

1. Record Nr.	UNISALENTO991003247539707536
Autore	Erbschloe, Michael, 1951-
Titolo	Physical security for IT [electronic resource] / Michael Erbschloe
Pubbl/distr/stampa	Amsterdam ; Boston : Elsevier Digital Press, c2005
ISBN	9781555583279 155558327X
Descrizione fisica	xix, 231 p. : ill. ; 23 cm.
Disciplina	004/.068/4
Soggetti	Computer networks - Security measures Electronic data processing departments - Security measures Electronic books.
Lingua di pubblicazione	Inglese
Formato	Risorsa elettronica
Livello bibliografico	Monografia
Nota di bibliografia	Includes bibliographical references and index.
Nota di contenuto	The physical security of IT, network, and telecommunications assets is equally as important as cyber security. We justifiably fear the hacker, the virus writer and the cyber terrorist. But the disgruntled employee, the thief, the vandal, the corporate foe, and yes, the terrorist can easily cripple an organization by doing physical damage to IT assets. In many cases such damage can be far more difficult to recover from than a hack attack or malicious code incident. It does little good to have great computer security if wiring closets are easily accessible or individuals can readily walk into an office and sit down at a computer and gain access to systems and applications. -- Even though the skill level required to hack systems and write viruses is becoming widespread, the skill required to wield an ax, hammer, or fire hose and do thousands of dollars in damage is even more common. Although many books cover computer security from one perspective or another, they do not thoroughly address physical security. This book shows organizations how to design and implement physical security plans. It provides practical, easy-to-understand and readily usable advice to help organizations to improve physical security for IT, network, and telecommunications assets.
Sommario/riassunto	The physical security of IT, network, and telecommunications assets is equally as important as cyber security. We justifiably fear the hacker,

the virus writer and the cyber terrorist. But the disgruntled employee, the thief, the vandal, the corporate foe, and yes, the terrorist can easily cripple an organization by doing physical damage to IT assets. In many cases such damage can be far more difficult to recover from than a hack attack or malicious code incident. It does little good to have great computer security if wiring closets are easily accessible or individuals can readily walk into an office and sit down at a computer and gain access to systems and applications. Even though the skill level required to hack systems and write viruses is becoming widespread, the skill required to wield an ax, hammer, or fire hose and do thousands of dollars in damage is even more common. Although many books cover computer security from one perspective or another, they do not thoroughly address physical security. This book shows organizations how to design and implement physical security plans. It provides practical, easy-to-understand and readily usable advice to help organizations to improve physical security for IT, network, and telecommunications assets. * Expert advice on identifying physical security needs * Guidance on how to design and implement security plans to prevent the physical destruction of, or tampering with computers, network equipment, and telecommunications systems * Explanation of the processes for establishing a physical IT security function * Step-by-step instructions on how to accomplish physical security objectives * Illustrations of the major elements of a physical IT security plan * Specific guidance on how to develop and document physical security methods and procedures.
