



# Business Continuity:

H.A / D.R Issues & Drivers

*An Overview*

The ultimate security for your business critical information

\*noMAX is developed by MAXIMUM AVAILABILITY  
www.maximumavailability.com info@maxava.com

## TABLE OF CONTENTS

<b>An Evolving View of Information as a Strategic Asset .....</b>	<b>3</b>
<b>Business Continuity – a Key Business Issue .....</b>	<b>3</b>
<b>Business Continuity – Some Initial Observations.....</b>	<b>4</b>
<b>A massive Increase in Data Volume and Complexity.....</b>	<b>4</b>
<b>Data Loss: an End-to-End Impact .....</b>	<b>5</b>
<b>Downtime - Perception VS Reality .....</b>	<b>5</b>
<b>Downtime - Perception VS Reality .....</b>	<b>6</b>
<b>Are You Prepared? .....</b>	<b>8</b>
<b>The Cost of Downtime – Budget and Revenue Impact .....</b>	<b>9</b>
<b>Business Continuity &amp; Compliancy: it’s a Big Deal .....</b>	<b>10</b>
<b>Business Continuity – The Key HA and DR Technology Drivers .....</b>	<b>11</b>
(1) Elimination of the “Back-Up Window” .....	11
(2) Tape Back-Up Integrity .....	11
(3) Managing “Orphan” Data.....	12
<b>Business Continuity – the Framework for an Optimized HA and DR Solution .....</b>	<b>13</b>
<b>Bringing HA and DR into Focus: A value and Investment Proposition .....</b>	<b>14</b>
<b>An HA and DR Business Continuity Check List.....</b>	<b>15</b>

## AN EVOLVING VIEW OF INFORMATION AS A STRATEGIC ASSET

Viewing a company's critical business information as a strategic asset has only recently begun to gain traction in the corporate world. Yet many organizations still accept slow or limited access to their data during data backup and recovery periods. Worse, even more are simply not aware of the exposure that their data is under in the event of an unplanned outage or have simply not taken the steps required to ensure that this information is protected and available during these times.

## BUSINESS CONTINUITY – A KEY BUSINESS ISSUE

With the advent of greater global instability, technology development in hyper-drive, an increasingly competitive commercial environment and simply the sheer volume of data being created, the security and integrity of business-critical information has raised Business Continuity (B.C) and Business Continuity Management (BCM) as a central operational and management issue.

As such, companies of all sizes are now forced to seriously address the issue of Business Continuity and what they need to do to secure and maintain access to their data.

In a recent survey CFOs were asked *"In which one of the following areas do you feel your company is most vulnerable?"*

Their responses were:

+ Disaster preparedness/recovery	37%
+ Security of information systems	24%
+ Protection of intellectual capital	11%
+ Detection of accounting fraud	10%
+ Theft by company employees	2%
+ Other	3%
+ None/not vulnerable	11%
+ Don't know/no answer	2%

Source: Robert Half Management Resources

## **BUSINESS CONTINUITY – SOME INITIAL OBSERVATIONS**

- + There is a small but consistent growth of awareness of Business Continuity Management issues, however, too many managers continue to work in organizations where there is no Business Continuity Plan in place or where they remain unaware of its existence
- + The rise of the Corporate Governance is - in particular – starting to drive this shift
- + The scope and vision of BCM is poorly defined with little proper benchmarking. In the UK, for example, a recent survey highlighted that only 32 percent of respondents had their business continuity plans externally evaluated or benchmarked
- + There is a perceived lack of “tangible” executive commitment to BCM (beyond the rhetoric). Recent IBM research identified that 67% of surveyed DR professionals believe that there is a lack of required executive support for the implementation of a proper BC infrastructure
- + Too many priorities are set – yet there is too little sustained focus on the most appropriate BC activities
- + The increased level of concern about threats to an organization has not translated to a significant increase in the adoption of Business Continuity Planning or related process implementation. In short, there is plenty of concern but not enough action by way of follow up
- + Too few organizations have implemented optimized BC Plans and/or adequately rehearse their implementation, thereby increasing the risks of using flawed BCM capability when faced with real disruption

## **A MASSIVE INCREASE IN DATA VOLUME AND COMPLEXITY**

The sheer volume of data being created is contributing to such statistics. For example:

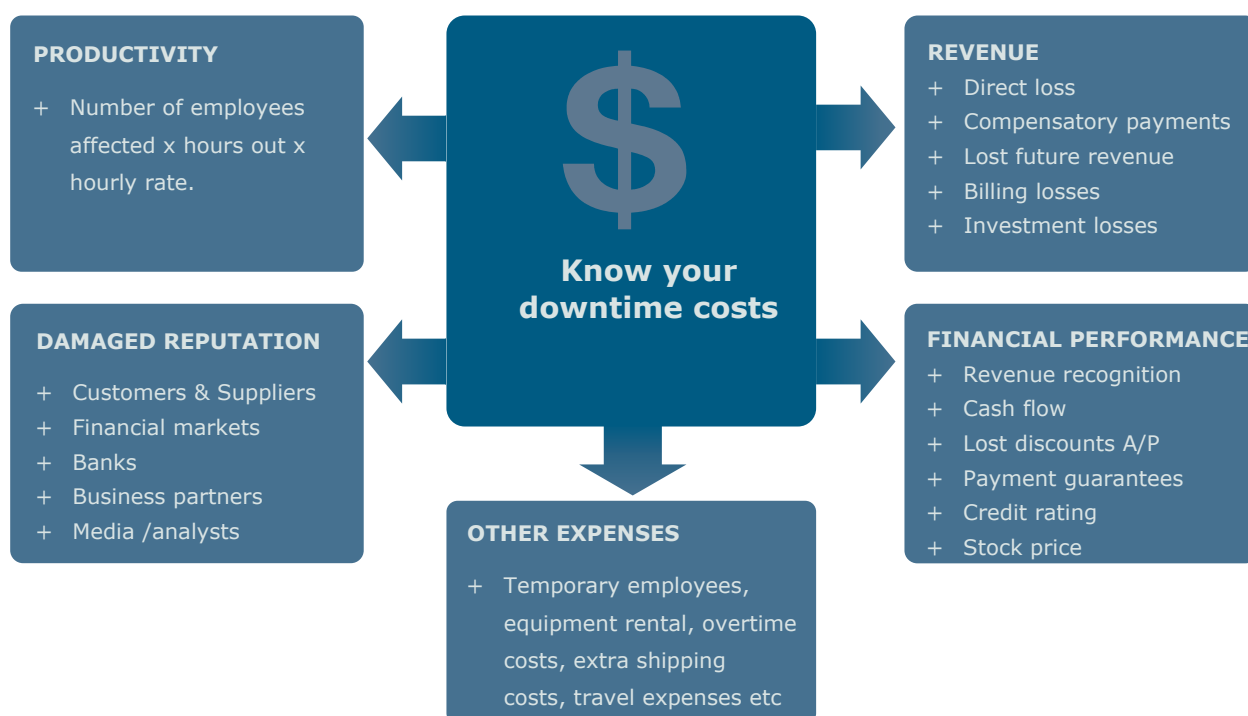
- + IDC has stated that between two and four exabytes\* of unique information per year is produced on a global basis. This is approximately 800 megabytes for every man woman and child on earth (\*an exabyte is a billion gigabytes, or 1018 bytes)
- + Conservative estimates – also from IDC - show data expanding at a rate of 50 to 80 percent per year while other industry analysts place the growth rate closer to 100% annually
- + In recent SunGard research, 61.5 percent of the organizations surveyed experienced an unplanned disruption of technology services in the last year. This is an increase over the 54 percent of executives that previously said their company experienced a disruption

## DATA LOSS: AN END-TO-END IMPACT

Critical data loss impacts heavily and directly on a business in both the short and longer term - and in numerous ways. In short, there is little in a business's infrastructure that is unaffected by major (planned and unplanned) downtime.

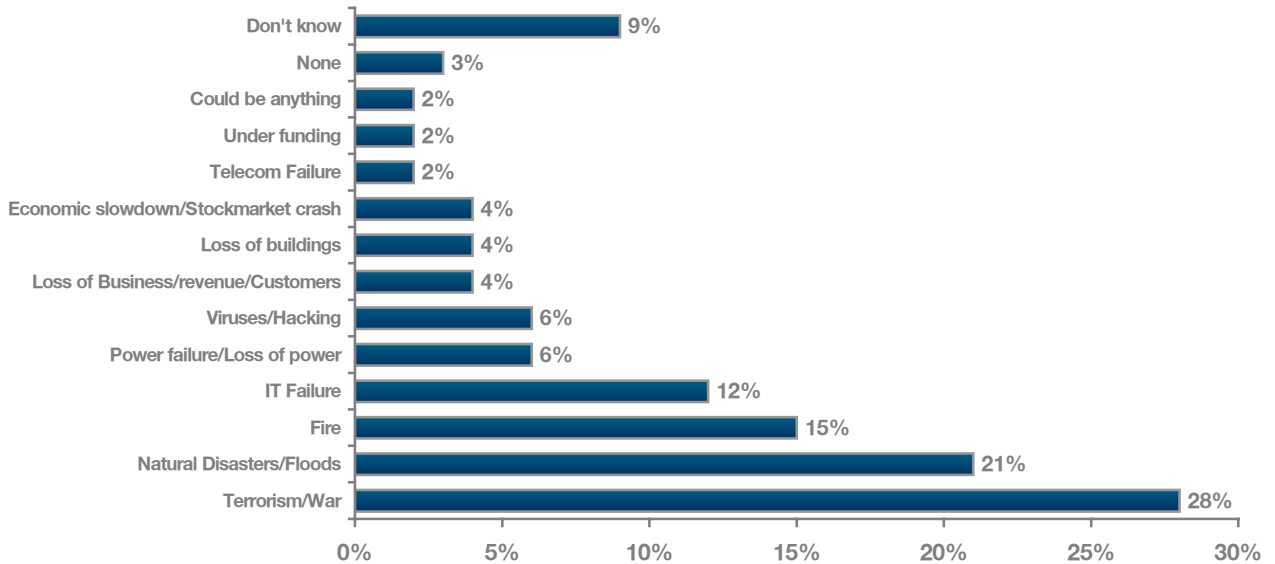
- + A recent study by the University of Texas reported that of companies suffering a severe loss of data, only 6% survived the impact of that loss, 51% had gone out of business within two years and 43% simply never again opened their doors

The impact of Downtime on an organization is not only broad but will also affect the business in a number of intangible ways (see edited table below – Source: Gartner Group)



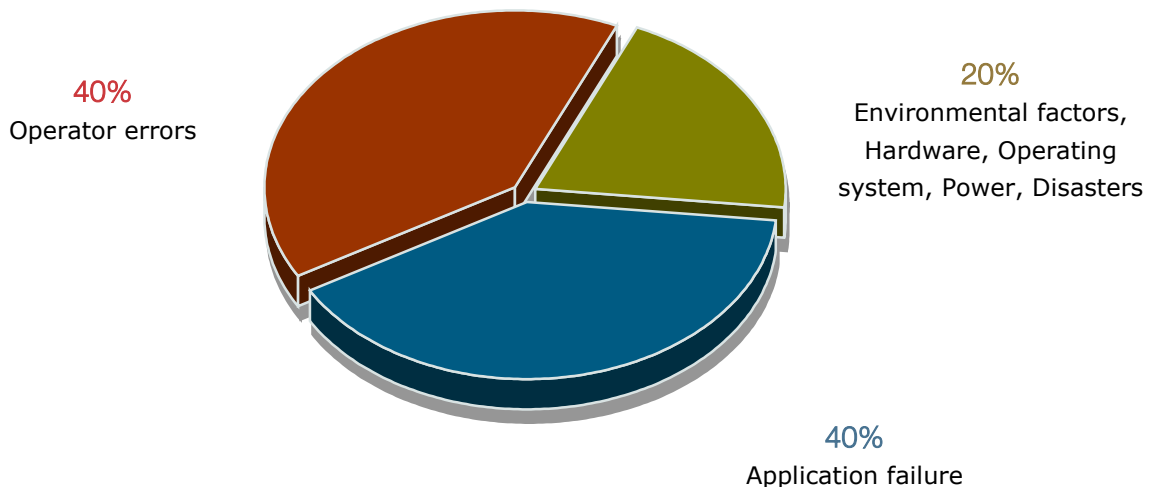
## DOWNTIME - PERCEPTION VS REALITY

A recent survey indicated that almost 30% of businesses across the globe cite a terrorist attack/natural disaster as the biggest threat to the security of their data and the most likely cause of sustained downtime.



Source: Business Continuity Institute

Surprisingly, the reverse is true: the bulk of outages or system downtime is caused by the day to day, rather than the unusual: operator/user error, or application failure account for 80% of outages. The remaining 20% of unplanned downtime is caused by environmental factors such as hardware failures, operating system failures, power/heating/cooling failures, while only a small percentage is attributable to natural disasters such as floods, fires or hurricanes.



Source: Gartner Group

As the Chart indicates, there are a surprising number of reasons behind the cause of downtime that are, in fact, within an organization's operating environment rather than a simple "Act of God."

Even an organization that grades itself an 'A' is still exposed if just one step in a five-step process fails and causes an unplanned disruption to a company's technology services. The only correct answer to score an overall passing grade, therefore, is to have an information availability strategy that will always keep business critical data secure and available - even under the most challenging circumstances.

The important point however is that – irrespective of the cause – Planned downtime **must** occur. Unplanned downtime **will** occur. As such – the key question to ask is: "Is your organization sufficiently protected?"

## ARE YOU PREPARED?

Statistics back up our own observation that there is a general lack of awareness, resource and focus on what constitutes a best-in-breed Business Continuity infrastructure for the protection and continuous availability of business critical information. For example:

- + An IBM survey identified that since 9/11 nearly 60% of companies had not increased their BCM-related staff
  
- + Only 35% of SMB's surveyed recently by Gartner had anything approaching a comprehensive Business Continuity Strategy in place
  
- + A recent survey of 237 small business conducted by The Small Business Pipeline has found that 73% have no written Disaster Recovery Plan. This is despite the fact that 35% of those ranked disaster recovery as equally important to other business functions
  
- + A Business Continuity Institute Survey found that only 42% of respondents saw a BCM plan was required to protect the core running of the business if an unexpected event occurs and only 8% as simply a back-up plan in case of loss of infrastructure/buildings
  
- + The same survey identified only 27% of organizations researched had dedicated Business Continuity personnel

## THE COST OF DOWNTIME – BUDGET AND REVENUE IMPACT

The cost of planned and unplanned downtime also contributes to the implementation of an HA and DR solution as part of the broader Business Continuity framework.

The dollar amount that can be assigned to each hour of downtime varies widely depending upon the nature of the business, the size of the company and the criticality of its IT systems to primary revenue generation processes.

- + 'On average, businesses lose US\$108,000 of revenue for every hour that their IT infrastructure is down' (Gartner Group)

And that's conservative. The numbers below also take into account the cost of *unplanned* downtime, the results of which are staggering.

### Cost (US dollars) to businesses of unplanned downtime per hour by industry:

<b>Brokerage Service</b>	\$6.48 million
<b>Energy</b>	\$2.8 million
<b>Telecom</b>	\$2 million
<b>Manufacturing</b>	\$1.6 million
<b>Retail</b>	\$1.1 million
<b>Health Care</b>	\$636,000
<b>Media</b>	\$90,000

Source: Gartner Group

- + It is estimated that in 2003, downtime (planned and/or unplanned outages) cost US business US\$9 billion.
- + In one 2000 study, 25% of organizations had a 'significant' disruption to their system annually. 45% of them experienced an outage of between nine to 24 hours, while according to a Dun & Bradstreet report, 59% of Fortune 500 companies alone experience a minimum downtime of 1.6 hours per week.
- + On November 20, 1985, The Bank of New York's (BNY) clearing operation handled more than 32,000 Treasury security trades – a record volume. This triggered a software problem, preventing the firm from delivering treasuries to buyers. The next morning – settlement day – the BNY began accumulating undelivered securities, which had to be financed by borrowings - a staggering US\$23 billion by the end of the day.

## BUSINESS CONTINUITY & COMPLIANCY: IT'S A BIG DEAL

The issue of compliance is now a major driver towards the implementation of a Business Continuity framework. For example:

- + Recent Envoy World Wide research in the US identified that over seventy-five percent of the companies surveyed cite that Federal, State or industry regulations directly affect their business continuity initiatives

Each industry has its own set of regulations for storing and protecting data. While the rules are constantly changing, the trend is constant: organizations are increasingly required to ensure that their data replication and backup infrastructure meets a range of stipulated regulations and mandatory guidelines:

The following are just a few of the many regulations across industries:

- + **Sarbanes – Oxley Act:** This corporate anti-crime law applies to all publicly traded US-based companies and requires CEOs and CFOs to certify the accuracy of their company's financial results. Data storage plays a key role as it pertains to record retention.
- + **BASEL II:** The 1988, G10 countries' New Basel Capital Accord (BASEL II) goal is to regulate capital requirements for credit exposures. Basel II could consume as much as 10 % of the banking industry's IT resources over the coming years.
- + **SEC 17a – 4:** This SEC regulation for Financial Institutions details what data must be saved, how long it must be retained and on what type of media – resulting in significant storage impact.
- + **USA PATRIOT Act:** Requires the development of anti-money laundering programmes, bans offshore "shell" banks and increases data availability and accessibility to the federal Government.
- + **Generally Accepted Principles of Computer-aided Accounting Systems (GoBS):** is a German Banking law referring to the use of computers in maintaining books and other necessary records: regulations such as "an entry may not be altered" have significant storage technology implications.
- + **National Association of Securities Dealers (NASD 3010 & 3110):** – NASD 3010 monitors electronic communications in securities industries; NASD 3110 specifies a retention programme for all correspondence.

## **BUSINESS CONTINUITY – THE KEY H.A AND D.R TECHNOLOGY DRIVERS**

We have identified three key technology-related drivers that are repeatedly evident when evaluating HA and DR solutions against a broader Business Continuity framework.

### **(1) Elimination of the “Back-Up Window”**

As previously noted, with the almost exponential amount of new data being created - and the requirement to back it up on a regular basis - traditional tape back-up procedures are under increasing pressure to do the job quickly and cost-effectively. In short – they are required to process more in less time, resulting in a significant reduction in the time available to undertake planned back-up and recovery procedures.

This is an issue that is simply not going to go away but, instead, will have even more significant resource and system up-time implications for organizations that plan to continue their replication processes using physical tape-back procedures.

The key questions to a prospect facing these issues include:

- + Is your backup and recovery window impacting on your production activity? If so – to what extent?
- + Have your users got used to - and accept - the current levels of downtime they experience?
- + Is there a move in your organization toward 7x24 uptime?

### **(2) Tape Back-Up Integrity**

In the vast majority of cases, tape back-up procedures are still the primary ‘strategy’ that many organizations have for the protection of business critical information. In many cases, this data will remain on-site either permanently or until such time as it can be stored off-site. The implications here are obvious: any data remaining on site is open to the same threat from a catastrophic event (fire, flooding, etc...). Equally, an organization’s data integrity is only as good as the last backup made. For a company undertaking weekly data backup using tape, in the event of a major disruptive event, it will lose up to one week’s worth of data.

The key questions to a prospect facing these issues include:

- + Do you know how much your organization is currently spending on tape-based backup recovery?
- + Are you certain that your enterprise is spending that money optimally?
- + Is the medium of using physical tape for back-up processes keeping pace with your technology requirements?
- + Are you aware of any short-cuts being taken with your physical tape back up procedures to help ensure a minimum of downtime is experienced by end-users?
- + (And associated with the above question) If shortcuts are being taken using tape-back-up, are you sure that all of the business information required for back-up is, in fact, being replicated?

### **(3) Managing "Orphan" Data**

Even with regular tape backup procedures in place there is no significant protection over data that is lost *between* saves. The only real way of avoiding an 'orphan data' scenario is to employ software that replicates changed-base data and data objects to a backup server in real time – all of which maintains a synchronized, switch-ready environment.

The key questions to a prospect facing these issues include:

- + Can you afford to loose a day's data?
- + Can you easily re-create data in the advent of a disaster?
- + How long will it take you to re-create all of your lost data?

## **BUSINESS CONTINUITY – THE FRAMEWORK FOR AN OPTIMIZED H.A AND D.R SOLUTION**

A robust and secure HA and DR solution is never implemented in isolation to an organization's key business needs. As such, it must ensure close and successful integration with a Business Continuity framework. At its core this includes:

- + **Access to expertise and skills** that will provide the infrastructure to support the easy acquisition and management of maintaining continuous business operations
- + **Regulatory awareness** – to have the processes and commitment in place to quickly and cost-effectively comply with new and changing government rules
- + **Security, privacy and data-protection** – that will protect against internal and external threats and help develop a critical information management policy
- + **Continuity of business operations** – to become more anticipatory, adaptive and robust, from IT through all business processes
- + **Market Readiness** – reliable and effective operations that will support the ability of an organization to anticipate and respond to changing market conditions
- + **Integrated risk management to reduce costs** – stay competitive by managing risk more efficiently and cost-effectively

## BRINGING H.A AND D.R INTO FOCUS: A VALUE AND INVESTMENT PROPOSITION

We can bring the value of a data replication solution into a very clearly-defined frame.

In essence – and when all is considered – a solution such as that provided by the \*noMAX Suite of High Availability and Disaster Recovery Products will:

- + **Deliver continuous uptime with zero data loss** so applications and business data are always available in a 24/7/365 business context
- + **Provide a delivery platform that incorporates a backup server with a current replica that is always available for failover or switchover** to replace the production server with an RTO of seconds or minutes and an RPO of zero
- + **Provide an integrated High Availability and Disaster Recovery Solution:** The HA component that will dramatically reduce the risks and costs of business interruptions while at the same time act as a Disaster Recovery strategy when the backup server is placed in a remote location

From an investment perspective, such a solution should also:

- + **Lower the risk** of significant cost to business such as lost revenue, productivity, legal penalties and brand damage caused by unplanned downtime
- + **Protect business relationships** with customers, partners and suppliers by ensuring that applications and data will be available to satisfy their needs and unique schedules
- + **Enforce Service Level Agreements** by maintaining predictable RTOs (Recovery Time Objectives) and RPOs (Recovery Point Objectives) in the event of an IT outage
- + **Enhance ROI** on existing resources by ensuring they will be available to generate revenue and support business processes; and
- + **Ensure compliance** with government and trade regulations by securing email and record retention requirements and protecting the availability of business data and reporting processes

## AN H.A AND D.R BUSINESS CONTINUITY CHECK LIST

When formulating an HA and DR solution as part of an overall Business Continuity solution, we will typically ask the following questions:

1. Can you identify the critical business activities that you undertake that most satisfy your customers' expectations and, in turn, form the basis of your operation?
2. Is Business Continuity an issue that has been discussed at board/Senior Management level within your organization?
3. If so, has a Business Continuity Strategy been developed that accounts for all aspects of BCM and data recovery? Is that strategy tested frequently?
4. Do you have a Change Management Process in place to keep your knowledge management current in the area of Business Continuity?
5. Have you developed an area-by-area checklist on what your business would need to continue to function effectively should an outage occur?
6. What information do you have on the causes, frequency and subsequent impact of system downtime?
7. Does this information enable you to prioritize your business activities?
8. Are you confident that in the event of a disaster or outage your business could recover quickly and run effectively enough to eliminate damage to your data, systems and reputation?

Source: IBM