

The changing face of business continuity

David Honour overviews the new generation technologies that will influence business continuity planning in the future.

Approaches to business continuity have changed dramatically over the past few years. High availability techniques, coupled with real-time data replication and system failover, have meant that many business continuity planners have built these elements into their plans as a first response to downtime, with disaster recovery being down-graded to a mechanism of last-resort. However, various new technologies could create a revolution in business continuity planning which will dwarf the impact of the above methods.

The first major change that is taking place is actually one of approach, rather than technology, but it is important to examine it in the context of this article, since it will set the foundation for the way business continuity is implemented throughout an organisation's IT and communications networks. The change in question is the move towards holistic business continuity management.

In tomorrow's organisation business continuity will no longer sit in its own 'silo', separated from IT disciplines; information security management; operational risk management; crisis communications; emergency planning etc (delete as appropriate for your organisation!) A movement is underway to bring all business protection issues under one umbrella, ensuring effective oversight of all mission critical processes, giving transparent insight into all areas of the organisation and allowing effective continuity management. This approach is driven by two main factors. Firstly: it makes sense from a management and resource allocation point of view - in too many organisations vital mission critical risks go unmitigated because separate departments all think that the threat is being handled by someone else. Secondly the convergence of information and communications technologies means that it is really the *only* practical way forward.

This point was forcibly made by Computer Associates' senior vice president and chief security strategist Ron Moritz, speaking at last year's RSA conference in the US. Moritz called for an end to the current fragmented approaches to access, authentication and auditing operations and stressed the need for total security management across IT and facilities systems in order to enhance responsiveness to new threats. Moritz suggested the convergence of responsibilities under the chief security officer (CSO), including business continuity, privacy controls, regulatory compliance and antiterrorism activities.

Convergence

The convergence of information technology and communications has been talked about for many years but is really only now becoming a reality for most businesses. Research and development into IP (Internet Protocol) is now bearing real fruit, with many companies now looking to implement Voice over IP (VoIP) communications networks. Additionally, IP-based Storage Area Networks and IP-based Wide Area Networks are really opening up the possibilities for new, highly resilient and cost-effective business continuity networks:

* VoIP – This was seen initially by many as a business continuity risk, since it moves telecoms into the same arena as IT systems, thereby opening up telecoms networks to new threats. However, more organisations are starting to see that VoIP also brings risk mitigation benefits. Telecoms can now benefit from all the failover techniques enjoyed by IT systems, making communications high availability a reality.

* IP-based Storage Area Networks – Such networks mean that company data storage can be centralised, offering more control over IT policies and procedures, but also over backup, recovery and availability methods. Data stored at a data centre is accessed via the IP network, meaning

that it is continuously available from any location, worldwide. The fact that data is centralised makes it much easier to ensure protection and availability of the data – one data continuity plan is required for protection of the data centre rather than many plans to protect data held in diverse locations, as was previously the case.

* IP-based Wide Area Networks – These offer the advantage of network resilience. Data replication and failover is no longer restricted by distance, allowing recovery facilities to be based as far away as separate continents for the ultimate in protection. This has a major benefit should a wide-area disaster occur.

Self healing networks

This future technology is being led by IBM, through its IBM autonomic computing initiative (previously known as Project eLiza.) IBM's vision is to develop self managing computer systems, which act in a similar fashion to the human autonomic nervous system – continually working in the background to ensure health and survival. IBM has identified four key characteristics which should be evident in all self-managing computing systems. These are:

- *Self-configuring*
Systems which are able to dynamically adapt to changing environments;
- *Self-healing*
Systems which can discover problems at their outset, and can then diagnose, opt for a solution and act to 'heal' the disorder;
- *Self-optimising*
Systems which can continually tune resources and balance workloads to maximise the use of IT resources;
- *Self-protecting*
Systems which can anticipate, detect, identify and protect against attacks.

In terms of handling day-to-day computer and network availability issues autonomic computing will really make business continuity an automatic process and, even when systems are threatened by a larger crisis, the intelligence and automation built into such 'intelligent' networks will help to make failover and disaster recovery much quicker and more efficient. Autonomic computing will help make true business continuity management a reality rather than the pipe-dream that it is today.

Grid computing

Sun is one company taking a lead in the grid computing arena through its N1 strategy. Basically, Sun's aim is to develop solutions which will allow 'n' number of computers to be managed as one single entity. Grid computing treats individual machines as one element of a larger super computer, allowing enhanced power for highly complex computations. It also potentially allows for the ultimate in high availability with the grid 'computer' not dependent on any single machine or location. This makes the system as a whole much more resilient and, although local nodes may be impacted by local crises, the whole system is impervious to all but a cataclysmic disaster. For the large multinational company grid computing is likely to be the future for data centre operations. While individual offices will still require conventional disaster recovery for their power supply, their fixed communications and their people, the need for data protection and recovery will be removed.

Utility computing

In utility computing enterprises treat computing resources in a similar way as any other utilities, such as power, the public telephone system, water, gas etc. The computing utility provider offers the service – such as applications provision or data storage and backup for example - and bears the responsibility for the availability of that service. This is significant to the business continuity arena in a number of ways. Firstly, the onus is on the utility computing suppliers to ensure that the applications being utilised are always the latest version, with the latest vulnerability patches installed. This should increase the overall quality of the software being used across enterprises and takes away the headache of patch management.

Utility computing should also result in a sharing of the business continuity burden, since the utility provider will have a reputational requirement and a contractual duty to ensure that the services provided are highly available and protected by strong business continuity measures.

Ten years time – the ultimate system?

The above developments are operable now, even if some are still in the testing stage. The next couple of years should see all of these becoming mainstream elements of company IT, but what of the longer term future? Many of today's technologies were pipe dreams ten years ago. Which of today's dreams will become reality?

The biggest change may be the privatisation of the Internet. Enterprises may have their own 'IP Sphere', within which sits most of the data and applications that the enterprise requires. This will essentially be an externalisation of today's Intranets with enterprises utilising Internet nodal points around the world to manage and operate their own private Internet. Gateways will be maintained to the public Internet but these will be well protected by enterprise firewalls and intelligent virus and content protection applications. Computers within the IP Sphere will no longer require their own protection. This will ensure that all machines operated by the enterprise will always adhere to IT protection and security policies.

Within the IP Sphere the enterprise will connect all its machines together in a grid, to ensure maximum manageability and control as well as extreme resilience of the network as a whole.

Both enterprise servers and individual machines down to desktop level will all benefit from autonomic technologies, resulting in maximum uptime. All applications will be operated across the IP Sphere from a central enterprise application hub, based on the utility computing mode. All data will be stored on an IP-Storage Area Network, again contained within the IP Sphere.

Telecommunications will use VoIP through the IP Sphere, with voice links to the external public Internet again strongly protected by intelligent firewalls which, as well as blocking VoIP spam, viruses and other threats, will continuously scan the content of voice calls, immediately blocking conversations which do not match the profile of allowable voice calls, as set out in the corporate communications policy.

Finally, enterprise services will be operated from a central data centre, which will be supported by a secondary mirrored data centre located many miles from the primary data centre, providing a final tier of resilience against major disaster.