CSG2132 Module 4
Business Continuity and Security

Business Continuity

Business Continuity refers to an organisation's capacity to re-establish and/or maintain its core business operations when impacted by a moderate to severe event such as a natural disaster, loss of network access, cyber-attack, human error or unanticipated economic disruption.

Business Continuity Planning is a *whole of organisation* process that plans for the occurrence of such events and puts contingencies in place to rapidly restore operations and minimise impact on productivity and profitability. It also involves setting key parameters such as recovery times, acceptable data loss tolerances and the form and specificity of stakeholder reporting.

Although robust business continuity planning and system implementation was once only possible and affordable for the largest of organisations due to the huge costs involved, the emergence of internet-based technologies such as *cloud data backups*, *cloud based disaster recovery as a service* and *managed security planning* have made it a standard practice for businesses of all sizes.

Business Continuity Planning is a critical business imperative because it deals with the unpredictable. It's very difficult to predict when a disaster is going to strike a business, be it natural, criminal or economic in nature. This is particularly the case for organisations that generate revenue primarily through network-based interactions with stakeholders such as customers, vendors and regulatory bodies. For very large organisations, even a few minutes of downtime can cost millions in lost revenue and reputational damage. For smaller organisations, a major business disruption can put them out of business permanently.

Case Study – WannaCry cyber attack hits the NHS in 2017

> *A cyber-attack known as the WannaCry hack went global in early 2017 shut down hundreds of thousands of computers worldwide, accompanied by messages from the criminals responsible demanding ransom payments for systems to be restored. A high-profile victim of the attack was the UK's National Health Service (NHS) that ended up having 200,000 of its computer systems locked out to hospital and GP users between 12 May and 19 May 2017. Although this only represented 1 per cent of all NHS services, the attack caused 19,000 appointments to be cancelled amount to lost revenue of 20 million pounds. It cost a further 72 million pounds over the longer term to restore the compromised computers systems and patch them against such an attack in the future. In the aftermath of the attack, the NHS was severely criticised for relying on the Windows XP operating system, which was 17 years old by that time, that was well known to be extremely vulnerable to all manner of cyber-attacks.* (ZDNET, October 12, 2018)

As the WannaCry cyber-attack against the NHS clearly shows, the loss of business continuity due to being vulnerable to or unprepared for an unexpected event can be very costly in monetary, reputational and human terms.

Business Continuity Planning

Business Continuity Plans (BCP) generally involve two things that are relevant to Information technology, these being *Incident Management and Risk Mitigation* and *Disaster Recovery*.

Incident Management and Risk Mitigation

Strategies for allowing the business to prevent risks from having a negative impact. Incident Management and Risk Mitigation plans must be designed and thoroughly tested to prove that they allow a rapid and effective response to a disruptive or destructive event in such a way as to mitigate and minimise risk. Such a planning will include all layers and units within the organisation and usually include management, HR, legal, IT, infosec and public relations.

Disaster Recovery

Strategies for allowing the business to respond and recover from an incident. Preferably in a way that allows the business to continue operations unhindered by rapidly restoring mission critical functions. Incidents may include cyberattack, natural disaster, power outages, terrorist attacks, and even civil unrest in some locations.

Very large organisations and government agencies are often required to make their ICT disaster recovery plans public as part of their obligations to stakeholders. For example, the Western Australian government has it Whole of Government ICT Disaster Recovery for Business Continuity Policy available for anyone to read at on its website.

High Availability

The concept of **high availability** refers to the ability of a system to remain accessible. *High Availability* systems are designed to minimize downtime and be resistant to incidents that may interrupt service. Many datacentre systems require high availability.

Common strategies to achieve high availability include:

- **Eliminating single points of failure**: - A single point of failure is any component of a business system that would result in service disruption were it to fail or otherwise become unavailable. It is therefore key to identify any such single points of failure with a business system and develop contingencies should it fail, e.g., building in a redundancy system.
- **Monitoring and detecting failures**: - Involves continuous monitoring of key business system components and assets to facilitate early detection of problems and that can then be responded to rapidly, or even pre-emptively. This is often achieved with network monitoring software tools such as those provided by Oracle and IBM.

- **Quickly recovering from failures**: - Involves putting system in place that allow failures to be recovered from as quickly as possible, and often without human intervention required. RAID systems and the redundancy / fault tolerance they provide in data storage system are a classic example of a rapid recovery from error technology.
- Load balancing to reduce the likelihood of oversaturation: - Load balancing involves efficiently distributing network traffic across a cluster of servers so that no server is either overloaded or underutilised. This is very important for the purposes of high availability because servers overloaded with network traffic are at a high risk of failing, and hence, causing a disruption in service. A load balancer mediates and routes client requests as evenly as possible across a server array so to maximises response times and minimise the possibility of server failure due to overloading.

Fault Tolerance

Fault Tolerance refers to the ability of a system to continue operating when sections of the system break and is a key part of any High Availability system. Nothing is completely fault tolerant, but some systems are more fault tolerant than others. A highly fault tolerant system may continue functioning perfectly after a failure. A less fault tolerant system may continue functioning but with reduced performance.

Fail Safe systems are designed to fail *gracefully*, that is to fail in a way that causes the least possible negative impact. For example, a system that fails without damaging anything or losing data and allows other systems to continue functioning while downtime occurs could be considered *Fail Safe*.

Examples of *fail safe* strategies in a datacentre may include:

Replication: - Having multiple identical systems or subsystems available and distributing processing load to then evenly in parallel so that if one system fails, the load can be recalculated and redistributed to the remaining operational systems.

Redundancy: - Having multiple identical instances of the same system and transferring processing to one of the remaining instances in the event of a failure. This is known as a *fail over* configuration. All implementations of RAID, except RAID 0, are examples of a fail safe fault-tolerant systems.

Fail Deadly systems are designed with the opposite purpose. To destroy data or cause damage at the first sign of tampering or failure. This is uncommon outside of military applications.

Fail Fast systems are designed to report errors at the first point of failure. It’s important to be able to detect failures early but some systems will only realise anything is wrong after other dependent components start to fail.

Redundancy and Failover

Redundancy is a method of achieving fault tolerance by having multiple devices that achieve the same purpose. If one device fails, a redundant device may take its place. This process is called **Failover**.

In a datacentre, many systems can (and often are) made with redundancy and failover in mind. For example:

Network Redundancy

Routers, Switches, Networking devices

Storage Redundancy

RAID, mirroring, ZFS, File Servers

Server Redundancy

Web servers, Database servers

Infrastructure Redundancy

Power/UPS, Cooling systems

Data Backup

Storage redundancy should not be confused with data backup. In the case of redundancy, if a physical storage device fails, another physical storage device can take its place without loss of data. In the case of data backup, a copy of the data exists *elsewhere* that can be restored should the original be lost, destroyed, deleted or corrupted.

Thus, it's very important to understand that redundancy strategies such as mirroring in a RAID array do not count as a backup. The fact is, that if a RAID completely fails, and no data backup exists, then total data loss will be the likely result. This is simply not tolerable in a datacentre context.

Data Recovery

When data loss occurs and there are no useable backups it can be very difficult to recover any lost data. Data recovery can be very expensive and sometimes impossible depending on the storage media. Deleted files can sometimes be recovered through file carving and digital forensics techniques. Disk forensics can take a significant amount of time as well as money.

Backup Strategies

Backups are for responding to a data loss event. When a storage pool is destroyed, or someone accidentally deletes a production database, failover and redundancy won't help. Changes to the data will be replicated in redundant systems and will not be recoverable without some form of backup.

Full System Imaging

A full system image stores an exact, complete copy of an entire volume. Good for making standardized images of known good configurations. Very large storage requirements. Data that has not changed between backups will be duplicated. Not good for data that is likely to change regularly.

Incremental Backups

Incremental backups store the differences between the current state and previous backups. Full backups are taken periodically and incremental backups store only the data that has changed. No duplication of identical data means smaller storage requirements. Better for data that will have many small changes over time. Can take a long time to restore depending on time since the last full back up as increments must be applied one at a time.

Differential Backups

Differential backups store the differences between the current state and previous Full backup. Similar advantages to an incremental backup strategy but faster to recover due to only needing two sources of backed up data (the last full and the differential).

Reverse Delta

Reverse Delta Backups keep a complete current system image. When a new incremental backup occurs, rather than storing the new changes, the full backup image is updated, and the difference data is stored to recreate the older version. This improves the time to restore the latest backup, while older backups will take longer as the deltas will need to be applied to recover previous data states. Reverse Delta is recommended for large files that change often, such as Outlook PST files or database backup files. However, when older versions of files will need to regularly be accessed and restored quickly, the Reverse Delta method is not advised.

Storage Locations

Where to store backups becomes an important issue. If your backups are stored in the same location as your live data, some causes of data loss could affect both your live and backup storage. On-Site storage can still be useful for backups but care should be taken to separate backup media from live media. Off-Site backups located in geographically distinct locations are more resilient though may be less economical.

Active storage such as a separate SAN or a tape library is convenient and relatively fast to recover. However, active storage can be vulnerable to data loss due to incidents such as disk failure or accidental deletion. Offline storage such as tapes or optical disks can be more resilient to such failures but can take longer to recover. Additionally, optical disks or solid-state storage tend to be relatively low capacity which may be an issue for large scale backups.

Remote Backup Services

Cloud backup services are becoming increasingly popular as a cheap and comparatively safe alternative to on-site backups. As internet speeds increase it has become progressively more viable to backup large amounts of data through the internet.

Backing up over the internet is generally much slower than an on-site backup. Security of backups can be an issue as a large amount of trust in your cloud provider is required.

There are many cloud backup service providers suitable for enterprises to use, including:

- Acronis
- Arcserve
- Cohesity
- Commvault
- IBM
- Rubrik
- Veritas

Datacentre Security

Like most Computer Security related topics, datacentre security is concerned with protecting **Confidentiality, Integrity and Availability (CIA)**.

Security protections for datacentres tend to be split into two major aspects:

1. **Physical Security**: Concerned with protecting the physical assets of the datacentre and controlling physical access to devices and infrastructure.
2. **Network Security**: Concerned with protecting the network from intrusion and controlling access to network resources and administration interfaces.

Physical Security

Physical Access control is vital to maintaining datacentre security.

- Datacentres are usually monitored 24/7 with cameras and temperature sensors.
- Single-person access can used to restrict critical areas to only the technicians that need to access them.
- ID cards and locked doors requiring authentication.
- Biometric security as multi-factor authentication.
- Physical construction of walls, floors, roofs, fences and doors built to resist physical intrusion.

Network Security

Network security is also a critical aspect of datacentre design.

- Firewalls
- Intrusion Detection Systems/Intrusion Prevention Systems
- Isolating security zones and splitting the network into manageable sections
- Data encryption for information transfers
- Server update policies
- Regular testing and scanning for application vulnerabilities
- Consolidating network security information into centrally monitorable systems

References

ZDNET. (2018). *This is how much the WannaCry ransomware attack cost the NHS*. https://www.zdnet.com/article/this-is-how-much-the-wannacry-ransomware-attack-cost-the-nhs/