1.	Record Nr.	UNINA9910825352603321
	Titolo	Cyber security policy guidebook / / Jennifer L. Bayuk ... [et al.]
	Pubbl/distr/stampa	Hoboken, N.J., : Wiley, c2012
	ISBN	9781299189324 1299189326 9781118241325 1118241320 9781118241530 1118241533 9781118241486 1118241487
	Edizione	[First edition]
	Descrizione fisica	1 online resource (xvi, 270 pages) : illustrations
	Classificazione	COM053000
	Altri autori (Persone)	BayukJennifer L
	Disciplina	005.8
	Soggetti	Information technology - Government policy Computer security - Government policy Data protection - Government policy
	Lingua di pubblicazione	Inglese
	Formato	Materiale a stampa
	Livello bibliografico	Monografia
	Note generali	Description based upon print version of record.
	Nota di bibliografia	Includes bibliographical references (p. 255-265) and index.
	Nota di contenuto	Cyber Security Policy Guidebook; Contents; Foreword; Preface; Acknowledgments; 1: Introduction; 1.1 What Is Cyber Security?; 1.2 What Is Cyber Security Policy?; 1.3 Domains of Cyber Security Policy; 1.3.1 Laws and Regulations; 1.3.2 Enterprise Policy; 1.3.3 Technology Operations; 1.3.4 Technology Configuration; 1.4 Strategy versus Policy; 2: Cyber Security Evolution; 2.1 Productivity; 2.2 Internet; 2.3 e-Commerce; 2.4 Countermeasures; 2.5 Challenges; 3: Cyber Security Objectives; 3.1 Cyber Security Metrics; 3.2 Security Management Goals; 3.3 Counting Vulnerabilities; 3.4 Security Frameworks 3.4.1 e-Commerce Systems3.4.2 Industrial Control Systems; 3.4.3 Personal Mobile Devices; 3.5 Security Policy Objectives; 4: Guidance for Decision Makers; 4.1 Tone at the Top; 4.2 Policy as a Project; 4.3 Cyber Security Management; 4.3.1 Arriving at Goals; 4.3.2 Cyber Security Documentation; 4.4 Using the Catalog; 5: The Catalog Approach; 5.1

Catalog Format; 5.2 Cyber Security Policy Taxonomy; 6: Cyber Security Policy Catalog; 6.1 Cyber Governance Issues; 6.1.1 Net Neutrality; 6.1.2 Internet Names and Numbers; 6.1.3 Copyrights and Trademarks; 6.1.4 Email and Messaging; 6.2 Cyber User Issues
6.2.1 Malvertising6.2.2 Impersonation; 6.2.3 Appropriate Use; 6.2.4 Cyber Crime; 6.2.5 Geolocation; 6.2.6 Privacy; 6.3 Cyber Conflict Issues; 6.3.1 Intellectual Property Theft; 6.3.2 Cyber Espionage; 6.3.3 Cyber Sabotage; 6.3.4 Cyber Warfare; 6.4 Cyber Management Issues; 6.4.1 Fiduciary Responsibility; 6.4.2 Risk Management; 6.4.3 Professional Certification; 6.4.4 Supply Chain; 6.4.5 Security Principles; 6.4.6 Research and Development; 6.5 Cyber Infrastructure Issues; 6.5.1 Banking and Finance; 6.5.2 Health Care; 6.5.3 Industrial Control Systems
7: One Government's Approach to Cyber Security Policy7.1 U.S. Federal Cyber Security Strategy; 7.2 A Brief History of Cyber Security Public Policy Development in the U.S. Federal Government; 7.2.1 The Bombing of New York's World Trade Center on February 26, 1993; 7.2.2 Cyber Attacks against the United States Air Force, March-May 1994: Targeting the Pentagon; 7.2.3 The Citibank Caper, June-October, 1994: How to Catch a Hacker; 7.2.4 Murrah Federal Building, Oklahoma City-April 19, 1995: Major Terrorism Events and Their U.S. Outcomes
7.2.5 President's Commission on Critical Infrastructure Protection-19967.2.6 Presidential Decision Directive 63-1998; 7.2.7 National Infrastructure Protection Center (NIPC) and ISACs-1998; 7.2.8 Eligible Receiver-1997; 7.2.9 Solar Sunrise-1998; 7.2.10 Joint Task Force-Computer Network Defense (JTF-CND)-1998; 7.2.11 Terrorist Attacks against the United States-September 11, 2001 Effects of Catastrophic Events on Transportation System Management and Operations; 7.2.12 U.S. Government Response to the September 11, 2001 Terrorist Attacks; 7.2.13 Homeland Security Presidential Directives
7.2.14 National Strategies

Sommario/riassunto

"Drawing upon a wealth of experience from academia, industry, and government service, this book details and dissects current organizational cybersecurity policy issues on a global scale. Using simple language, it includes a thorough description of each issue, lists pros and cons, documents policy alternatives for the sake of clarity with respect to policy alone, and dives into organizational implementation issues. It also equips the reader with descriptions of the impact of specific policy choices, both positive and negative. This book gives students, scholars, and technical decision-makers the necessary knowledge of cybersecurity policy in order to make more informed decisions"--Provided by publisher.