STANDBY Consulting (ME) Limited

IT RESILIENCE AND CYBER SECURITY

Improving Your IT Resilience

Most organisations nowadays are heavily dependent on uninterrupted Information Technology (IT) operations, but with this dependence also comes significant vulnerabilities.

Failure of IT systems is often quickly obvious to the organisations stakeholders or clients and the willingness to accept outages has lessened significantly over time. Organisations must now have plans and procedures in place to minimise the impact of any IT outage.

IT Disaster Recovery (DR) planning is about business survival; providing the process, policies and procedures that will help to keep your IT infrastructure running, even in the face of adversity.

IT DR is a subset of the much larger process, Business Continuity Management (BCM) and should therefore incorporate planning for resumption of hardware, communications (such as networks), applications, data and other IT infrastructure.

The creation and maintenance of a sound IT DR Plan is a complex undertaking, usually involving the following steps:

- ✓ Risk Evaluation
- ✓ Business Impact Analysis
- ✓ Strategy Development
- ✓ Disaster Recovery Plan (DRP) development
- ✓ Fail over testing
- ✓ Plan Maintenance.

Cyber Breach Management

Cyber-attacks are now a very viable and dangerous threat to all organisations and it is becoming increasingly difficult to stay ahead of the game in defence of your IT systems. It is generally felt that a cyber breach is now only a matter of **WHEN and not IF** for most organisations.

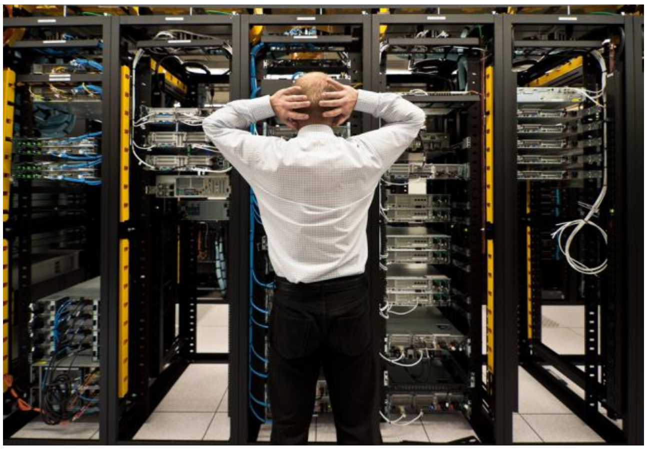
Effective DR planning and subsequent Cyber Breach Response planning are vital ways to help your organisation effectively manage any breach and not allow an attack to cause significant and lasting damage.

Advantages of Disaster Recovery and Cyber Breach Planning

The key objective of DR and Cyber Breach Planning is to minimise the impact of an IT crisis event or outage on your business.

The advantages can be numerous, touching on many aspects of the business including:

- ✓ Provides capability to maintain or resume operational trading
- ✓ Minimises downtime
- ✓ Increases confidence of business associates, shareholders, stakeholders, clients and regulators
- ✓ Prevents loss of customers to competitors due to inability to trade
- ✓ Safeguards against business reputation, brand and image
- ✓ Lessens the cost of recovery and risk of business survival than if your organisation doesn’t have a plan.
- ✓ Organisation effectively manage any breach and not allow an attack to cause significant and lasting damage.



A well developed and up to date Disaster Recovery and Cyber Breach Response Plan could mean the difference between the closure of your organization or its survival