1.

Record Nr.	UNINA9910820975603321
Autore	Gregory Peter H
Titolo	IT disaster recovery planning for dummies / / Peter Gregory ; foreword by Philip Jan Rothstein
Pubbl/distr/stampa	Hoboken, NJ, : Wiley, c2008
ISBN	9781118050637 1118050630 9780470277218 0470277211
Edizione	[1st edition]
Descrizione fisica	1 online resource (386 p.)
Collana	For Dummies
Classificazione	336.57
Disciplina	658.4/78
Soggetti	Information technology - Security measures Information resources management Emergency management
Lingua di pubblicazione	Inglese
Formato	Materiale a stampa
Livello bibliografico	Monografia
Note generali	Includes index.
Nota di contenuto	IT Disaster Recovery Planning for Dummies; About the Author; Dedication; Author's Acknowledgments; Contents at a Glance; Table of Contents; Foreword; Introduction; About This Book; How This Book Is Organized; What This Book Is - and What It Isn't; Assumptions about Disasters; Icons Used in This Book; Where to Go from Here; Write to Us!; Part I: Getting Started with Disaster Recovery; Chapter 1: Understanding Disaster Recovery; Disaster Recovery Needs and Benefits; Beginning a Disaster Recovery Plan; Managing the DR Project; Understanding the Entire DR Lifecycle Chapter 2: Bootstrapping the DR Plan EffortStarting at Square One; Resources to Begin Planning; Emergency Operations Planning; Preparing an Interim DR Plan; Building the Interim Plan; Testing Interim DR Plans; Chapter 3: Developing and Using a Business Impact Analysis; Understanding the Purpose of a BIA; Scoping the Effort; Conducting a BIA: Taking a Common Approach; Capturing Data for the BIA; Introducing Threat Modeling and Risk Analysis; Performing Threat Modeling and Risk Analysis; Identifying Critical Components; Determining the Maximum Tolerable Downtime

Calculating the Recovery Time ObjectiveCalculating the Recovery Point Objective; Part II: Building Technology Recovery Plans; Chapter 4: Mapping Business Functions to Infrastructure; Finding and Using Inventories; Using High-Level Architectures; Identifying Dependencies; Chapter 5: Planning User Recovery; Managing and Recovering End-User Computing; Managing and Recovering End-User Communications; Chapter 6: Planning Facilities Protection and Recovery; Protecting Processing Facilities; Selecting Alternate Processing Sites; Chapter 7: Planning System and Network Recovery

Managing and Recovering Server ComputingManaging and Recovering Network Infrastructure; Implementing Standard Interfaces; Implementing Server Clustering; Chapter 8: Planning Data Recovery; Protecting and Recovering Application Data; Choosing How and Where to Store Data for Recovery; Protecting and Recovering Applications; Off-Site Media and Records Storage; Chapter 9: Writing the Disaster Recovery Plan; Determining Plan Contents; Structuring the Plan; Managing Plan Development; Preserving the Plan; Taking the Next Steps; Part III: Managing Recovery Plans; Chapter 10: Testing the Recovery Plan

Testing the DR PlanConducting Paper Tests; Conducting Walkthrough Tests; Conducting Simulation Testing; Conducting Parallel Testing; Conducting Cutover Testing; Planning Parallel and Cutover Tests; Establishing Test Frequency; Chapter 11: Keeping DR Plans and Staff Current; Understanding the Impact of Changes on DR Plans; Incorporating DR into Business Lifecycle Processes; Establishing DR Requirements and Standards; A Multi-Tiered DR Standard Case Study; Maintaining DR Documentation; Training Response Teams; Chapter 12: Understanding the Role of Prevention

Preventing Facilities-Related Disasters

Sommario/riassunto

If you have a business or a nonprofit organization, or if you're the one responsible for information systems at such an operation, you know that disaster recovery planning is pretty vital. But it's easy to put it off. After all, where do you start? IT Disaster Recovery Planning For Dummies shows you how to get started by creating a safety net while you work out the details of your major plan. The right plan will get your business back on track quickly, whether you're hit by a tornado or a disgruntled employee with super hacking powers. Here's how to assess the situation, develop both