

IT disaster recovery

The use of IT is ever more prevalent in today's global marketplace; therefore IT disaster recovery is a high priority for an organisations corporate plan

Technological advances in ERP and web-based procurement systems have provided the tools for Purchase and Supply Management (P&SM) professionals to consolidate information, reduce costs and increase service by building end to end purchase to pay systems.

What is disaster recovery?

Also known as Business Continuity Planning (BCP), it is the methodology used to plan for business practises to resume as much as possible following a disaster or disruption.

The booklet *Expecting the Unexpected*, jointly published by the police National Counter Terrorism Security Office, London First and the Business Continuity Institute, outlines five steps that you can follow to develop a business continuity plan:

1. **Analyse your business.** Working with the full support of senior management, you need to understand your business and the way it works, including which functions are essential and where vulnerabilities lie.
2. **Assess the risks.** You need to understand what emergencies might affect your business and what impact they would have. By focusing on impacts rather than causes, you will make sure your plan allows you to deal effectively with an incident, no matter what the source.
3. **Develop your strategy.** You will need to agree with senior management the organisation's appetite for risk. You can then decide which risks can be accepted, which risks can be reduced and which risks should be managed using business continuity planning.
4. **Develop your plan.** You should then develop a business continuity plan covering the agreed areas. All plans look different, but they should be clear about roles and responsibilities, easy to understand and open for consultation and review around your organisation.

5. **Rehearse your plan.** Rehearsal helps you to confirm that your plan will be connected and robust if ever you need it. Rehearsals are also a good way to train staff who have business continuity management responsibilities. Lessons from exercises can be used to refine your decisions in steps one to four.



e-attack

BCP plans can not remain static, modern risks over the past 10+ years have included terrorism, chemical attacks, global warming and electronic-attacks (e-attacks). e-attacks can come in a variety of forms, from hackers, malicious software attacks (virus), terrorists, or foreign intelligence services. As business moves into global marketplaces and information and technology is outsourced or offshored the risks increase further.

An e-attack could potentially

- Expose confidential information of which you could have a duty of care or legal obligation to protect
- Allow others to gain access to your computer system to make amendments, deletions
- Make systems impossible to use, known as a denial of service.

Some risks are more difficult to pre-empt, 9-11, foot and mouth, MRSA and Sars for example could not have been easily anticipated. What will be the next emergent risk? The challenge is for BCP teams to regularly meet in an attempt to identify future risks. Workshops, brainstorming, interviews, and reviewing current and historical data are some of the ways in which we can attempt to predict the future.

Most recently mobile short message service (SMS) have been targeted. The new threat dubbed 'SMiShing' is currently targeting the consumer market directing mobile users to a website in order to cancel a subscription. Fearful of incurring premium rates consumers are navigated to a website to download a program which is actually a virus allowing the hackers to gain access to their system. Many organisations now provide mobile phones to their employees, some of which use them to access their e-mail or shared network. Trends such as this should be used to anticipate the impact on the business environment.

What can you do?

MI5 recommend the following general countermeasures that will considerably reduce the chances of a successful attack against your information systems.

- Acquire your systems from reputable manufacturers and suppliers

IT disaster recovery

The use of IT is ever more prevalent in today's global marketplace; therefore IT disaster recovery is a high priority for an organisations corporate plan

- Ensure your software is as up to date as possible
- Ensure internet connections are equipped with anti-virus software
- Information is regularly backed-up, a copy should be kept in another location
- Make certain that all those operating, maintaining and guarding your systems are reliable and honest
- Seek security advice from system and service providers and act upon it
- Use encryption packages for highly confidential material
- Implement a program of security awareness amongst staff and train them on a regular basis
- Invest in security cabinets and firm locking doors
- Dispose of confidential material in an appropriate manner¹.

Written by Emma Brooks, Professional Practice Team, CIPS

¹ *Adapted from M15 IT security advice <http://mi5.gov.uk>*