Chapter 3 – Business Continuity Planning

Planning for Business Continuity

- Business Continuity Planning (BCP) invovles assessing the risks to organizational processes and creating policies, plans, and procedures to minimize the impact those risks might have on the organization if they were to occur.
- Let’s think of scenarios.

CISSP Focuses

- Business Continuity Planning (BCP)
  - Now
- Disaster Recovery Planning (DRP)
  - Chapter 18

Planning for Business Continuity

- Goal is to be quick, calm, and efficient in any emergency
- Four main elements
  - Project scope and planning
  - Business impact analysis
  - Continuity planning
  - Plan approval and implementation

CISSP Focus

- Top priority in both BCP and DRP is always **PEOPLE**
- The primary concern is to get people out of harm's way, then address IT recovery and restoration issues

Project Scope and Planning

- Goals
  - Organizational Review
  - BCP Team Selection
  - Resource Requirements
  - External Dependencies
- Exact process depends on the size and nature of an organization

Organizational Review

- First responsibility
  - Individuals responsible for BCP
  - Identifying all departments and individuals who have a stake in the BCP process
- Two Reasons
  - Help identify potential BCP members
  - Sets reminder of BCP process

Organizational Review

- Be sure to account for your HQ and all other locations (physical and cloud)
- BCP team selection
  - What can go wrong?
  - IT = Security Department
  - Let’s mitigate some of the issues

BCP Team Selection

- A balance is required
- Different view points and creating a team
- Three areas for each organization
  - Technical
  - Financial
  - Political Environment

BCP Resource Requirements

- BCP Development
- BCP Testing, Training, and Maintenance
- BCP Implementation

Real World Scenario

- Explaining the Benefits of BCP
- Let’s discuss

BCP External Dependencies

- Vendors e.g. SaaS, SLA, etc.
  - SOC 1, 2, and 3
- Legal and Regulatory Requirements
  - Federal, state, and local

Business Impact Analysis

- Identifying priorities
- Risk identification
- Likelihood assessment
- Impact analysis
- Resource prioritization

Business Impact Analysis

- Identifying priorities
- Risk identification
- Likelihood assessment
- Impact analysis
- Resource prioritization

Identifying Priorities

- Asset Value (AV)
- Maximum Tolerable Downtime (MTD)
- Maximum Tolerable Outage (MTO)
- Recovery Time Objective (RTO)
- Recovery Point Objective (RPO)

Risk Identification

- Can you think of any?

Likelihood Assessment

- Will there be a volcano eruption in downtown Chicago?
- Annualized Rate of Occurrence (ARO)

Impact Analysis

- Exposure Factor (EF)
- Single Loss Expectancy (SLE)
- SLE = AV * EF
- Annualized Loss Expectancy (ALE)
- ALE = SLE * ARO
- Qualitative vs Quantitative

Resource Prioritization

- Quantitative
  - Create a list of all the risk and sort them computing the ALE
- Qualitative
  - Elevating or lowering the priority of risks that already exist on the ALE-sorted quantitative list

Continuity Planning

- Primary subtasks are:
  - Strategy development
  - Provisions and process
- The overall goal is to create a Continuity of Operations Plan (COOP)

Strategy Development

- Bridges the gap between the business impact analysis and the BCP development
- Determining risks and where to mitigate and the need for those resources then we can move on to the provisions and processes

Provisions and Processes

- There are three assets a business must protect and that is
  - People
  - Building/facilities
  - Infrastructure

People

- Poeple are the most valualbe assets of your organizations and you want to make sure they are safe at all cost before, during, and after an emergency
- The safety of people must always come before the organization's business goals

Building and Facilities

- Many buidling need specialized facilities to conduct business operations
- 1. Hardening Provisions
  - Protecting existing facilities
- 2. Alternate Sites
  - If it's not feasible then we need to invest in an alternate site under DRP

Infrastructure

- IT backbone of communications and computer systems that process orders, manage the supple chain, handle customer interaction, etc.
- Physical Hardening System
  - Protective measures introduced
- Alternative System
  - Redundancy

Plan Approval and Implementation

- Senior management buy-in is essential to the success of the overall BCP efforts
- Plan Approval
- Plan Implementation
- Communication, Training and Education
- BCP Documentation

BCP Documentation

- Continuity Planning Goals
- Statement of Importance
- Statement of Priorities
- Statement of Organizational Responsibility
- Statement of Urgency and Timing
- Risk Assessment

BCP Documentation

- Risk Acceptance/Mitigation
- Vital Record Program
- Emergency Response Guidelines
- Maintenance
- Testing and Exercises