VENOM·IT

Business Continuity VS Disaster Recovery

Business Continuity

Disaster Recovery

Definition

Is the long-term plan of action to ensure stability in your organisation before, during and after disruption or disaster.

Is the strategy to reduce the impact of a disaster and the recovery of critical IT systems.

Business Aspects

There are 3 main types of risk:

1) Risks that can be avoided completely

2) Risks that cannot be avoided but can be mitigated to a greater or lesser degree

3) Risks that cannot be avoided or even mitigated, and need to be dealt with as and when they happen

BC is more strategic, and looks at sorting and prioritising risks, and pre-emptively avoiding or reducing risks.

Disaster recovery is the ability to solve the problem and get your business back on track as quickly as possible. It focuses on technology and your IT systems.

Disaster recovery plans usually include a 'playbook' of specific actions or step-by-step procedures to initiate under specific circumstances.

DR leans more towards handling risks that could only be mitigated (e.g. DDoS attacks, or nation-state attacks) or those that cannot be avoided at all (e.g. flooding or fire).

Risk Factors

Cyber Security

The world we live in today is filled with cyberattacks that are well documented in the media. Large organisations have experienced well-publicised breaches in their servers over the past few years.

Theft of data

The increase in remote working has resulted in a lot of sensitive corporate data being accessed from employees' personal devices which can be 'accidentally' shared or accessed by unwanted parties.

Physical Security

The general rule is to know what you've got! You can't secure something you don't know you have. From video surveillance to fire alarms – you need to fully know your physical security system. If disaster strikes, it's important to check and test all physical securities are future proof.

Viruses

The most common culprit behind massive data loss remains viruses from an email. Having data backups is crucial in this sense. That way, you can at least ensure you have data recovery systems capable of restoring any lost or compromised data.

Economic and Financial Risks

675,000 businesses have fallen victim to fake invoice fraud in the UK*. Businesses need to raise their standards in their financial risks to put in place policies, tools and systems to enable business continuity following large-scale data theft or loss.

Malware and Ransome

Malware is growing year-on-year and can affect systems, backups and storage. Should an organisation be subject to ransomware, one decision a company must make is whether to pay the ransom. Many cyber insurance companies will cover this cost but is this questionable in ethics?

Compliance

Compliance and risk systems are often deprioritised within the business continuity plan. However, industry regulators are now fining companies for non-compliance, regardless of the disruption and costs that organisations are already facing.

Cyber-attacks

Identify what is lost and the extent of the damage. What was attacked, which controls failed? A post-incident report will expose the root cause, what was affected, and the extent of the damage. This will ensure no other vulnerabilities are at risk.

Unsecure networks

Unsecure networks often lack any sort of protection and any information transmitted across the network is unencrypted for someone to hack. Should your system be attacked on an unsecure network, the main aim is to ensure that a network is restored to its normal state as rapidly as possible.

Natural disasters and pandemics

Fire, floods, COVID; all should have a backup plan to recovery. Whether that's a remote desktop, a cloud backup or a virtual machine to work on. Your natural disaster recovery plan should be updated, practiced, and tested regularly.

Accidental deletion of data

We've all been there. Most cloud storage systems will back this up as well as virtual machines giving you a machine's entire configuration state, which can be reverted back to if needed.

Reputation

By having documented disaster recovery plans during the recovery process, it is easier for an organisation to manage user sentiments during a hacking incident.

Complacency

Businesses in the UK are showing an "alarming level of complacency" when it comes to business continuity planning.* IT failure is the issue most likely to impact future costs, followed by telecoms failure, and the loss of access to work sites.

Human error

Is responsible for up to 47% of major IT disaster recovery mistakes. Your employees are your first line of defence, yet many companies fail to train their staff in their security responsibilities.