Departamento de ENGENHARIA INFORMÁTICA
Instituto Superior de Engenharia do Porto

Systems and Information Security SEGSI

TP04

Disaster Recovery Plan

Pinto Leite, Jorge (jpl@isep.ipp.pt)

Disaster Recovery Plan (DRP)

- What is a Disaster Recovery Plan (DRP)?
- When defining the Business Continuity Management (BCM) some items were raised
  - Business Impact Analysis (BIA)
  - Risk Assessment (RA) and its representation on a Risk Matrix (RM)
  - Maximum Tolerable Downtime (MTD)
  - Maximum Tolerable Period of Disruption (MTPD)
  - Minimum Business Continuity Objective (MBCO)

Disaster Recovery Plan (DRP)

- According to the BIA, RA and RM, some measures have been taken or are in implementation process to avoid the loss of continuity
- The possible possibilities are:
  - Avoid
    - By taking appropriate actions to eliminate the risk
  - Transfer
    - By using third parties to assume the responsibility and action if they happen
  - Mitigate
    - By reducing risk exposure or implementing controls
  - Accept
    - By accepting it “as it is” without implementing any action

Disaster Recovery Plan (DRP)

- If they cost to avoid or mitigate is too expensive to be implemented as the result of the Annualized Loss Expectancy (ALE), that should have been reflected on the RA and, perhaps, a change on the planned action
    - From “Accept” to “Transfer”, for example
    - The “Accept” action should not be used except under very special reasons that should be characterized and described on the BCM system

Disaster Recovery Plan (DRP)

- Whichever action you choose, a violation of the MTD and / or MTPD can always occur
- Therefore, a plan must be defined to get normal activity up and running
- During the analysis of the BCP, it was noticed that MTD = RTO + WRT, however on some situations that might not be possible to achieve
- That is the *leitmotiv* of DRP

Disaster Recovery Plan (DRP)

- When designing a DRP it should be kept in mind the actions to be taken when an accident that would imply a violation of the MTD or MTPD
- It must contain
  - Who is responsible to decide its activation
  - The actions to be performed
  - When it should be left

Disaster Recovery Plan (DRP)

- Who is responsible to decide its activation
  - The responsibility to activate DRP should not be ambiguous
  - The name, role, and contact number (at least, better two contact numbers) must be clearly stated on the document as well as on the BCM and BCP
  - It is not usually mandatory, but a second level contact should also be defined also with its name, role and contact number (or two, as above)

Disaster Recovery Plan (DRP)

- The actions to be performed (i)
  - If DRP is activated, it is due to a situation that implied the loss of usual activity by the company
  - Several environments might have happened to that catastrophic (in business view) situation, so it could have a varied format
  - In spite of this, the mandatory aspect is to bring back as soon as possible the defined MBCO
  - In severe cases, premises offsite might be necessary
    - The main point here is to assure the MBCO, not the whole activity
  - Take in consideration that if offsite premises are planned, that would have an implication on several premises, for example, on the privacy and confidentiality of data, so it should be reflected on the service level agreement (SLA)

Disaster Recovery Plan (DRP)

- The actions to be performed (ii)
  - The Cloud is an usual infrastructure to use on the DRP
  - But where is the data?
    - Is it protected?
    - Is it confidential on the applicable parts?
    - Is it integrity assured?
  - On DRP and if Cloud (or any other provider) is used, the partner to use should have be contracted previously

Disaster Recovery Plan (DRP)

- When it should be left
  - After recovering the functioning of the infrastructure, DRP must be deactivated and restored the use of the usual infrastructure
  - Again, the name, role, and contact number(s) of the responsible to take that decision must also be stated on DRP
  - Usually, a mutual decision of the DRP responsible and the BCP responsible
    - As the decision to leave DRP and restore BCP needs to be taken by both, that might eventually be different people

Disaster Recovery Plan (DRP)

- The design of DRP, as noted before, has implications on the design of BCP
  - And BCM design has implications on the design of DRP
- There is a cross responsibility and activity between both plans
- There are always systems, applications and data involved on both plans
- Any change in any part of the BCP plan is reflected, if applicable, on DRP plan?

Disaster Recovery Plan (DRP)

- Systems
  - DRP systems might be slightly different from the usually used
  - Does that imply differences on requirements?
  - If devices like sensors or any other IoT device is needed, how can they be incorporated on DRP infrastructure?
    - Or, at least, how are they going to be replaced or its outputs going to be input on the DRP?

Disaster Recovery Plan (DRP)

- Applications and operating systems have regular updates
  - Are they also applied to the infrastructure that will be used on DRP?
  - What are the consequences if they are not?
  - In this case, severe problems might arise in operational behavior and activity
    - No one intends to have, for example, two versions of an application, one for use habitually, other to use if DRP is in use

Disaster Recovery Plan (DRP)

- Data is always changing
  - Are those changes reflected when DRP is activated?
- Supply chain might have an impact and be used on usual infrastructure
  - Will it be available or unavailable when DRP is activated?

Disaster Recovery Plan (DRP)

- It is mandatory to test the DRP on a regular basis
- Unexpected problems might be noted during tests, allowing measures to be taken during usual operation, thus avoiding them to show up under bad circumstances