

1. Record Nr.	UNINA9910688556703321
Autore	Foreman Park
Titolo	Vulnerability Management
Pubbl/distr/stampa	Milton, : Auerbach Publications, 2019
ISBN	1-000-01193-3 1-000-00509-7 0-415-01546-4 0-429-28965-0
Edizione	[2nd ed.]
Descrizione fisica	1 online resource (330 pages)
Disciplina	005.8 658.478
Soggetti	Information technology - Security measures Computer security
Lingua di pubblicazione	Inglese
Formato	Materiale a stampa
Livello bibliografico	Monografia
Note generali	Description based upon print version of record.
Nota di contenuto	The vulnerability experience -- Program and organization -- Technology -- Selecting technology -- Process -- Execution, reporting, and analysis -- Planning -- Strategic vulnerabilities -- Managing vulnerabilities in the cloud.
Sommario/riassunto	Vulnerability management (VM) has been around for millennia. Cities, tribes, nations, and corporations have all employed its principles. The operational and engineering successes of any organization depend on the ability to identify and remediate a vulnerability that a would-be attacker might seek to exploit. What were once small communities became castles. Cities had fortifications and advanced warning systems. All such measures were the result of a group recognizing their vulnerabilities and addressing them in different ways. Today, we identify vulnerabilities in our software systems, infrastructure, and enterprise strategies. Those vulnerabilities are addressed through various and often creative means. Vulnerability Management demonstrates a proactive approach to the discipline. Illustrated with examples drawn from Park Foreman's more than three decades of multinational experience, the book demonstrates how much easier it is to manage potential weaknesses than to clean up after a violation.

Covering the diverse realms that CISOs need to know and the specifics applicable to singular areas of departmental responsibility, he provides both the strategic vision and action steps needed to prevent the exploitation of IT security gaps, especially those that are inherent in a larger organization. Completely updated, the second edition provides a fundamental understanding of technology risks--including a new chapter on cloud vulnerabilities and risk management--from an interloper's perspective. This book is a guide for security practitioners, security or network engineers, security officers, and CIOs seeking understanding of VM and its role in the organization. To serve various audiences, it covers significant areas of VM. Chapters on technology provide executives with a high-level perspective of what is involved. Other chapters on process and strategy, although serving the executive well, provide engineers and security managers with perspective on the role of VM technology and processes in the success of the enterprise.

---