



Ref No P0903

November 2003

Telecommunications and Business Continuity.

With the ever-increasing pace of commercial activity, the reliance by modern corporate organizations on an efficient telecommunication service becomes crucial. Although much attention has been given to disaster recovery planning for mainframe data centres, most organizations have still not implemented telecommunication service recovery plans.

As information is passed round the world ever faster and in forms available to more and more people, sudden loss of this contact can be devastating in terms of financial exposure or potential missed business opportunity.

Developing corporate reliance based on continuous availability of these telecommunication systems, together with potential client access, requires special plans to be developed for protecting services, particularly when unexpected events threaten the business.

- **The Corporate Network**

Most large global organizations now operate some form of international voice and data network. When these are planned, it is essential that consideration be given to methods of protecting the network from unauthorised access.

At the physical level, this means that all critical network equipment should be located in secure locations. It is essential to provide suitable stable environmental conditions and to control temperature, airflow and electrical stability.

Extra reliability can be achieved with the provision of uninterruptible power supplies (UPS), isolated grounding, water detection and good electromagnetic screening. Consideration should be given to the need for transient overvoltage protection from lighting and other high power sources. It is important to make frequent back-ups of configuration records which should be stored remotely from the main site.

At the terminal access level, such techniques as password protection and virus checking should always be implemented. Once data is passed to the network, all sorts of route diversity and error correction can be built into the system. In extreme cases, encryption can be used, although this can imply both a cost and performance penalty.

- **Outsourcing**

The current trend to 'outsource' the management and maintenance of corporate network services should be carefully evaluated with regard to business continuity. There needs to be complete confidence that the contracting external organization will provide the same level of security and resilience in handling corporate confidential information as would be expected from in-house staff.

Complete checks in this area should be conducted before handing over the responsibility for the networking to an external organization. In addition, it is wise to check on what their Business Continuity plans are in the event of a disaster.

- **Phone Hacking**

As telecommunication expenditure rises, so does corporate vulnerability to serious fraud. Increased complexity of company telephone systems, with services such as voicemail and wireless access, increase the chance of undesirable access to the system and the potential for catastrophic financial loss. The era of hackers accessing private phone systems for 'fun' has passed and attacks are now more commercially motivated.

In North America, there is a thriving industry in corporate phone hacking and even organizations such as many Metropolitan Police Forces have suffered major unauthorized access to their phone systems at the hand of hackers. Another organization reportedly encountered over \$500,000 worth of illegal calls in one weekend!

- **The Internet**

There is now widespread personal and corporate use of the Internet. Extreme care should be taken in how the corporate network is connected to the Internet.

This is not only because personal message transmissions are inherently at risk and may be intercepted but also, the fact that it is possible to load screen messages with 'embedded code' programs. The user can innocently appear to access an interesting page which in turn loads in an unchecked program. This is very similar to loading a virus from a floppy disc except that potentially, it now has access to the whole corporate network.

Devices known as firewalls can be incorporated into the entry point of the corporate network to provide checking and protection to reduce the likelihood of such events.

- **Public Network Providers**

Public Network Operators tend to have special plans in place to protect their own networks in the event of major national disasters, although often, some disruption to service may be encountered by the local user. However, one aspect that is often overlooked is the access point into the client's location.

Ideally there should be at least two separate physical points of entry into critical buildings so that service can be provided over two completely separate physical routes. This type of diversity should, where possible, also be extended back to two local phone exchanges so that complete resilience of service is available to the end users.

Ref No P0903

November 2003