1. WHAT IS THE FUTURE FOR ORGANISATIONS WHOSE NETWORK INFRASTRUCTURE IS NOT RESILIENT?

1.1 Will Resilient Businesses be the Market Leaders in the 21st Century?

For many years, there has been considerable activity in the usage of communications products and services, leading to the development of even more sophisticated networks & technologies that are now an indispensable part of our daily life. Such sophistication has meant that if there is any *"unplanned outage"* the impact and subsequent disruption is significantly greater.

There are many documented examples of *"communications outages"* with each one having the possibility of causing major impacts on the day-to-day running of an organisation and/or community that has been affected.

Sometimes those organisations and individuals who are involved come out of the experience with an enhanced reputation and with little detrimental effect to the business. In 80% of other cases, the company does not survive. A *"business disaster"* is described as being:

"Any unwanted significant incident that threatens personnel, buildings and/or the operational effectiveness of an organisation, which requires special measures to be taken to restore the business back to normal".

(source: Home Office - How Resilient is your Business to a Disaster)

Such organisations have pursued a *"stack-it-high, sell-it-cheap"* approach, dependency on *"sophisticated communications"* products and services to survive in a competitive market, and as such have have, in the main, not planned for a *"business disaster".* This *"denial"* approach, following a disaster will obviously impact on the *"customers"* for their products and/or services.

This growth has led to the development of even more sophisticated networks & technologies to meet the needs of our need for faster communications that have become indispensable as part of our daily life.

What are these *"unwanted significant incidents",* and how would they impact on your business? The following provide are examples for you to consider:

a) Human error;

- Lapse of security
- Misunderstanding of directions
- Carelessness
- Pressure of home and/or work
- Stress related
- Accidental damage

b) Natural causes;
- Fire
- Flood
- Lightning
- Solar flare
- Tornado
- Hurricane

c) Intentional causes;
- Terrorism
- Vandalism
- Industrial action
- Espionage
- Computer viruses
- Fraud

For each of these categories there are many more examples that could be listed and classified as a *"business disaster"***,** all requiring *"special measures to restore business back to normal",* when there has been a significant:

a) loss of operating capacity;
b) loss of capital or profits;
c) loss of market share;
d) loss of credibility and/or image; and,
e) impact on compliance with legislation or codes of practice.

How can we reduce the cost and impact on a company following a *"business disaster",* whilst at the same time delivering the product and/or service that will retain **"customer loyalty",** *"before, during and after a disaster?"*

2. HOW THEN CAN YOUR COMPANY BECOME RESILIENT TO A BUSINESS DISASTER?

2.1 Dictionary Definition of Resilient

As we move forward into the 21st Century, there is now a need to develop a *"business resilient"* culture that will build resilience into processes and procedures, and guarantee the *"continuance"* of business activities.

The nearest dictionary definition for Resilient is one for a ***"resilient object"***, something which is:

"capable of regaining its original shape or position after bending, stretching, or other deformation"

(source: The New Collins Concise Dictionary - The Guild Publishing London)

However, what if the object is a physical fibre optic cable that provides critical communications to your company, or a data processing system that supports critical business-wide applications and services. Such elements do not easily bend or stretch to any great degree, and would certainly take exception to being deformed!

2.2 What is the key to becoming a Resilient Company?

A key factor in reducing the cost and impact to the operational structure of a company, following a *"business disaster",* would be to have a ***"resilient communications".*** What does resilient really mean when applied to communications, and how will it assist in the *"before, during and after"* a disaster?

Perhaps then a better definition of a resilient company, is one that accepts the fact that processes and procedures, and the supporting technology, will at some time fail, and accepts the need to:

"resist and tolerate failure, and recover critical operational elements within a business acceptable time scale by planning and design"

(source: Survive! The Business Continuity Group - Communications Special Interest Group)

Having a strategic approach to resilience could be the *"key"* to your company preventing, and if necessary managing, a ***"business disaster".*** This strategy should not only include the service infrastructure and associated technology, but also establish a state of *"readiness"* should a disaster happen. This begins from the management of business changes through to establishing a response to any *"crisis"* situation.

3. WHAT IS THE RESILIENT COMMUNICATION STRATEGIC APPROACH?

3.1 Preparation Phase

The Preparation Phase should begin with the identification of risks to critical components. This could be prior to implementing new, or changing existing communications technologies. In both cases the areas for consideration are similar, and relate to the risk of ***"poor"*** **-**

a) planning & design;
b) manufacture;
c) installation; and/or
d) maintenance**.**

The key question that any company should ask itself is:

"How long can your Business survive without critical communications"

The ***"counter-risk"*** strategy should be to establish a company policy that covers, not only purchase of external products & services, but also their selection and project management. This transforms into detailing the business requirements for resilience, and by ensuring that within any *"Invitation to Tender"* (ITT) document the equipment manufacturer, supplier, maintainer and network provider are made fully aware of the business requirements:

a) project management process;
b) reference sites;
c) resilient connectivity;
d) emergency management processes & procedures; and,
e) disaster recovery services offered.

Obviously the ideal situation is one where all interested parties work together to highlight a resilient solution, before there is any impact on business operations. To achieve this the *"resilience project sponsor"* must agree an acceptable ***"down time",*** not only for the communications network but also when it is customer affecting.

3.2 Planning Phase

The Planning Phase should embrace and provide key resilience enablers arising from the physical separation of complementary technologies and creation of a *"contingency"* capability. Therefore, the basic principle should therefore be to provide in-built protection within any sophisticated communications structure, and provide standby options during failure conditions. This can be achieved by understanding the physical and logical elements of the communication technology being implemented or in use.

Plans must also be put-in place that will safeguard the communications technology, either terminating directly on the network or working independently. Such *"contingency"* plans can either be implemented automatically using the in-built capability of the technology and/or involve invocation with a *"disaster recovery"* supplier.

Following the moment when a real *"business disaster"* occurs there will be a period when the company will need to assess any *"damage"* that has taken place. During this time telephone calls and facsimile transmissions may be left unanswered, e-mails not responded to, post not collected, letters not responded to, and suppliers left awaiting payment. There will be many other areas where communications are left wanting, dependent on the maturity of the market and *"sophistication"* of technology being used.

At some point, only you will be able to judge when this has occurred, the situation deteriorates to a level where there is a major impact on business activities. This impact is easier to assess when physical damage has occurred to the building or technology. In the case of *"product contamination",* communications to the media become a high priority. Many examples exist where a *"business disaster"* has affected the integrity of the company, and where a *"crisis management plan"* has been invoked.

4. WHERE IS BUSINESS TODAY IN PROVIDING RESILIENT COMMUNICATIONS?

Most business operations want to believe they are resilient to a *"business disaster",* and wish to believe that third party agreements they have in-place will recover critical business operations within what is deemed as an acceptable time scale. As business continues to change, whether due to *"mergers & acquisitions"* or because of *"business process re-engineering & knowledge management",* or maybe just day-to-day events, this approach becomes difficult to keep up to date. And, it should also be remembered that customers, suppliers, manufacturers and maintainers are also experiencing the same type of changes. The recipe for disaster is almost complete!

The final ingredient is in business thinking; ***"it will all be right on the night",*** or even *"denial"* that anything could possible go wrong, and deciding that a *"crisis management*

plan" will not be needed. All of these factors put at risk the corporate integrity of a business, when an unplanned event happens.

Only time and more awareness about *"communication disasters"* will, hopefully, move the directors of companies towards taking a strategic approach to:

"resilient communications".

Remember proper preparation and planning prevents poor performance!