

Ensuring business continuity backing up business data

Backing up your corporate asset (Records/Information) can be tough these days, with the phenomenal rates at which data sets are growing, coupled with users demand for instant information availability.

Ensuring confidentiality, integrity, and availability of records and information should be the goal of any serious minded management, because no organization survives without any of the aforementioned characteristics of good information. Some of the developmental challenges faced in achieving these are:

- Database explosion (rapid growth of database).
- Demand of instant information access (growing influence of downtime).
- Distributed system with lack of control.
- Technology gap.
- Regulation.
- Disaster recovery plan control and recovery.
- Security

PHENOMENAL GROWTH OF DATA/INFORMATION.

Almost all forms of business and consumer-oriented dealings can be conducted online, and rich record of past transactions and events are also available.

Majority of the Records and Information that were once in paper record form is given online. Those medical records, public records and other different types of formerly paper business records are being transformed and converted to online resources. A number of organizations have begun to scan and digitized their archives of paper records and putting them online to streamline present and future access.

DEMAND FOR INSTANT INFORMATION ACCESS.

These days, the near-instantaneous access to current and past business records and information has resulted in new service capabilities where business and government are often expected to make these records available on demand; most especially now that the freedom of information (FOI) bill is expected to be passed into law in Nigeria. What use to take weeks is now expected in seconds. Instant access to records and information has become the norm, and often the failure to live up to this expectation is considered disastrous.

Aside customers, business workers need specific information right now, so they can complete the task that support mission-critical business processes.

Downtime is no longer tolerated but instead is seen as a failure to provide adequate infrastructure and capacity

DISTRIBUTED SYSTEM CHALLENGES.

In most organizations, distributed applications rely on many servers and database, often located in remote locations. Different server and data components often are based on different technologies like mainframe, UNIX, and windows, to mention a few. Even when all these components in a distributed system are within the control of the organization, their complexity often make it more challenging to properly manage their information.

In spite of the fact that some of the systems in a distributed application are even owned or controlled by the organization, they still provide a vital (and sometime critical) part of the correct functioning of applications.

TECHNOLOGY GAP.

About 20-30 years ago, tape back-up was not only the standard choice, but also the only choice. All the enterprise data resided in one place. There were no desktop or laptop computers, networks, or distributed application, and organizations did not depend on instantaneous access to enterprise data anytime, from any place. The notion of online privacy which we witness now had not been thought of, and there was hardly any regulation in data integrity, security, or privacy at all, although up till date in Nigeria, there still has not been any known regulation to the members of the public governing data integrity, security, or privacy as available in other developed part of the globe.

Tape backup is not cutting it any more. Although significant advances in tape backup medium have taken place, primarily I capacity and speed, tape is now in its fifth decade of commercial use and is being overtaken by disk-based solutions. Some of the draw-backs of tapes include:

- It is a serial-access medium that is hundreds of times slower than online disk-based storage.
- Tape is a fragile medium.
- It is subject to stretching and tearing.
- It is sensitive to temperature swings.
- Date on tape medium slowly decays over time.

REGULATION AND COMPLIANCE.

In the developed society, there are new laws in every industry sector that require organizations (public or private) to improve the backup and archival capacities in the key systems.

Regulations require robust controls and record keeping for key business activities. The fact that the majority of business processes are information-based, this translate into the need to frequently backup data as a hedge bet against the potential for hardware or software failures that can destroy or corrupt vital business information.

Please, note that legislation has a distinctive "frickle down" effect. That is why certain laws apply to companies in specific industry sectors, often the laws also to companies that provide service to those companies directly affected. For examples, an organization may outsource its e-mail system to an online e-mail service provider in order to reduce costs

However the e-mail service provider will be required to demonstrate compliances to laws related to the protection and archival of email data that the organization is required to comply to.

Banks, credit unions, and other financial institutions endure a significant regulatory burden that requires the protecting of business records and information about depositors.

HEALTH CARE.

Organization providing health-care –related services should enact several safeguards to protect business information. For example in the United State of America,HIPAA’S (Health Insurance Portability and Accountability Act) security rule requires that organizations securing back-up media, and develop a disaster-recovery plan that ensures that vital records will not be lost in a natural or man-made disaster.

DISASTER RECOVERY PLAN ,CONTROL AND RECOVERY.

Business continuity planning (BCP) and Distant Recovery Planning (DRP) together encompass a vast array at prevention and response activities that ensure the survival of a business through a natural or man-made disaster.

In a number of disaster scenarios, I.T systems are directly damaged or made inaccessible, which effectively knocks vital business processes “off the air” until I.T system functionality and connectivity is restored.Often, this requires that critical data be recovered onto servers in original or alternate business locations.

Backup data needs to be located at a secure location that is far enough away, that is not involved in a regional disaster, but positioned for rapid “over-the-wire” recovery that does not depend on couriers to ship backup tape to a disaster recovery site.

SECURITY

Finally, laws and regulations that require the protection of stored information should also apply to the same data on backup media. Data should be protected from unauthorized disclosure regardless of its location or the types of media it is stored on.

To ensure a truly secured backup data, it must be encrypted not only on transit but also in storage. This Measure will effectively eliminate disclosure of sensitive data to any unauthorized party. The elimination of physical transport of backup media can further ensure security.

Oyedokun Ayodeji Oyewole is the president of Records and Information Management Awareness Foundation (RIMA Foundation), a Not-for-profit NGO that seek to promote proper management and security records and information for the benefit of the society and humanity. He can be contacted at: president@rimaw.org