1. Record Nr. UNINA9910459843303321

Autore	Mehan Julie E.
Titolo	CyberWar, CyberTerror, CyberCrime and CyberActivism : an in-depth guide to the role of standards in cybersecurity environment / / Dr. Julie E. Mehan
Pubbl/distr/stampa	[Cambridge, England] : , : IT Governance Publishing, , 2014 ©2014
ISBN	1-84928-572-1
Edizione	[2nd ed.]
Descrizione fisica	1 online resource (352 p.)
Disciplina	658.478
Soggetti	Computer crimes - Prevention Cyberterrorism - Prevention Computer networks - Security measures - Standards Electronic books.
Lingua di pubblicazione	Inglese
Formato	Materiale a stampa
Livello bibliografico	Monografia
Note generali	Includes index.
Nota di contenuto	Cover; Title; Copyright; Preface; About the Author; Contents; Introduction; Chapter 1: Technology Is a Double-Edged Sword; From the printing press to the information age; The 'dark side of high tech'; Chapter 2: Cyber Attack: It's A Dangerous World for Information Systems; Cyberwar; Cyberterror; Cybercrime; CyberEspionage (and Information Exfiltration) - It's midnight; do you know where your data is?; Social Media - an opportunity and a challenge; Supply Chain (In-) security; The blended threat; The asymmetric effects of cyber attacks; Porous perimeters, compromisable software - or both? If we know about the vulnerabilities, why are exploits still successful? Chapter 3: The Human Factor: The Underrated Threat; Are people the problem?; Who are the attackers?; Most likely forms of attack; Sometimes it's just human error; People can also be the solution!; Chapter 4: Transition from an Environment of 'FUD' to a Standards-Based Environment; Chapter 5: Establishing a Culture of Cybersecurity; Chapter 6: Increasing Internationalism: Governance, Laws, and Ethics; Information globalism equals increased exposure; Following the lead of good governance; The proliferation of laws

Ethics in an information society and a minimum standard of due care in cybersecurityCybersecurity and privacy; Chapter 7: Standards: What Are They and Why Should We Care?; What are standards?; How and by whom are standards developed?; The importance of terminology; Standards-based process improvement; Focus on consensus-based cybersecurity; Standards provide a level playing-field for co-ordination and co-operation; If standards are so good, then why is it so hard?; Chapter 8: From Reaction to Proaction: Applying Standards in an Environment of Change and Danger
Moving beyond compliance and reactionA quick look at relevant standards; Take four steps forward; The future is 'ROSI'; Making the case for cybersecurity assurance; Chapter 9: Conclusion: Where Do We Go From Here?; Cybersecurity program roadmap; Appendix 1: Gap Analysis Areas of Interest; Appendix 2: Standards Crosswalk; Definitions; Acronyms; Index; A; B; C; D; E; F; G; H; I; J; K; L; M; N; O; P; Q; R; S; T; U; V; W; X; Y; ITG Resources

Sommario/riassunto

Successful cyberattacks can damage your organisation, no matter who is behind them The goals of the cyberterrorist, the cybercriminal, the cyberactivist and the state-sponsored hacker may not be the same – but the outcomes can be equally devastating. Each can cause serious challenges for your organisation, ranging from information theft and disruption of normal operations to loss of reputation or credibility. Cyber security is much more than technology Many books on cybersecurity focus on technical responses to these threats. As important as this is, human fallibility and other known vulnerabilities will still allow hackers to easily break into a system that has not taken account of these factors. CyberWar, CyberTerror, CyberCrime and CyberActivism encourages cybersecurity professionals to take a wider view of what cybersecurity means, and to make the most of international standards and best practices to create a culture of cybersecurity awareness within their organizations that complements their technology-based defences. A cyber aware workforce equals better security This second edition takes a deep look at the changing threats in the cyber landscape, and includes an updated body of knowledge that describes how to acquire, develop, and sustain a secure information environment that goes beyond technology. This enables you to move towards a cyber aware organisational culture that is more robust and better able to deal with a wider range of threats. Related references, as well as recommendations for additional reading, are included at the end of each chapter making this a valuable resource for trainers, researchers and cybersecurity practitioners. Order this book today and see how international standards can boost your cyber defences About the author Dr Julie Mehan is the Founder and President of JEMStone Strategies and a Principal in a strategic consulting firm in the State of Virginia. She has delivered cybersecurity and related privacy services to senior commercial, department of defence and federal government clients working in Italy, Australia, Canada, Belgium, and the United States. Dr Mehan is also an Associate Professor at the University of Maryland University College, specializing in courses in Cybersecurity, Cyberterror, IT in Organizations and Ethics in an Internet Society.