1.

Record Nr.	UNINA9910280812803321
Autore	Harkins Malcolm
Titolo	Managing risk and information security : protect to enable / / Malcolm W Harkins
Pubbl/distr/stampa	[Place of publication not identified] : , : Apress Open, , [2016] New York, NY : , : Distributed to the book trade worldwide by Springer Science+Business Media New York ©2016
ISBN	1-4842-1456-0
Edizione	[Second edition.]
Descrizione fisica	1 online resource (1 volume) : illustrations
Disciplina	005.8
Soggetti	Computer security Electronic information resources - Access control
Lingua di pubblicazione	Inglese
Formato	Materiale a stampa
Livello bibliografico	Monografia
Nota di bibliografia	Includes bibliographical references and index.
Nota di contenuto	Intro -- Contents at a Glance -- Contents -- Foreword -- Praise for the second edition of Managing Risk and Information Security -- About the Author -- Acknowledgments -- Preface -- Chapter 1: Introduction -- Protect to Enable® -- Building Trust -- Keeping the Company Legal: The Regulatory Flood -- Privacy: Protecting Personal Information -- Personalization vs. Privacy -- Financial Regulations -- E-Discovery -- Expanding Scope of Regulation -- The Rapid Proliferation of Information, Devices, and Things -- The Changing Threat Landscape -- Stealthy Malware -- Nine Irrefutable Laws of Information Risk -- A New Approach to Managing Risk -- Chapter 2: The Misperception of Risk -- The Subjectivity of Risk Perception -- How Employees Misperceive Risk -- The Lure of the Shiny Bauble -- How Security Professionals Misperceive Risk -- Security and Privacy -- How Decision Makers Misperceive Risk -- How to Mitigate the Misperception of Risk -- Uncovering New Perspectives During Risk Assessments -- Communication Is Essential -- Building Credibility -- Chapter 3: Governance and Internal Partnerships: How to Sense, Interpret, and Act on Risk -- Information Risk Governance -- Finding the Right Governance Structure -- Building Internal Partnerships -- Legal -- Privacy -- Litigation -- Intellectual Property -- Contracts -- Financial

Compliance -- Legal Specialists Within Business Groups -- Human Resources -- Setting Employee Expectations in Security Policies -- Employee Communications -- Investigations -- Finance -- Sarbanes-Oxley Compliance -- Working with Business Groups -- Internal Audit -- Corporate Risk Management -- Privacy -- Corporate Security -- Business Group Managers -- Conclusion -- Chapter 4: External Partnerships: The Power of Sharing Information -- The Value of External Partnerships -- External Partnerships: Types and Tiers -- 1:1 Partnerships.

Communities -- Community Characteristics -- Community Goals -- Sharing Information about Threats and Vulnerabilities -- Sharing Best Practices and Benchmarking -- Influencing Regulations and Standards -- Corporate Citizenship -- Conclusion -- Chapter 5: People Are the Perimeter -- The Shifting Perimeter -- Compliance or Commitment? -- Examining the Risks -- Adjusting Behavior -- A Model for Improving Security Awareness -- Broadening the Awareness Model -- The Security Benefits of Personal Use -- Roundabouts and Stop Signs -- The Technology Professional -- Insider Threats -- Deter -- Detect -- Discipline -- Finding the Balance -- Chapter 6: Emerging Threats and Vulnerabilities: Reality and Rhetoric -- Structured Methods for Identifying Threat Trends -- The Product Life Cycle Model -- Understanding Threat Agents -- Playing War Games -- Trends That Span the Threat Landscape -- Trust Is an Attack Surface -- Barriers to Entry Are Crumbling -- The Rise of Edge Case Insecurity -- The Enemy Knows the System -- Key Threat Activity Areas -- The Industry of Malware -- The Web Expands to the Internet of Things -- Smartphones -- Web Applications -- Conclusion -- Chapter 7: A New Security Architecture to Improve Business Agility -- The 9 Box of Controls, Business Trends, and Architecture Requirements -- 9 Box of Controls -- IT Consumerization -- New Business Needs -- Cloud Computing -- Changing Threat Landscape -- Privacy and Regulatory Requirements -- New Architecture -- Trust Calculation -- Source Score -- Destination Score -- Available Controls -- Calculating Trust -- Security Zones -- Untrusted Zones -- Selective Zones -- Trusted Zones -- Balanced Controls -- Users, Data, and the Internet of Things: The New Perimeters -- Data Perimeter -- User Perimeter -- Internet of Things -- Conclusion -- Chapter 8: Looking to the Future: Emerging Security Capabilities.

Internet of Things -- Consistent User Experience Across Devices -- Cloud Computing -- Big Data Analytics -- Artificial Intelligence -- Business Benefits and Risks -- New Security Capabilities -- Baseline Security -- Protected Environments -- Encryption -- Hardware Acceleration -- Enhanced Recovery -- AI-Based Security and Automation -- Context-Aware Security -- Cloud Security and Context Awareness -- Security Analytics and Data Protection -- Conclusion -- Chapter 9: Corporate Social Responsibility: The Ethics of Managing Information Risk -- The Expanding Scope of Corporate Social Responsibility -- The Evolution of Technology and Its Impact -- Maintaining Society's Trust -- The Ethics of Managing Information Risk -- Conclusion -- Chapter 10: The 21st Century CISO -- Chief Trust Officer -- The Z-Shaped Individual -- Foundational Skills -- Becoming a Storyteller -- Fear Is Junk Food -- Accentuating the Positive -- Demonstrating the Reality of Risk -- The CISO's Sixth Sense -- Taking Action at the Speed of Trust -- The CISO as a Leader -- Learning from Other Business Leaders -- Voicing Our Values -- Discussing Information Risk at Board Level -- Conclusion -- Chapter 11: Performance Coaching -- How to Use the Tables -- Independence and Initiative -- Efficiency and Effectiveness -- Commitment --

Professionalism -- Discipline -- Teamwork -- Problem-Solving -- Communication -- Listening -- Style -- Clarity -- Goal-Setting -- Conclusion -- Appendix A -- Index.