Disaster Recovery and Business Continuity

http://www.eccouncil.org

EC-Council

Introduction

A disaster recovery plan (DRP) - sometimes referred to as a business continuity plan (BCP) or business process contingency plan (BPCP) - describes how an organization is to deal with potential disasters. Just as a disaster is an event that makes the continuation of normal functions impossible, a disaster recovery plan consists of the precautions taken so that the effects of a disaster will be minimized, and the organization will be able to either maintain or quickly resume mission-critical functions. Typically, disaster recovery planning involves an analysis of business processes and continuity needs; it may also include a significant focus on disaster prevention.

Disaster recovery is becoming an increasingly important aspect of enterprise computing. As devices, systems, and networks become ever more complex, there are simply more things that can go wrong. As a consequence, recovery plans have also become more complex. According to Jon William Toigo (the author of Disaster Recovery Planning), fifteen years ago a disaster recovery plan might consist of powering down a mainframe and other computers in advance of a threat (such as a fire, for example, or the sprinkler system), disassembling components, and subsequently drying circuit boards in the parking lot with a hair dryer. Current enterprise systems tend to be too complicated for such simple and hands-on approaches, however, and interruption of service or loss of data can have serious financial impact, whether directly or through loss of customer confidence.

Appropriate plans vary a great from one enterprise to another, depending on variables such as the type of business, the processes involved, and the level of security needed. Disaster recovery planning may be developed within an organization or purchased as a software application or a service. It is not unusual for an enterprise to spend 25% of its information technology budget on disaster recovery.

Six years after the events of 9/11, many corporate IT operations are overconfident about their ability to handle a disaster, according to a Forrester Research, Inc. 2007 report.

The survey of 189 data center decision makers found a severe lack of IT preparation for natural and manmade disasters.

For example, the report found that 27% of the respondents' data centers in North America and Europe do not run a failover site to recover data in the event of a disaster. About 23% of respondents said they do not test disaster recovery plans, while 40% test their plans at least once a year.

Faced with potential catastrophe caused by anything from the weather to a malicious attack, company's need to make sure their disaster recovery plans match best practices.

Requirements

Pass exam 312-76 to achieve EC-Council Disaster Recovery Professional (EDRP) certification. Benefits EDRP is for experienced hands in the industry and is backed by a curriculum designed by the best in the field. Greater industry acceptance as seasoned security professional.

Exam

Students will be prepared for EC-Council's EDRP exam 312-76 on the last day of the class.

Course Description

The EDRP course teaches you the methods in identifying vulnerabilities and takes appropriate countermeasures to prevent and mitigate failure risks for an organization. It also provides the networking professional with a foundation in disaster recovery principles, including preparation of a disaster recovery plan, assessment of risks in the enterprise, development of policies, and procedures, and understanding of the roles and relationships of various members of an organization, implementation of the plan, and recovering from a disaster.

This EDRP course takes an enterprise-wide approach to developing a disaster recovery plan. Students will learn how to create a secure network by putting policies and procedures in place, and how to restore a network in the event of a disaster.

Who Should Attend

Network server administrators, Firewall Administrators, Security Testers, System Administrators and Risk Assessment professionals.

Duration:

5 days (9:00 – 5:00) Certification

Course Outline v2

Module 01: Introduction to Disaster Recovery and Business Continuity

Disaster Recovery & Business Continuity: Terminologies
Disaster Types
Consequences of Disaster
Disaster Recovery & Business Continuity
Principles of Disaster Recovery and Business Continuity
Disaster Recovery & Business Continuity: Issues Addressed
Activities of Disaster Recovery & Business Continuity
Disaster Recovery and Business Continuity Program
Disaster Recovery & Business Continuity Solutions
Best Practices in Disaster Recovery & Business Continuity Program
International Strategy for Disaster Reduction (ISDR)
International Day for Disaster Reduction

Module 02: Nature and Causes of Disasters

Nature of Disasters
Categorization of Disasters
Natural Disasters
Earthquakes
Protecting Yourself During Earthquake
Earthquakes: Volcanoes
Protection from Volcanoes
Forecasting Volcanoes
Estimating Earthquakes
Earthquakes: Tsunami
Protecting Yourself During Tsunami
Landslides
Effects of Landslides
Protecting Yourself from Landslides
Hurricanes
Safety Measures During Hurricanes
Predicting Hurricanes
Floods
Effect of floods
Prevention Measures
Wildfires
Safety Measures
Drought
Consequences of Drought
Measures to Overcome Drought Effects
Man-Made Disasters
Accidents
Power Outage
Telecommunication Outage
Categorization of Human Intentional Disasters
Arson
Civil Disorder
Terrorism
War

Module 03: Emergency Management

Emergency
Emergency Management
Need for Emergency Management
Emergency Management Phases
Mitigation
Preparedness
Response
Recovery
Effect of Disaster on Business Organizations
Emergency Management for Business Organizations
FEMA- Federal Emergency Management Agency
FEMA as an Organization
Activities of FEMA

Module 04: Laws and Acts

Introduction
Applicable Acts in DR
Laws and Acts in United States of America
Industries: Sarbanes-Oxley Act
Foreign Corrupt Practices Act (FCPA)
Healthcare: HIPAA Regulations
Financial Institutions: Gramm-Leach-Bliley Act
Flood Disaster Protection Act of 1973
Robert T. Stafford Disaster Relief and Emergency Assistance Act
CAN-SPAM Act of 2003
Federal Financial Institutions Examinations Council (FFIEC)
Personal Information Protection and Electronic Documents Act (PIPEDA)
Laws and Acts of Europe
Data Protection Act 1998
Transmission of Personal Data: Directive 2002/58/EC
Personal Data: Directive 95/46/EC
Insurance: Financial Groups Directive (FGD)
The Foundation of Personal Data Security Law: OECD Principles

Dutch Personal Data Protection Act
Austrian Federal Act concerning the Protection of Personal Data
German Federal Data Protection Act
Laws and Acts in Australia
Health Records and Information Privacy Act (HRIP)
Financial Transactions Reporting (FTR) Act 1988

Module 05: Business Continuity Management

Business Continuity Management
Business Continuity Planning
Objectives of Business Continuity Planning
Essential Resources in Business Continuity Planning
Business Continuity Management Planning Steps
ISO (International Organization for Standardization)
Overview of BS 7799 / ISO 17799
ISO/IEC 17799:2005
ISO/IEC 17799:2005: Business Continuity Management
Risk Analysis
Risk Assessment
Basic Elements of Risk Assessment
Business Impact Analysis (BIA)
Components of Business Impact Analysis
Threat Analysis
Risk Analysis and Business Impact Analysis
Crisis Management
Steps in Crisis Management
Crisis Management Phases
Compliance
Preparedness
Training and Resource Development
Contingency Planning
Points to remember in BCM Plan Testing
Birmingham City Council's BCM Assessment Template
Greenwich Council – Emergency and BCM Plan

Module 06: Disaster Recovery Planning Process

Disaster Recovery Planning Process
Management Support
Organizing DR Team
Components of Disaster Recovery Team
Disaster Recovery Planning Team
Building a Planning Team
Establishing Team at the Departmental Level
Risk Assessment
Risk Assessment
Conduct Business Impact Analysis
Critical Business Activities
Analysis Sheet
Example: Analysis Sheet for IT System
Roles and Responsibilities
Individual: Leader
Individual: Disaster Recovery Coordinator
Individual: IT Administrator
Individual: Network Manager
Individual: Disaster Recovery Manager
Individual: DR Team Member
Team: Administration Team
Team: Technical Team
Team: Damage Evaluation and Salvage Team
Team: Physical Security Team
Team: Communications Team
Responsibilities Common to all Disaster Recovery Teams
Developing Charts of Responsibilities
Facility Disaster Recovery Chart of Responsibilities
Department Disaster Recovery Chart of Responsibilities
Business Process Disaster Recovery Chart of Responsibilities
Developing Policies and Procedures
Assumptions for DR Planning
Need for Disaster Recovery Planning
Disaster Recovery Plan Development
Disaster Recovery & Management: Budgeting

Centralized Office of DR Planning: Budget
Safety and Health Procedures
Procedures for Internal and External Communications
Procedures for Containment and Property Protection
Procedures for Recovering and Resuming Operations
Assessing Insurance Requirements & Coverage Needs
Need for Insurance
Evaluating Insurance Policies
Testing and Training
DRP Testing and Rehearsal Process
DRP Testing: Advantages
DRP Testing: Methods
DRP Testing Steps
DRP Testing Flow Chart
Training DR Teams
Commence Training Program for Disaster Recovery
Training for Executives
Training for Middle Managers
Training for Supervisors
Training for Disaster Response Teams
Training for Employees
Documentation of DR Procedures
Need for Documentation of Plans
Important Documentations in Disaster Recovery Process
Writing Disaster Recovery Plan
Best Practices for Documentation
Managing Records
DRP Maintenance
Monitoring Process
Monitoring Procedures
Evaluate Latest Technologies
Conducting Regular Reviews
Conducting Training Programs for Updated Plan
DRP Implementation
DR Plan Implementation
Internal and External Awareness Campaigns

Module 07: Risk Management

What is Risk
Introduction to Risk Management
Functions of Risk Management
Analytic Process of Risk Management
Risk Analysis
Risk Reduction Analysis
Management Decision
Risk Reduction Planning
Reviews and Audit
Project Risk Management
IT Security Risk Management
Risk Management Standards
Financial Risk Management
Basel II and Risk Management
Pillar I: Minimum Capital Requirement
Pillar II: Supervisory Review Process
Pillar III: Market Discipline
Quantitative Risk Management
Best Practices in Risk Management

Module 08: Facility Protection

Facility Protection
Water Supply
Protecting Water Supply
Fire
Types of Fire Extinguishers
APW Extinguishers
Dry Chemical Extinguisher
Carbon Dioxide Extinguishers
Points to Remember
Using a Fire Extinguisher
Fire Suppression for Companies
Fire exits
Power Supply
Common Power Supply Problems

Ensuring Steady Power Supply
Ventilation
Kinds of Ventilation
Measures for Proper Ventilation
Air Conditioners
Measures for Proper Working of Air Conditioners
Building and Premises
Checklist for Securing Facility

Module 09: Data Recovery
Introduction - Data Recovery
Types of Data Recovery
Logical Data Recovery
Physical Data Recovery
Disk-to-Disk-to Disaster Recovery (3DR) Concept
Steps in Data Recovery
Recovery Management
Recovery Management Evaluation Metrics
Recovery Time Objective (RTO)
Role of RTO in Disaster recovery
Recovery Point Objective (RPO)
Network Recovery Objective (NRO)
Recovery Management Model Layers
Data Protection Continuum
Do's and Don'ts
Lumigent's Log Explorer
Best Practices in Data Recovery

Module 10: System Recovery
System Restore in Windows XP
Linux System Recovery
Linux System Crash Recovery
Crash Recovery Kit for Linux
Mac System Recovery
Restoring Windows Server 2003
Recovering from Boot problems in Windows Server 2003

Step 1: Start computer by using Last Known Good Configuration
Step 2: Starting computer in Safe Mode
Step 3: Use Event Viewer to Identify the Cause of the Startup Problem
Step 4: Use System Information to Identify the Cause of the Startup Problem
Step 5: The Safe Mode Boot Log File
Step 6: Use Device Manager to Identify the Cause of the Startup Problem
Step 7: Use System Configuration Utility
Microsoft Windows Recovery Console
Automated System Recovery
Windows 2000 Backup and Restore Utility
Methods for Restoring Replicated Data
Restoring Server Services
Active Directory Recovery: Non-Authoritative Restore
Active Directory Recovery: Authoritative Restore
Verifying Active Directory Restoration: Advanced Verification
Verifying Active Directory Restoration: Basic Verification
Active Directory Recovery on a Computer with a Different Hardware Configuration
Sysvol Recovery: Primary Restore
Sysvol Recovery: Non-authoritative Restore
Sysvol Recovery: Authoritative Restore
Recovery of Global Catalog Server
Recovery of an Operations Master
Domain Controller Recovery: With a Working Domain Controller
Domain Controller Recovery: Without a Working Domain Controller
Database Integrity Testing
Rights Management Services Restoration
Rights Management Services Database Restoration
Tools for Active Directory Disaster Recovery: Recovery Manager
Restoring IIS Configurations: iisback.vbs
Restoring Microsoft IIS Metabase Backup
WANSync IIS
WANSync IIS: Working
Restoring Exchange Server 2003
Data Recovery Scenarios
Exchange Data Recovery Preparation
Single Mailbox Recovery
Single Item Recovery using Deleted Items Retention

Single Item Recovery using Third-party Brick Backup Programs
Full-Server Recovery: Preparation
Full-Server Recovery: Option 1
Full-Server Recovery: Option 2
Full-Server Recovery: Option 3
Full-Server Recovery: Option 4
Exchange Server Backup/Recovery Solution: SonaSafe
Recovering Blackberry Enterprise Server
IBM WebSphere Application Server Recovery
Recovering Coldfusion Application Server: CFMAIL Bug
Recovering Coldfusion Application Server: Variable Deadlocks
Recovering Coldfusion Application Server: ODBC Errors
Recovering Coldfusion Application Server:500 IIS Internal Server Error
Recovering Coldfusion Application Server: System Registry Access Problem
Recovering from Domino Server Crashes
Tool: SteelEye LifeKeeper
Restoring MySQL Server
Restoring MS SQL Server: Option 1
Restoring MS SQL Server: Option 2
Restoring MS SQL Server: Option 3
Restoring MS SQL Server: Option 4
Restoring MS SQL Server: Option 5
Restoring MS SQL Server: Option 6
Restoring MS SQL Server: Option 7
Restoring MS SQL Server: Option 8
Restoring My SQL Server
Recovering Cisco IOS

Module 11: Backup and Recovery

Backup
Need for Backup
Types of Backup:
Full Backup
Incremental Backup
Differential Backup
Hot Backup

Hot Backup Sample Code
Cold Backup
Cold Backup Sample Code
Backup Sites
Hot Site/ Cold Site
Redundant Array of Inexpensive Disks (RAID)
RAID: Some Important Levels
Wide Area File Services (WAFS)
Backup for UNIX
Bare Metal Recovery for LINUX
Bucky Backup for Mac OS X
System Backup Administrator
NanoCopy Technology
Backup4all
Backup4all Features
ABC Backup Software
Genie Backup Manager
NTI BackupNow
High Availability Disaster Recovery (HADR)
Best Practices in Backup & Recovery

Module 12: Centralized and Decentralized System Recovery

Distributed Computing
Objectives of Distributed Computing
Architecture for Distributed Computing
Working of Distributed Computing
Centralized Backup
Centralized Backup Using SAN or NAS Server
Data Consolidation
Cross-Platform Data Consolidation
Mainframe as Centralized Storage Source
Tiers of Disaster Recovery
GDPS/PPRC
GDPS/PPRC Configuration
GDPS/PPRC Single-site Workload Configuration
GDPS/PPRC Multi-site Workload Configuration

Module 13: Windows Data Recovery Tools

Digital Photo Recovery
Active@ UNERASER
Test Disk
PhotoRec
BadCopy Pro
Directory Snoop
Data Advisor
Fast File Undelete
File Scavenger
GetDataBack
Kernel Recovery for FAT+NTFS
R-Mail
R-Studio
Recover4all
Recover It All
Recover My Files Data Recovery
Quick Recovery for Windows
Restorer2000
File Recovery
EasyRecovery DataRecovery
EasyRecovery Professional
RecoverSoft Media Tools Professional
RecoverSoft Data Rescue PC
ADRC Data Recovery Software Tool
SalvageRecovery for Windows
Disk Doctors Email Recovery
Winternals Recovery Manager

Module 14: Linux, Mac and Novell Netware Data Recovery Tools

Kernel Recovery for Linux
Kernel Recovery for ReiserFS
Kernel Recovery for JFS
Kernel Recovery for Macintosh

Kernel Recovery for Novell-Netware
Stellar Phoenix Linux
R-Linux
Quick Recovery for Linux
Quick Recovery for Macintosh
SalvageRecovery for Linux
SalvageRecovery for Mac
SalvageRecovery for Netware
Disk Doctors Linux Data Recovery Software
DiskInternals Linux Reader

Module 15: Incident Response

Incident
Category of Incidents
Low Level
Mid Level
High Level
How to Identify an Incident?
How to Prevent an Incident?
Relationship between Incident Response, Incident Handling, and Incident Management
Incident Management Plan
Incident Handling
Information Security Life Cycle
Incident Response
Incident Response Policy
Risk Analysis
Risk Analysis and Incident Response
Incident Response Methodology
Preparation
Identification
Containment
Eradication
Recovery
Follow up
CERT (Computer Emergency Response Team)
CSIRT (Computer Security Incident Response Team)

General Categories of CSIRTs
Members of CSIRT Team
Building an Effective CSIRT
FIRST (Forum of Incident Response and Security Teams)
Request Tracker for Incident Response
Helix – Incident Response & Computer Forensics Live CD
Incident Response Tools Present in Helix CD
THE FARMER'S BOOT CD
Resources

Module 16: Role of Public Services in Disaster

Public Services
State and Local Governments
Public Utilities and Departments
Hospitals
Blood Banks
Medical Laboratories
Food Banks
Fire Fighting Service
Waste/ Debris Management
Police
Armed Forces
Public Transportation
Water Supply System
Electricity Department
Information & Public Relations Department
IT Service Providers

Module 17: Organizations Providing Services during Disasters

Organizations Providing Services during Disasters
Relief Organizations
International Committee of the Red Cross (ICRC)
International Federation of Red Cross and Red Crescent Societies (IFRC)
United Nations Children's Fund (UNICEF)
National Emergency Response Team (NERT)
CARE

Ananda Marga Universal Relief Team (AMURT)
Action Against Hunger (AAH)
Emergency Nutrition Network (ENN)
Doctors Without Borders
Hunger Plus, Inc.
InterAction
International Rescue Committee (IRC)
Mennonite Central Committee (MCC)
Mercy Corps (MC)
Refugees International
Relief International
Save the Children
Project HOPE

Module 18: Organizations Providing Disaster Recovery Solutions

Organizations Providing Disaster Recovery Solutions
Symantec
System Sizing
System Sizing: Practices
Disk-based Backup
Manual System Recovery
Disadvantages
Automated System Recovery
IBM
Human Capital Resilience
Human Capital Risks in Crisis Situations
Business Resilience
Elements of Business Resilience
Framework for Business Resilience
Causes of E-Mail Outages
E-Mail Continuity
DELL
Oracle Data Guard Utility
RMAN Utility for Database Backup
NAS (Network Attached Storage)
Sun Microsystems

Integrated Solutions of Sun and Vignette
Sun Cluster Geographic Edition
Infosys Business Continuity Planning Solution
Infosys BCP solution
Sybase Business Continuity Planning Solution
Sybase Model
HP Business Continuity and Availability solutions
HP 3-tiered Service Levels Balance Investment with Risk
PricewaterhouseCoopers Fast Track BCP
AT&T's Business Continuity and Disaster Recovery

Module 19: Case Studies

Business Continuity for Critical Applications
Jones Walker: Weathering the Storm
Let's be prepared: An educational project about disasters in Cuba
From rehabilitation to safety: Gujarat school safety initiative, India
Disaster-resistant schools: A tool for universal primary education
Disaster Recovery Situation Assessment
Disaster Recovery Planning
Business Continuity Planning and Business Impact Analysis
Local risk management in earthquake zones of Kazakhstan
Disaster Recovery Case Study: Max Re
Disaster Recovery Case Study: GSD&M
Storage Assessment Services
Backup and Recovery Plan and Design
Storage Infrastructure Design and Implementation
Continuous Data Protection and Disaster Recovery
Disaster Recovery Testing
Disaster Recovery Strategy Assessment and Validation
Case Study: Improving Disaster Recovery Without Breaking the Bank