**D1 – Disaster Recovery**

Disaster recovery is the process of recovering from a disaster that has affected a system, from a crash to full destruction of hardware and other infrastructure.  
Most disaster recovery revolves around protocols that are already in place in case of such an event, but it can be possible to recover even without preparation.

**Backups**Backups are the first line of defence against disasters of all kinds. A backup is a redundant but up-to-date copy of data. This could be important files or directories, or a copy of the entire system. Most systems back up data on a regular basis – this may be a fixed schedule, such as once a night, or be event-driven, only backing up when a certain condition is met, such as a certain amount of data being modified.  
When a disaster happens, such as accidentally deleting data or the hard drives failing, then the backups can be used to restore it. Systems that use the hard drives a lot will need more regular backups, otherwise data that was changed between the last backup and a disaster will be lost.

**Redundant Hardware**  
Some disasters only affect a piece of hardware or single machine, as opposed to the whole system. Redundancy is used to protect against this kind of disaster.  
Redundant hardware is hardware that is not strictly necessary, but is there to ensure the system continues to function even if something fails. An example of this would be having an extra power supply in a machine. If the main power supply fails, the redundant one can take over and the machine will continue to run, so they system stays up.  
Redundancy can be applied to all aspects of computing. A RAID hard drive configuration uses multiple drives to keep real-time backups of entire systems. For large datacentres, such as those used by google, redundancy is achieved through distribution – that is, designing the system so that nothing is dependent on a single piece of hardware. If something fails, another server will take over while the problem is fixed. If an entire one of Google’s (or most cloud service based companies) data centres was destroyed, most users wouldn’t even notice a drop in performance, as everything would be re-routed to compensate for the disaster.  
This is the principle the internet was built on – in the 1960’s, during the Cold War, computers were becoming important for military purposes, such as guiding missiles and communication. The engineers and technicians decided to link all of the military computers and distribute important data across them, so that of one was destroyed, nothing would be lost and communication could be achieved by routing around destroyed nodes (components of the network). This network was called ARPAnet, and was the precursor to the internet.

**Recovery without preparation**Some disasters are impossible to recover from without preparation, particularly those that involve the destruction of hardware. However, one of the most common disasters – accidentally deleting data – is possible to recover from. In most cases, when data is deleted, it is not actually gone. Instead, the space it occupies on the drive is marked as free, so that it can be written over when new data is saved. Specialised software can read this space and re-write the data.