The Resilience Challenge

By Steve Yates, FBCI, FICPEM, MEPS

Today, national and international network providers offer a wide range of individual or integrated communication network services delivered via complex multiple inter-linked systems. It is at the physical network layer that there is probably the greatest challenge when using multiple network providers to each deliver what may be part of a complete service. This is especially true when an outage could impact one or multiple integrated communication network service providers.

Under normal circumstances, a network outage may start out as just an annoyance, depending on the time of day, month or year. Without adequate resilient protection mechanisms in place, the impact of a major or even minor outage can quickly spread exponentially through a network, leading to a serious or, in the worst case, total degradation or failure of service. Such outages may be caused by anything from a software problem to a catastrophic failure of all network services. Problems can get worse when people re-dial calls during outages or network congestion.

A realistic risk assessment of corporate telecommunications systems should see the 80/20 rule at work, where 20% of high-risk and mission-critical systems require 80% of the available resources. It is therefore critical for your organisation to recognise which communications system(s) and/or circuit(s) need 100% availability, and to plan for specific resilience measures to ensure that outcome.

Any organisation seeking to protect itself by providing specific resilience measures must be prepared to invest time and resource into due diligence activities, thus ensuring an acceptable level of service assurance. This investment must also be viewed over the life cycle of each service, taking into account changing technology and ongoing business requirements. These kinds of preparations can ensure that resilience is maintained during an operational reorganization or service disruption.

Goals for Delivering Resilient Services

First, it is necessary to define service objectives. For some organisations this may be quite difficult, especially those operating in multiple business areas, with distributed management responsibility. Consider the following resilience statements, determine where they would fit into your corporate culture, and evaluate each one against your "high risk or business critical" elements.

"Resilience is the ability of an organisation, staff, system, network, activity or process to absorb the impact of a business interruption, disruption and/or loss while continuing to provide a minimum acceptable level of service."

Source: Scottish Executive

"Resilience is the ability of a network to withstand internal failures and external events at best without affecting traffic or at worst with a manageable reduction in service level."

Source: Ireland - Office of the Director of Telecommunication Regulation

Although both descriptions may seem acceptable, note that unless your organisation is prepared to separate and duplicate all network service and technology elements, both internally and externally, across multiple sites; then at some time there will be a service outage. It is inevitable. The challenge is therefore to ensure that your organisation is able:

"To resist and tolerate failure, and recover critical communication elements within a business acceptable time-scale by planning and design."

Source: Survive! The Business Continuity Group - Communications Special Interest Group

Whichever description best meets the needs of your organisation, you must be able to manage the changing "business" environment throughout the life cycle of the resilient service. We must therefore view this subject matter inside as well as out, reminding ourselves that:

"Change is everywhere today. Major change is occurring in almost every aspect of people's personal and work lives. That change is not just technological. Change has affected how people interact with each other. It has affected the policies and regulations that guide their work. Many industries have experienced structural changes that are now impacting how business is done. There are many value and ethical questions that these changes are creating. In the midst of all this change, many people are asking themselves, "What are we to do?" They often feel overwhelmed because they feel that what they always depended upon to be true, no longer is."

Source: Sharon M Danes, Ph.D., University of Minnesota

When technology that supports the "services behind the services" decides to fail, you can expect to be overwhelmed. So when considering a resilient service you should begin by establishing a partnership with your network provider.

Building a Resilient Network

As with most complex issues, the KISS rule would seem the best way to move forward. Therefore, one approach for building a resilient network infrastructure involves following the 7 R's:

1. **Review** - Identify risks to communication networks. Audit the network by establishing a Resilience Program Team, comprised of relevant experts, and using schematics of network routing/cabling and system connectivity; provision, maintenance and service level agreements (SLAs); change management, contingency and emergency procedures;
2. **Risk** – Determine an acceptable level of risk by conducting a risk analysis of physical and logical network components, especially internal and external, high-risk and mission-critical systems;
3. **Redundancy** – Determine which critical communication elements need full redundancy by conducting a business impact (what if) analysis, reviewing both internal and external information regarding network design, the network provider, and the network and system-level resources needed for redundancy;
4. **Resiliency** – Determine what resilient means, and its value to the organisation; determine the cost for a truly resilient solution; perform a business case analysis;
5. **Recoverability** – Determine how quickly mission-critical infrastructure elements must be recovered; do the same for non-critical communications assets; develop contingency plans for those assets where no resiliency can be provided; once recovery time frames have been identified, establish service level

agreements with equipment and network service providers, and establish command and control procedures to manage recovery;

6. **Restoration** – Determine the amount of time needed to restore full network operations; as needed, activate contingency plans to restore services within acceptable time frames; ensure that management is aware of and have agreed on the proposed restoration time frames;
7. **Responsibility** – Identify who is responsible for delivering network resilience; establish a Resilience Program Team that includes internal staff and vendor representatives; secure agreement on resilience life cycle elements, including change management;

A Real World Example

An example of how resilient networks on a large scale are developed can be found in the results of a project carried out by the Lower Manhattan Telecom Users' Working Group, following the September 11, 2001 attacks. The group published a report that described a number of strategies for building a resilient and survivable network infrastructure for lower Manhattan.

Summary

Where communications are critical to business, or constitute a high business risk if they are disrupted, then your organisation must be prepared to invest time and resources to obtain an acceptable level of service assurance. A key part of this process is the identification of business services that require special attention. So, are you ready to accept the challenge?