Lecture objectives

- Define Business Continuity Plans and disaster recovery
- Describe why organisations should plan for a disaster
- Discuss the key components of a BCP and disaster recovery
- Identify the steps in a disaster recovery plan

Research

- 14% of companies using Internet business functions have an effective plan in place
- 25% of Local Area Networks (LAN) are vulnerable to disaster or disruption
- 64% of organizations are unprepared to protect their Wide Area Networks (WAN)
- 80% of all businesses w/o a BCP before Hurricane Andrew failed within 2 years (www.Contingencyplanning.com)
- 40 to 60% of Australian sites have done very little about disaster recovery. (IDC 2002)

Business Continuity & Disaster Recovery

- What is Business Continuity and Disaster Recovery Planning?
  - The process of creating plans, processes and/or procedures to resume or re-establish mission critical business functions within an acceptable time frame
  - A DR Plan recovers technology platforms and associated technology functions (i.e., networks, etc.)
  - Business Continuity plans focus on recovery of business functions and workgroup functions (i.e., Payroll Department, Call Center, etc.)

You can't have one without the other

DISCUSSION POINT:
WHAT ARE THE IMPLICATIONS OF THESE FINDINGS FOR BUSINESS??
Business Continuity Plan Considerations

- Will business operations stop if a particular information system fails?
- How much lost revenue and cost will be incurred for each hour that the system is down?
- Which critical business functions cannot be completed?
- How will customers be supported?
- How long can the system be down before the company goes out of business?
- Who is coordinating and managing the disaster recovery?
- What will the users do while the system is down?
- How long will it take before the system is available for use?

Consequences of a Disaster

Issues:
- Who owes you money?
- Who are your customers?
- What orders do you have?
- Will the competitors take away your customers?

Result:
Your company could go out of business...

...if your company is gone...so is your job.

Complexity Of BCP Planning (disaster recovery journal)

Consequences Of IS Defence Breaches

SECURITY BREACH

FINANCIAL LOSS

CUSTOMER CONCERNS AND TRUST

LOSS OF MARKET SHARE

DAMAGE TO IMAGE

DAMAGE

REPUTATION DAMAGE

Process Inventory

- Identify critical systems, processes and functions;
- Establish an estimate of the maximum tolerable downtime (MTD) for each business process;
- Assess the economic impact of incidents or disasters that result in a denial of access to systems, services or processes; and,
- Determine the priorities and processes for recovery of critical business processes.
**Document Landscapes**

- It includes:
  - business process
  - business process steps
  - system interdependencies

**Logical Interfaces Solution Landscape**

- It includes:
  - internal and external interfaces
  - software components
  - existing system landscape

**Technical System Solution Landscape**

- It includes:
  - servers
  - storage subsystem
  - network configuration

---

**Review and Prioritise Risk Factors**

- Review risk factors
  - All Hazards Analysis
  - Likelihood of Occurrence
  - Impact of Outage on Operations
  - System Interdependence
  - Revenue Risk
  - Personnel and Liability Risks
- Prioritise risk factors

---

**Example: Core Business Process Solution Landscape**

**Key Components of BCP**

- **Assess** - identify and assess all threats
- **Evaluate** - assess likelihood and impact of each threat
- **Prepare** – plan for contingent operations
- **Mitigate** - identify actions that may eliminate risks in advance
- **Respond** – take actions necessary to minimize the impact of risks that materialize
- **Recover** – return to normal as soon as possible

---

**What About External Dependencies?**

**Risk Misconceptions**

- Sure, but… (common misconceptions)
  - …We are immune to disasters
  - …That never happens here
  - …We have an insurance policy, that’s enough
  - …We never had an outage before
- Learn from other situations:
  - Floods
  - Fires
  - Infrastructure Sabotage
Risk Rating Methodology

<table>
<thead>
<tr>
<th>Risk Factor</th>
<th>Risk Rating</th>
<th>Numeric Score</th>
<th>Explanation</th>
</tr>
</thead>
<tbody>
<tr>
<td>Degree of H</td>
<td>8</td>
<td>Process must function for core operations</td>
<td></td>
</tr>
<tr>
<td>Organizational M</td>
<td>6</td>
<td>Process required for daily settlement</td>
<td></td>
</tr>
<tr>
<td>Dependence L</td>
<td>3</td>
<td>Process is not critical in daily operations</td>
<td></td>
</tr>
<tr>
<td>Probability H</td>
<td>0</td>
<td>Probability &gt; 0.5 that alternative process will work</td>
<td></td>
</tr>
<tr>
<td>of Success M</td>
<td>2</td>
<td>Probability &lt; 0.5 that alternative process will work</td>
<td></td>
</tr>
<tr>
<td>Alternative L</td>
<td>3</td>
<td>No plan for alternative process</td>
<td></td>
</tr>
<tr>
<td>Dependence H</td>
<td>5</td>
<td>Business functions depend highly on process</td>
<td></td>
</tr>
<tr>
<td>on M</td>
<td>3</td>
<td>Business functions depend somewhat</td>
<td></td>
</tr>
<tr>
<td>Automation L</td>
<td>1</td>
<td>Manual operation possible w/o penalty</td>
<td></td>
</tr>
<tr>
<td>Criticality of H</td>
<td>4</td>
<td>Critical business function - core process</td>
<td></td>
</tr>
<tr>
<td>Business M</td>
<td>2</td>
<td>Secondary line-of-business</td>
<td></td>
</tr>
<tr>
<td>Process L</td>
<td>0</td>
<td>Not a critical process</td>
<td></td>
</tr>
</tbody>
</table>

Assessment – Organising Team

4 key people
- Recovery manager
  - Manages the entire recovery. All recovery activities and issues should be coordinated through this person.
- Communication liaison
  - Handles user phone calls and keeps top management updated with the recovery status.
- Technical recovery team
  - Does the actual technical recovery.
- Review and certification manager
  - Coordinates and plans the post-recovery testing and certification with users.

Assessment – Prioritising Risks

- Identify the 3 most common
  - Description of disaster event
  - High level plan of major tasks to be performed
  - Estimated time to have the system available to the users
- Most Common
  - Corrupt database (downtime 8 hours)
  - Hardware failure (downtime 7 days)
  - Loss of Facility (downtime 8 days)
- Recovery Script
  - Completing as many tasks as possible in parallel
  - Adding timetables for each step
- Why
  - Script is necessary because it helps you:
    - Develop and use a proven series of steps to restore system
    - Prevent missing steps
    - Missing a critical step may require restarting the recovery process from the beginning, which delays the recovery.
    - If the primary recovery person is unavailable, a recovery script helps the backup person complete the recovery.

Recovery Process

- To reduce recovery time, define a process by:
  - Completing as many tasks as possible in parallel
  - Adding timetables for each step
- Major Steps
  1. During a potential disaster, anticipate a recovery by:
    - Collecting facts
    - Recalling the latest offsite tapes
    - Calling all required personnel
    - Preparing functional organizations (sales, finance, and shipping) for alternate procedures for key business transactions and processes.
  2. Minimize the effect of the disaster by:
    - Stopping all additional transactions into the system
    - Waiting too long could worsen the problem
    - Collecting transaction records that have to be manually re-entered
  3. Begin the planning process by:
    - Analysing the problem
    - Fitting the disaster to your predefined scenario plans
    - Modifying the plans as needed
  4. Define when to initiate a disaster recovery procedure:
    - What are the criteria to declare a disaster, and have they been met?
    - Who will make the final decision to declare a disaster?
Recovery process continued

- 5. Declare the disaster.
- 6. Perform the system recovery.
- 7. Test and sign off on the recovered system.
  - Key users, who will use a criteria checklist to determine that the system has been satisfactorily recovered should perform the testing.
- 8. Catch up with transactions that may have been handled by alternate processes during the disaster.
  - Once completed, this step should require an additional sign-off.
- 9. Notify the users that the system is ready for normal operations.
- 10. Conduct a postmortem debriefing session.
  - Use the results from this session to improve your disaster recovery planning.

Crash Kit

What
- A crash kit contains everything needed to:
  - Rebuild the system servers
  - Reinstall system
  - Recover the system database and related files

Why
- Easy to get and carry in a disaster

Where
- Should be stored separately from servers
- Should be offsite but easily accessible

Crash Kit Contents

- Documentation (continued...)
  - Instructions to recall tapes from offsite data storage
  - An equipment list
  - File system layout
  - Hardware layout
- Key Phone numbers for:
  - Key users
  - Information services personnel
  - Facilities personnel
  - Other infrastructure personnel
  - Consultants
  - Systems hotline
  - Offsite data storage
  - Security department personnel
  - Service agreement contacts
  - Hardware vendors

Testing Disaster Recovery

- A test is a simulated disaster recovery which verifies that you can recover the system and exercise every task outlined in the disaster recovery plan.
- Test to find out if:
  - Your disaster recovery procedure works
  - Something changed, was not documented, or updated
  - There are steps that need clarification for others
  - Older hardware is no longer available
- Since many factors affect recovery time, actual recovery times can only be determined by testing. Once you have actual times (not guesses or estimates), your disaster planning

Disaster Planning

- Plan for the worse, hope for the best
- Disaster Plan
  - have one
  - if you don’t have one, start working on one
  - Ass-U-Me nothing
- Test the Plan … does your plan really work?
Conclusion

- As part of your security management procedures, BCP and disaster recovery plans are an integral part.
- Most often overlooked as an organisation's priority is more involved with their critical processes than considering what to do if a disaster occurred.

Business Continuity & Disaster Recovery

- Where else can I get information?
  - Free publications:
    - Disaster Recovery Journal
    - Contingency Planning & Management
  - Web Sites:
    - www.drj.com
    - www.contingencyplanning.com
    - www.globalcontinuity.com
    - www.recovery.sungard.com
    - www.disaster-resource.com
- Online Data security email
  - CSOonline.com.au
- Disaster Strategies for Record Keeping