Business Continuity Planning

Information Security

Prof Hans Georg Schaathun

Ålesund University College

Autumn 2011 – Week 13

Session objectives

- understand the relationship between incident response, disaster recovery, and business continuity
- be able to identify risks and possible solutions to business continuity

Incident response and disaster recovery

- Incident response
- Disaster recovery

Introduced before; what do we mean?

Incident response and disaster recovery

- Incident response (IR)
  - immediate action
  - effective IR should mean negligible effect on operation
  - serious disasters may be out of scope for IR
- Disaster recovery
  - restoring status quo
  - restoration may take time
  - production loss may incur while we wait

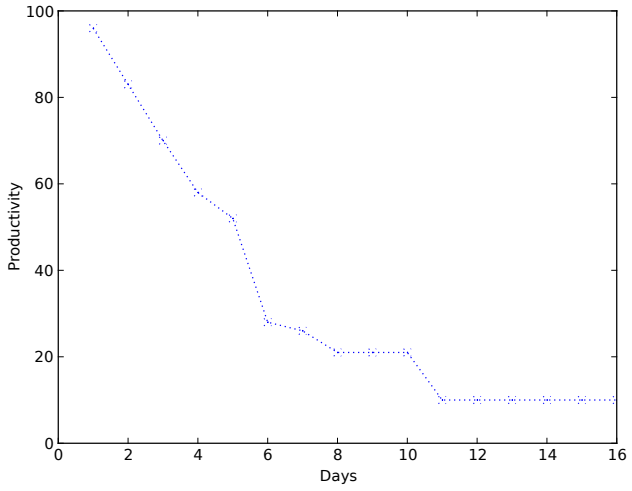
Business Continuity Plans

- *keep the business going*
  - when incident response falls short
  - while we wait for disaster recovery
- BCP supplements IR and DR
- The scope is the most serious incidents
  - when IR/DR is insufficient

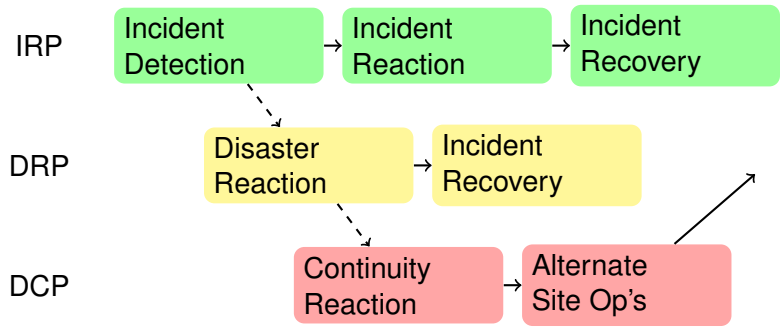
Why is BCP important?

- What happens if you loose email connection for
  - . . . 10 minutes?
  - . . . 1 hour?
  - . . . 4 hours?
  - . . . 2 days?
  - . . . a week?
  - . . . a month?

Incidents and Productivity



Contingency Planning



What are the challenges in a disaster?

- Hardware
- Software and configuration
- Data (restored from backup)
- Location — Buildings

Dedicated sites

Hot Sites a fully functional computing facility installed and configured for the organisation

Warm Site a partially installed computing facility. It typically includes server hardware, but not applications and workstations.

Cold Site is just a spare building where a computing facility may be installed

Shared facilities

Time-Share several organisations share a hot/warm/cold site. This gives more value for money, assuming that two organisations will not hit simultaneous disasters...

Service Bureaus provide a service for a few, such as an agreement to provide physical facilities in the event of a disaster

Mutual Agreements is some agreement between organisations to assist eachother in the event of a disaster.

Different facilities

Server and Data Centres High-security facilities. Security-aware management. Good planning is common.

PC-s and Workstations Are often forgotten. Left to the attention of individual users.

Remote Storage

- Backup is an obvious control
- Most common threats to control are
  - media decay and disk failure
  - user errors (deleting the wrong file)
- Rarer events include fire and theft
- Remote storage is essential to avoid losing both in the same event
- BCP: roll out the backup on an alternate site
  - can you do it quickly enough?

Do you make remote backups as frequently as local backups?

Continuity Planning versus Insurance

Is insurance an alternative to continuity planning?

- Insurance will normally cover recovery.
- It will rarely cover consequential loss
  - such as lost productivity
- Extended down-time may cause irrepairable loss

Conclusions

- Business Continuity Planning supplements other plans for security
- Where other plans focus on resolving a situation
  - BCP only provides a temporary solution
  - to keep going while the other plans are executed
- BCP often includes a backup facility
  - to run operations temporarily