1. Record Nr. UNINA9910786630203321

Autore	Ulsch N. MacDonnell <1951->
Titolo	Cyber threat! : how to manage the growing risk of cyber attacks / / N. MacDonnell Ulsch
Pubbl/distr/stampa	Hoboken, New Jersey : , : Wiley, , 2014 ©2014
ISBN	1-118-93595-0 1-118-91502-X 1-118-93596-9
Edizione	[1st edition]
Descrizione fisica	1 online resource (227 p.)
Collana	Wiley Corporate F&A
Classificazione	BUS083000
Disciplina	658.4/78
Soggetti	Corporations - Security measures Business enterprises - Computer networks - Security measures Computer crimes - Prevention Computer security Computer networks - Security measures
Lingua di pubblicazione	Inglese
Formato	Materiale a stampa
Livello bibliografico	Monografia
Note generali	Includes index.
Nota di bibliografia	Includes bibliographical references and index.
Nota di contenuto	Cyber Threat!: How to Manage the Growing Risk of Cyber Attacks; Contents; Foreword; Preface; Acknowledgments; Introduction: What Every Current and Future Senior Executive Must Know about the Cyber Threat: A Perfect Digital Storm Is Forming; What Factors Create a Perfect Storm?; Industry Vulnerability; Threat Intensification; Inadequate Government Preparedness; Low Level of Awareness; Inadequate Risk Assessments; Offshoring of Data; Insider Threat; Denial of Vulnerability; Increasingly Sophisticated Attacks; Mobile Devices at Higher Risk; Sometimes Security Just Doesn't Take Hold It Wasn't Always Like ThisWithout a Bang; A Board Issue; The Cyber Frankenstein Cometh; Defining Success; Notes; Part I: The Cyber Threat to the Corporate Brand: How It Will Impact Your Company; Chapter 1: The Rise of Cyber Organized Crime and Its Global Impact; Is Nothing Sacred?; The Liberty Reserve Case: Money Laundering in the Digital Age; The Corruption Factor; Information Threat, Physical Threat; Notes; Chapter 2: The Emergence of the Cyber Nation-State and Technology

Espionage: Red China Rising and Its Global Cyber Theft Strategy; A Case of Cyber Espionage Conspiracy?
According to the Select Committee . . .Notes; Chapter 3: Cyber Al Qaeda Poses a Threat to Critical Infrastructure; A Disabled America; A New Age: Inspiring Terrorists and Terrorism; A Call Heard Vaguely; Attack upon Attack, No Peace in Sight; Notes; Part II: Corporate Vulnerabilitiesin the Digital Society: Prepare to Defend Yourself and Your Brand; Chapter 4: What Is the True Cost of a Cyber Attack?; Cyber Attack Detection Sometimes Takes Years; One of the First Questions: "How Much Will This Cost?"; A Few Common Cost Factors; What about Unreported Breaches?
Cyber Attacks Result in a Wider Impact: The CommunityNotes; Chapter 5: U.S. Cyber Public Policy: Don't Rely on It to Protect the Brand; No Guarantees with This Executive Order; Government-Industry Cooperation: No Silver Bullet; The Challenge of Defining Cyber Public Policy; Cold War II: The Cyber Chapter; Is There a Silver Lining in an Attack?; Notes; Chapter 6: Four Trends Driving Cyber Breaches and Increasing Corporate Risk: Technological, Cultural, Economic, and Geopolitical Shifts; Technology Trend; Loss of Situational Awareness: Distraction; Culture; Technology Is a Double-Edged Sword NotesChapter 7: Social Media and Digital Protest; Social Media: A Tool for Disruption, a Model for Change; The Hacker Group Anonymous; Anonymous Is an "Anti" Outfit of Malcontents; In Reckless Move, Anonymous Targeted Law Enforcement; Anonymous: Making All Information Free for All; In Pursuit of the Anonymous Definition of Civil Liberties; Anarchaos: In the Image of Anonymous; Notes; Part III: Protecting the Brand: Actions Executive Management Must Take to Reduce Cyber Risk; Chapter 8: Managing the Brand When the Worst Occurs; Be Prepared; 1. Initiation
2. Discovery and Forensic Evidence Capture

Sommario/riassunto

"Conquering cyber attacks requires a multi-sector, multi-modal approachCyber Threat! How to Manage the Growing Risk of Cyber Attacks is an in-depth examination of the very real cyber security risks facing all facets of government and industry, and the various factors that must align to maintain information integrity. Written by one of the nation's most highly respected cyber risk analysts, the book describes how businesses and government agencies must protect their most valuable assets to avoid potentially catastrophic consequences. Much more than just cyber security, the necessary solutions require government and industry to work cooperatively and intelligently. This resource reveals the extent of the problem, and provides a plan to change course and better manage and protect critical information. Recent news surrounding cyber hacking operations show how intellectual property theft is now a matter of national security, as well as economic and commercial security. Consequences are far-reaching, and can have enormous effects on national economies and international relations. Aggressive cyber forces in China, Russia, Eastern Europe and elsewhere, the rise of global organized criminal networks, and inattention to vulnerabilities throughout critical infrastructures converge to represent an abundantly clear threat. Managing the threat and keeping information safe is now a top priority for global businesses and government agencies. Cyber Threat! breaks the issue down into real terms, and proposes an approach to effective defense. Topics include: The information at risk The true extent of the threat The potential consequences across sectors The multifaceted approach to defense The growing cyber threat is fundamentally changing the nation's economic, diplomatic, military, and intelligence operations, and will extend into future technological, scientific, and

geopolitical influence. The only effective solution will be expansive and complex, encompassing every facet of government and industry. Cyber Threat! details the situation at hand, and provides the information that can help keep the nation safe"--

"Cyber Threat! is an in-depth examination of the very real risks facing all facets of government and industry, and the various factors that must align to maintain information integrity. The book describes how businesses and government agencies must protect their most valuable assets to avoid potentially catastrophic consequences"--