Assignment 1

Business Continuity Management with focus on Backup and Restore

Andreas Ntaflos* Andreas Ntaflos† Christoph Seidl‡

December 23, 2014
Organizational Aspects of IT Security
VU 2.0 188.312 2014W

In this document we examine the implementation of company-wide data backup and restore solutions from a Business Continuity Management approach, specifically in a Disaster Recovery context. We discuss relevant concepts such as Business Continuity Planning and Disaster Recovery Planning, key metrics such as Recovery Point Objective, Recovery Time Objective and others which define the requirements of backup and restore solutions and techniques, and how these metrics must be based on a Business Impact Analysis to be useful in the business context. We look at the risks associated with backup and restore from an information security point of view and how to control for these risks when implementing a backup solution.

After reviewing different, representative backup solutions and techniques and discussing their merits and drawbacks—again from an information security point of view—we highlight various challenges and potential problems a company faces when implementing backup solutions. Finally we discuss future developments and how backup and disaster recovery requirements may change over time.

1 Business Continuity Management

Business Continuity Management (BCM) is a strategic management process covering *Business Continuity Planning* (BCP) and *Disaster Recovery Planning* (DRP) to ensure critical

*Matrikelnummer e0326302, daff@pseudoterminal.org
†Matrikelnummer e1328682, e1328682@student.tuwien.ac.at
‡Matrikelnummer e0427434, e0427434@student.tuwien.ac.at

business functions can continue during and after major incidents (flood, fire, earthquake, terrorism, vandalism, ...) with minimal loss of operations, systems and life.

BCM provides a framework for integrating resilience with the capability for effective responses that protects the interests of an organisation's key stakeholders. The main objective of BCM is to allow the organisation to continue to perform business operations under various conditions [3].

In BCM the two most important artifacts are the *Business Continuity Plan* (BCP) and the *Disaster Recovery Plan* (DRP). The BCP ensures that critical business functions can continue to operate during a disaster and its aftermath. This may include moving critical equipment to standby locations, bringing up emergency power generators, performing normally automated business operations manually or temporarily hiring additional personnel.

The DRP is usually a part of the BCP and is focused on the IT infrastructure itself. It defines how to prepare the IT infrastructure for a disaster, what to do in the event of a disaster and how to restore IT operations so that the business can go back to operating normally. The DRP's scope is thus much narrower and technology-focused than the BCP as a whole.

Disaster recovery can be quantified by four key metrics:

Maximum Tolerable Downtime (MTD) The maximum outage time of a critical business function or system that can be endured before the impact on the company becomes unacceptably severe

Recovery Point Objective (RPO) The amount of data loss, measured in time, that can be sustained from a disaster without causing irreparable damage to the company and its business functions

Recovery Time Objective (RTO) The time it may take to restore business functions after a disaster

Work Recovery Time (WRT) The time it may take to recover data and bring infrastructure back so that normal operation can continue

The MTD consists of the RTO and the WRT while the RPO exists independently of the MTD. Figure 1 shows the metrics in relation to each other. The MTD is also known as the *Maximum Tolerable Period of Disruption* (MTPD).

It should be noted that IT vendors of backup and DR solutions tend to conflate RTO and WRT into just RTO, which makes sense considering that a business function or process can hardly be declared "restored" when it is still missing its key business data. We will refer to RTO in the same manner in the remainder of this document.

The values for MTD, RPO and RTO usually differ between systems, business functions and processes. It is thus important not to define them ad-hoc and on a whim but on a solid understanding of the business functions in question. This understanding comes from the Business Impact Analysis.

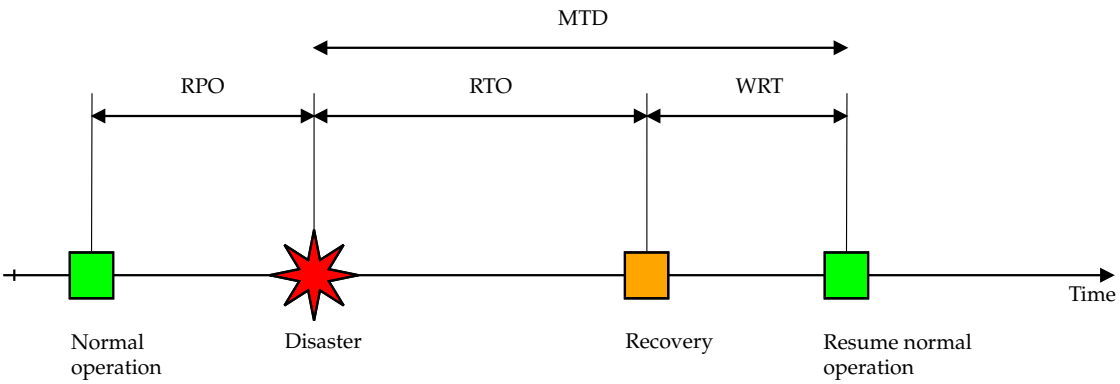

Figure 1: The disaster recovery metrics in relation to each other on a time line

2 Business Impact Analysis

The *Business Impact Analysis* (BIA) is a functional analysis that identifies the various business processes, functions, activities, resources and systems that define the business. It assigns them criticality levels and identifies threats and vulnerabilities for these functions and calculates the risk for each. The Business Impact Analysis is a key step in creating a disaster recovery plan and defining backup requirements.

In any reasonably sized organisation a BIA cannot be conducted by a single person or team without the help and input of key employees such as department heads and process owners. Thus the data for the BIA is gathered by means of interviews, questionnaires, workshops, existing documentation, etc. The result of the data gathering phase is a comprehensive list of business processes, functions and resources relevant to the organisation.

After all business processes and functions have been identified these resources need to be categorised by their criticality to the organisation. A resource is regarded as critical when its availability is imperative for the survival of the organisation and downtime of that resource is unacceptable. The most critical resources will receive the highest priority when recovering from a disaster while less- or non-critical systems will receive attention only after all critical systems have been dealt with. It is at this step that concrete values for MTD (MTPD), and later RPO and RTO of a critical resource can first be estimated.

MTD values can be categorised into *Nonessential*, *Normal*, *Important*, *Urgent* and *Critical*. The identified business resources are each assigned one of these categories and treated accordingly. The shorter the MTD, the more critical the resource, and the higher the priority it will be afforded when recovering.

When conducting the BIA it is important to consider interdependencies between business functions, resources or systems. Most business functions do not stand alone but depend on other business functions and systems, so when estimating the MTD these dependencies need to be taken into account.

The next step is threat and risk assessment. This includes identifying vulnerabilities,

threats and to the most critical business resources, determining the impact each threat may have and the likelihood of its occurrence. Vulnerabilities in resources are single points of failure or security issues, threats may include sabotage, vandalism or theft but also natural disasters or major utilities outages. The risk to a business function or resource is thus calculated as Risk = Threat × Impact × Probability.

At this point it is important to note that while identifying and planning for specific threats with high impact or likelihood is prudent it is not useful to try to account and prepare for *all* possible threats. Instead the organisation should prepare for the loss of any or all business resources, regardless of specific threats. This will provide the organisation with the proper flexibility when the time of disaster recovery comes.

After determining the MTD for critical business functions taking into account their dependencies on other business functions and resources reasonable values for RPO and RTO can be defined. These are more meaningful than just the MTD in a disaster recovery context and are an important basis for each critical business function's disaster recovery strategy.

3 Disaster Recovery Strategies

4 Review of backup tools and solutions

5 Challenges and potential problems

6 Future developments and requirements

References

[1] O.H. Alhazmi and Y.K. Malaiya. Evaluating disaster recovery plans using the cloud. In *Reliability and Maintainability Symposium (RAMS), 2013 Proceedings—Annual*, pages 1–6, Jan 2013.

[2] P. Fallara. Disaster recovery planning. *Potentials, IEEE*, 22(5):42–44, Dec 2004.

[3] Shon Harris. *CISSP All-in-One Exam Guide*. McGraw-Hill Osborne Media, 6th edition, 2012.

[4] M. Wiboonrat and K. Kosavisutte. Optimization strategy for disaster recovery. In *Management of Innovation and Technology, 2008. ICMIT 2008. 4th IEEE International Conference on*, pages 675–680, Sept 2008.