurity implementation.

Although many of the concepts included in staff cyber-security awareness training are universal, such training often must be tailored to address the policies and requirements of a particular organization. In addition, many forms of training fail because they are rote and do not require users to think about and apply security concepts. A flexible highly interactive video game, CyberCIEGE, is described as a security awareness tool that can support organizational security training objectives while engaging typical users in an engaging security adventure.

This book gathers the refereed proceedings of the Applied Informatics and Cybernetics in Intelligent Systems Section of the 9th Computer Science On-line Conference 2020 (CSOC 2020), held on-line in April 2020. Modern cybernetics and computer engineering in connection with intelligent systems are an essential aspect of ongoing research. This book addresses these topics, together with automation and control theory, cybernetic applications, and the latest research trends.

Business approaches in today’s society have become technologically-driven and highly-applicable within various professional fields. These business practices have transcended traditional boundaries with the implementation of internet technology, making it challenging for professionals outside of the business world to understand these advancements. Interdisciplinary research on business technology is required to better comprehend its innovations. Interdisciplinary Approaches to Digital Transformation and Innovation provides emerging research exploring the complex interconnections of technological business practices within society. This book will explore the practical and theoretical aspects of e-business technology within the fields of engineering, health, and social sciences. Featuring coverage on a broad range of topics such as data monetization, mobile commerce, and digital marketing, this book is ideally designed for researchers, managers, students, engineers, computer scientists, economists, technology designers, information specialists, and administrators seeking current research on the application of e-business technologies within multiple fields.

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.

This book constitutes the refereed post-conference proceedings of the Second International Workshop on Model-Driven Simulation and Training Environments for Cybersecurity, MSTEC 2020, held in Guildford, UK, in September 2020 in conjunction with the 24th European Symposium on Research in Computer Security, ESORICS 2020. The conference was held virtually due to the COVID-19 pandemic. The MSTEC Workshop received 20 submissions from which 10 full papers were selected for presentation. The papers are grouped in thematically on: cyber security training modelling; serious games; emulation & simulation studies; attacks; security policies.

Conferences Proceedings of 20th European Conference on Cyber Warfare and Security

With the continued progression of technologies such as mobile computing and the internet of things (IoT), cybersecurity has swiftly risen to a prominent field of global interest. This has led to cyberattacks and cybercrime becoming much more sophisticated to a point where cybersecurity can no longer be the exclusive responsibility of an organization's information technology (IT) unit. Cyber warfare is becoming a national issue and causing various governments to reevaluate the current defense strategies they have in place.

Cyber Security Auditing, Assurance, and Awareness Through CSAM and CATRAM provides emerging research exploring the practical aspects of reassessing current cybersecurity measures within organizations and international governments and improving upon them using audit and awareness training models, specifically the Cybersecurity Audit Model (CSAM) and the Cybersecurity Awareness Training Model (CATRAM). The book presents multi-case studies on the development and validation of these models and frameworks and analyzes their implementation and ability to sustain and audit national cybersecurity strategies. Featuring coverage on a broad range of topics such as forensic analysis, digital evidence, and incident management, this book is ideally designed for researchers, developers, policymakers, government officials, strategists, security professionals, educators, security analysts, auditors, and students seeking current research on developing training models within cybersecurity management and awareness.

This book constitutes the refereed proceedings of the 12th SIGSAND/PLAIS EuroSymposium 2019 held in Gdansk, Poland, on September 19, 2019. The objective of the EuroSymposium on Systems Analysis and Design is to promote and develop high quality research on all issues related to information systems (IS) and in particular in systems analysis and design (SAND). The 12 papers presented in this volume were carefully reviewed and selected from 32 submissions. They were organized in topical sections named: information systems in business; health informatics and life-long-learning; IT security; agile methods and software engineering.

This book offers a practice-oriented guide to developing an effective cybersecurity culture in organizations. It provides a psychosocial perspective on common cyberthreats affecting organizations, and presents practical solutions for leveraging employees' attitudes and behaviours in order to improve security. Cybersecurity, as well as the solutions used to achieve it, has largely been associated with technologies. In contrast, this book argues that cybersecurity begins with improving the connections between people and digital technologies. By presenting a comprehensive analysis of the current cybersecurity landscape, the author discusses, based on literature and her personal experience, human weaknesses in relation to security and the advantages of pursuing a holistic approach to cybersecurity, and suggests how to develop cybersecurity culture in practice. Organizations can improve their cyber resilience by adequately training their staff. Accordingly, the book also describes a set of training methods and tools. Further, ongoing education programmes and effective communication within organizations are considered, showing that they can become key drivers for successful cybersecurity awareness initiatives. When properly trained and actively involved, human beings can become the true first line of defence for every organization.

Research Anthology on Artificial Intelligence Applications in SecurityIGI Global

Through the rise of big data and the internet of things, terrorist organizations have been freed from geographic and logistical confines and now have more power than ever before to strike the average citizen directly at home. This, coupled with the inherently asymmetrical nature of cyberwarfare, which grants great advantage to the attacker, has created an unprecedented national security risk that both governments and their citizens are woefully ill-prepared to face. Examining cyber warfare and terrorism through a critical and academic perspective can lead to a better understanding of its foundations and implications. Cyber Warfare and Terrorism: Concepts, Methodologies, Tools, and Applications is an essential reference for the latest research on the utilization of online tools by terrorist organizations to communicate with and recruit potential extremists and examines effective countermeasures employed by law enforcement agencies to defend against such threats. Highlighting a range of topics such as cyber threats, digital intelligence, and counterterrorism, this multi-volume book is ideally designed for law enforcement, government officials, lawmakers, security analysts, IT specialists, software developers, intelligence and security practitioners, students, educators, and researchers.

Cybersecurity is vital for all businesses, regardless of sector. With constant threats and potential online dangers, businesses must remain aware of the current research and information available to them in order to protect themselves and their employees. Maintaining tight cybersecurity can be difficult for businesses as there are so many moving parts to contend with, but remaining vigilant and having protective measures and training in place is essential for a successful company. The Research Anthology on Business Aspects of Cybersecurity considers all emerging aspects of cybersecurity in the business sector including frameworks, models, best practices, and emerging areas of interest. This comprehensive reference source is split into three sections with the first discussing audits and risk assessments that businesses can conduct to ensure the security of their systems. The second section covers training and awareness initiatives for staff that promotes a security culture. The final section discusses software and systems that can be used to secure and manage cybersecurity threats. Covering topics such as audit models, security behavior, and insider threats, it is ideal for businesses, business professionals, managers, security analysts, IT specialists, executives, academicians, researchers, computer engineers, graduate students, and practitioners.

These proceedings represent the work of researchers participating in the 13th International Conference on Cyber Warfare and Security (ICCWS 2018) which is being hosted this year by the National Defense University in Washington DC, USA on 8-9 March 2018.

Although many of the concepts included in cyber security awareness training are universal, such training often must be tailored to address the policies and requirements of a particular organization. In addition, many forms of training fail because they are rote and do not require users to think about and apply security concepts. A flexible, highly interactive video game, CyberCIEGE, is described as a security awareness tool that can support organizational security training objectives while engaging typical users in an engaging security adventure. The game is now being successfully utilized for information assurance education and training by a variety of organizations. Preliminary results indicate the game can also be an effective addition to basic information awareness training programs for general computer users "e.g., annual awareness training."

This comprehensive Research Handbook provides an in-depth analysis of the different financial law approaches, legal systems and trends throughout Asia. It considers how reforms following the crises have been critical for the development and growth of the region and explores a broad range of post-crisis financial regulatory issues. This timely book also examines how inconsistent and divergent approaches to financial market regulation are curtailing the region's potential.

This book covers the security and safety of CBRNE assets and management, and illustrates which risks may emerge and how to counter them through an enhanced risk management approach. It also tackles the CBRNE-Cyber threats, their risk mitigation measures and the relevance of raising awareness and education enforcing a CBRNE-Cy security culture. The authors present international instruments and legislation to deal with these threats, for instance the UNSCR1540. The authors address a multitude of stakeholders, and have a multidisciplinary nature dealing with cross-cutting areas like the convergence of biological and chemical, the development of edging technologies, and in the cyber domain, the impelling risks due to the use of malwares against critical subsystems of CBRN facilities. Examples are provided in this book. Academicians, diplomats, technicians and engineers working in the chemical, biological, radiological, nuclear, explosive and cyber fields will find this book valuable as a reference. Students studying in these related fields will also find this book useful as a reference.

"This book evaluates the implementation and validation of the Cyber Security Audit Model (CSAM), along with the delivery and inception of the Cybersecurity Awareness TRAining Model (CATRAM) to train personnel on cyber security awareness matter"--

The Los Alamos National Laboratory (LANL), which is overseen by the National Nuclear Security Admin. (NNSA), has experienced a number of security lapses in controlling classified information stored on its classified computer network. This report: (1) assesses the effectiveness of security controls LANL used to protect information on its classified network; (2) assesses whether LANL had fully implemented an information security program to ensure that security controls were effectively established and maintained for its classified network; and (3) identifies the expenditures used to operate and support its classified network from FY 2001 through 2008. Charts and tables.

What framework can be designed to gamify cyber security awareness trainings? Have cyber security awareness needs been identified for the critical services? What metrics do you use to evaluate cyber security awareness across your organization? What is current attitude towards cyber security Awareness Training? Which does your organization require to complete cyber security awareness training? This best-selling Cyber Security Awareness self-assessment will make you the assured Cyber Security Awareness domain leader by revealing just what you need to know to be fluent and ready for any Cyber Security Awareness challenge. How do I reduce the effort in the Cyber Security Awareness work to be done to get problems solved? How can I ensure that plans of action include every Cyber Security Awareness task and that every Cyber Security Awareness outcome is in place? How will I save time investigating strategic and tactical options and ensuring Cyber Security Awareness costs are low? How can I deliver tailored Cyber Security Awareness advice instantly with structured going-forward plans? There's no better guide through these mind-expanding questions than acclaimed best-selling author Gerard Blokdyk. Blokdyk ensures all Cyber Security Awareness essentials are covered, from every angle: the Cyber Security Awareness self-assessment shows succinctly and clearly that what needs to be clarified to organize the required activities and processes so that Cyber Security Awareness outcomes are achieved. Contains extensive criteria grounded in past and current successful projects and activities by experienced Cyber Security Awareness practitioners. Their mastery, combined with the easy elegance of the self-assessment, provides its superior value to you in knowing how to ensure the outcome of any efforts in Cyber Security Awareness are maximized with professional results. Your purchase includes access details to the Cyber Security Awareness self-assessment dashboard download which gives you your dynamically prioritized projects-ready tool and shows you exactly what to do next. Your exclusive instant access details can be found in your book. You will receive the following contents with New and Updated specific criteria: - The latest quick edition of the book in PDF - The latest complete edition of the book in PDF, which criteria correspond to the criteria in... - The Self-Assessment Excel Dashboard - Example pre-filled Self-Assessment Excel Dashboard to get familiar with results generation - In-depth and specific Cyber Security Awareness Checklists - Project management checklists and templates to assist with implementation INCLUDES LIFETIME SELF ASSESSMENT UPDATES Every self assessment comes with Lifetime Updates and Lifetime Free Updated Books. Lifetime Updates is an industry-first feature which allows you to receive verified self assessment updates, ensuring you always have the most accurate information at your fingertips.

Based on related courses and research on the cyber environment in Europe, the United States, and Asia, Cyberspace and Cybersecurity supplies complete coverage of cyberspace and cybersecurity. It not only emphasizes technologies but also pays close attention to human factors and organizational perspectives.Detailing guidelines for quantifying and me

For any organization to be successful, it must operate in such a manner that knowledge and information, human resources, and technology are continually taken into consideration and managed effectively. Business concepts are always present regardless of the field or industry – in education, government, healthcare, not-for-profit, engineering, hospitality/tourism, among others. Maintaining organizational awareness and a strategic frame of mind is critical to meeting goals, gaining competitive advantage, and ultimately ensuring sustainability. The Encyclopedia of Organizational Knowledge, Administration, and Technology is an inaugural five-volume publication that offers 193 completely new and previously unpublished articles authored by leading experts on the latest concepts, issues, challenges, innovations, and opportunities covering all aspects of modern organizations. Moreover, it is comprised of content that highlights major breakthroughs, discoveries, and authoritative research results as they pertain to all aspects of organizational growth and development including methodologies that can help companies thrive and analytical tools that assess an organization’s internal health and performance. Insights are offered in key topics such as organizational structure, strategic leadership, information technology management, and business analytics, among others. The knowledge compiled in this publication is designed for entrepreneurs, managers, executives, investors, economic analysts, computer engineers, software programmers, human resource departments, and other industry professionals seeking to understand the latest tools to emerge from this field and who are looking to incorporate them in their practice. Additionally, academicians, researchers, and students in fields that include but are not limited to business, management science, organizational development, entrepreneurship, sociology, corporate psychology, computer science, and information technology will benefit from the research compiled within this publication.

The essential guide for today's savvy controllers Today's controllers are in leadership roles that put them in the unique position to see across all aspects of the operations they support. The Master Guide to Controllers' Best Practices, Second Edition has been revised and updated to provide controllers with the information they need to successfully monitor their organizations' internal control environments and offer direction and consultation on internal control issues. In addition, the authors include guidance to help controllers carryout their responsibilities to ensure that all financial accounts are reviewed for reasonableness and are reconciled to supporting transactions, as well as performing asset verification. Comprehensive in scope the book contains the best practices for controllers and: Reveals how to set the right tone within an organization and foster an ethical climate Includes information on risk management, internal controls, and fraud prevention Highlights the IT security controls with the key components of successful governance Examines the crucial role of the controller in corporate compliance and much more The Master Guide to Controllers' Best Practices should be on the bookshelf of every controller who wants to ensure the well-being of their organization.

This book constitutes the proceedings of the 6th International Conference on Electronic Voting, E-Vote-ID 2021, held online -due to COVID -19- in Bregenz, Austria, in October 2021. The 14 full papers presented were carefully reviewed and selected from 55 submissions. The conference collected the most relevant debates on the development of Electronic Voting, from aspects relating to security and usability through to practical experiences and applications of voting systems, as well as legal, social or political aspects.

This book constitutes the revised selected papers of the 4th International Conference on Information Systems Security and Privacy, ICISSP 2018, held in Funchal - Madeira, Portugal, in January 2018. The 15 full papers presented were carefully reviewed and selected from a total of 71 submissions. They are dealing with topics such as data and software security; privacy and confidentiality; mobile systems security; biometric authentication; information systems security and privacy; authentication, privacy and security models; data mining and knowledge discovery; phishing; security architecture and design analysis; security testing; vulnerability analysis and countermeasures; web applications and services.

This book constitutes the refereed proceedings of 14th International Conference on Augmented Cognition, AC 2020, held as part of the 22nd International Conference on Human-Computer Interaction, HCII 2020, in July 2020. The conference was planned to be held in Copenhagen, Denmark, but had to change to a virtual conference mode due to the COVID-19 pandemic. From a total of 6326 submissions, a total of 1439 papers and 238 posters has been accepted for publication in the HCII 2020 proceedings. The 21 papers presented in this volume were organized in topical sections as follows: cognitive modeling, perception, emotion and interaction; electroencephalography and BCI; and AI and augmented cognition.

This book focuses on the vulnerabilities of state and local services to cyber-threats and suggests possible protective action that might be taken against such threats. Cyber-threats to U.S. critical infrastructure are of growing concern to policymakers, managers and consumers. Information and communications technology (ICT) is ubiquitous and many ICT devices and other components are interdependent; therefore, disruption of one component may have a negative, cascading effect on others. Cyber-attacks might include denial of service, theft or manipulation of data. Damage to critical infrastructure through a cyber-based attack could have a significant impact on the national security, the economy, and the livelihood and safety of many individual citizens. Traditionally cyber security has generally been viewed as being focused on higher level threats such as those against the internet or the Federal government. Little attention has been paid to cyber-security at the state and local level. However, these governmental units play a critical role in providing services to local residents and consequently are highly vulnerable to cyber-threats. The failure of these services, such as waste water collection and water supply, transportation, public safety, utility services, and communication services, would pose a great threat to the public. Featuring contributions from leading experts in the field, this volume is intended for state and local government officials and managers, state and Federal officials, academics, and public policy specialists.

This volume constitutes the refereed proceedings of the 7th International Conference on Virtual, Augmented and Mixed Reality, VAMR 2015, held as part of the 17th International Conference on Human-Computer Interaction, HCI 2015, held in Los Angeles, CA, USA, in August 2015. The total of 1462 papers and 246 posters presented at the HCII 2015 conferences was carefully reviewed and selected from 4843 submissions. These papers address the latest research and development efforts and highlight the human aspects of design and use of computing systems. The papers thoroughly cover the entire field of human-computer interaction, addressing major advances in knowledge and effective use of computers in a variety of application areas. The 54 papers included in this volume are organized in the following topical sections: user experience in virtual and augmented environments; developing virtual and augmented environments; agents and robots in virtual environments; VR for learning and training; VR in Health and Culture; industrial and military applications.