



VERITAS™

Data BackUp in the Public Sector

CONTENTS

Data BackUp in the Public Sector	1
Archives – The Backbone of Open Government	1
Vision	2
Challenges	2
Securing While Assuring - Assuring Consistent Reliable Backup	2
Securing Every Copy of All Data	2
Cloud Implications	2
FOIA and eDiscovery Requirements	2
Cost to Taxpayers of Backing Up Useless Data	3
Regulatory Considerations	3
Operational Issues	3
Standardization of BackUp Tools, Platforms, and Standards	3
Retention Requirement Policies, Data Destruction Policies and the FRCP	3
New Challenges from New Technologies	3
Virtualization	3
Mobility	4
Cloud	4
People-Centered Challenges	4
Veritas™ Enterprise Vault	4

The fundamental reason for backing up data is to better assure continuity or rapid return to business operations in the aftermath of an outage. Outages range from a hardware failure or user error all the way to major catastrophes such as earthquakes, hurricanes, tsunamis, and acts of terror.

“Statistics show that, of the businesses that close because of a disaster, at least **one in four never reopens**,” says the [Insurance Institute for Business and Home Safety](#) (IBHS).

When the business you’re speaking of is the business of the city, state, or country, the level of criticality leaps. Short of partisan politics, nothing should ever stop the running of the business of the government, and losing the availability of key information is simply unacceptable when the health and welfare of the citizenry is at stake. For this reason, the U.S. government maintains a comprehensive “backup” of all records of all important transactions, actions, and other communications called the National Archives.

ARCHIVES - THE BACKBONE OF OPEN GOVERNMENT

In his Presidential Memorandum on Managing Government Records for the heads of Executive Departments and Agencies issued in November 2011, President Obama explains the importance of maintaining an Archive of records of all actions and decisions as follows:

“Records transferred to the National Archives and Records Administration (NARA) provide the prism through which future generations will understand and learn from our actions and decisions.

“When records are well managed, agencies can use them to assess the impact of programs, to reduce redundant efforts, to save money, and to share knowledge within and across their organizations. In these ways, proper records management is the backbone of open Government.”

According to their official [website](#), “An archives is a place where people can go to gather firsthand facts, data, and evidence from letters, reports, notes, memos, photographs, and other primary sources. The National Archives is the U.S. Government’s collection of documents that records important events in Amer-

ican history. The National Archives and Records Administration (NARA) is the Government agency that preserves and maintains these materials and makes them available for research.”

Vision

The Vision of the U.S. National Archives is:

“We will be known for cutting-edge access to extraordinary volumes of government information and unprecedented engagement to bring greater meaning to the American experience.

Our Vision is to transform the American public’s relationship with their government, with archives as a relevant and vital resource. This vision harnesses the opportunities to collab-



Nothing should ever stop the running of the business of the government, and losing the availability of key information is simply unacceptable when the health and welfare of the citizenry is at stake.

orate with other Federal agencies, the private sector, and the public to offer information—including records, data, and context—when, where, and how it is needed. We will lead the archival and information professions to ensure archives thrive in a digital world.”

Fundamentally, Public Sector Responsibility for backup of all information is proscribed by law.

CHALLENGES

Although “data backup” sounds like a simple enough concept, the actual practice of consistently performing reliable backups offers up many significant challenges.

Securing While Assuring - Assuring Consistent Reliable Backup

Governments operate a wide variety of departments and agencies, each of which generates

tremendous volumes of new data daily. Making a complete backup of all this data daily is, in and of itself, a daunting task. Even incremental backups, where only the day’s additions, deletions, and changes are added to the backup may not execute fast enough to achieve adequate Restore Point and Restore Time Objectives (RPO & RTO). Faster technologies with higher input/output and lower latency are often required.

Securing Every Copy of All Data

By definition, a data backup is a complete copy of the live production data. Beyond the fact that securing government data is important to achieve regulatory compliance, it is critical that government data not be allowed to fall into unauthorized hands. All backup devices and all media must be kept under strict, secure control at all times. Rotated media must be secured.

Cloud Implications

Many organizations, including governments and governmental departments and agencies, are now evaluating the cost and operational benefits available from backing up data to cloud computing services. Administrators must make certain that their cloud service provider offers complete isolation of all government data where it cannot “leak” to unauthorized other tenants of shared facilities. Also, all data must be kept encrypted at all times, while at rest in storage as well as during transport. This will make it impossible for anyone intercepting or inappropriately accessing such data to interpret or use it in any way.

FOIA and eDiscovery Requirements

Effective security processes and procedures do not change the fact that, by law, required information must be made available in a rapid manner for purposes of legal eDiscovery as well as

responses to Freedom of Information Act and other valid requests.

Cost to taxpayers of Backing Up Useless Data

Mandates such as the President's Memorandum stimulate a tendency to store everything. This seems to be the easiest way to assure that required information is not lost or discarded, but it comes at a staggering cost. Gartner estimates that it costs \$5 million annually to manage a petabyte (that's \$5,000 per TB) of data.

View this in the context of another observation from the Forbes article that 69% of all data that organizations store contains no legal, regulatory, or business value. More than two-thirds of all data stored is debris, and therefore \$3,450 of every \$5,000 spent on every terabyte stored is wasted.

Virtualized server technologies put the combined contents of many servers into a single machine. This does not change the requirement Data BackUp in the Public Sector 4 to back up all data from every virtual machine located on every host device.

Regulatory Considerations

The importance of regulatory considerations to the backing up of data is possibly best expressed by understanding the implications of the two key words in the title of the HIPAA Act.

Many people misspell the acronym as "HIP-PA" because they are unaware of the actual name, which is the Health Insurance Portability & Accountability Act. Clearly, the key words "Portability & Accountability" provide us with an excellent context for what is most important.

It is said that information only gains value when it is in motion. Contrary to popular belief, HIPAA does not inhibit or prohibit the electronic conveyance of private patient health information. In fact, it promotes and supports it. It responds

to the natural mandate that information must be available when and where it is most needed.

The HIPAA Act and other regulatory acts encourage the sharing of data under strict control and protection from unauthorized access.

OPERATIONAL ISSUES

Achieving operational consistency is a challenge to any organization, but with the proliferating number of department and agencies in government, any hope of consistency must be grounded in standardization.

Standardization of BackUp Tools, Platforms, and Standards

The rapid growth of the Internet of Things has underscored the importance of achieving interoperability on every level. This is just as true for data backup as it is for any technology. The ability of organizations to interchange data and to support each others' operations grows in direct proportion to the degree of standardization achieved. Ideally, all government agencies will operate on identical platforms, adhering to well-known published standards, and using tools that are common amongst them.

Retention Requirement Policies, Data Destruction Policies and the FRCP

Federal Rules for Civil Procedure (FRCP) stipulate that every organization must establish a consistent policy and consistently adhere to said policy. This carefully developed policy must clearly define which data must be retained, backed up, and protected, and which data may be deleted or destroyed. This applies to data backups as well as production data.

NEW CHALLENGES FROM NEW TECHNOLOGIES

Virtualization

Virtualized server technologies put the com-

bined contents of many servers into a single machine. This does not change the requirement to back up all data from every virtual machine located on every host device.

Mobility

Users with mobile devices increase the variety of locations in which data may be resident. Care must be taken to thoroughly specify how data on each mobile device will be managed and backed up.

Cloud

As mentioned earlier, data being backed up from or to cloud-based services must be isolated and protected from data leakage. This includes encrypting all data at all time whether at rest in storage or in transport between endpoints.

PEOPLE-CENTERED CHALLENGES

Information Technology Professionals tell us that the hardest segment of the network to manage

is that segment which occurs between the keyboard and the back of the chair – the user.

Any data backup policy is only as good as its enforcement. Enforcement begins with thorough training of all involved personnel as to their responsibilities and duties regarding data backup.

Once trained, vigilant scrutiny must be maintained to assure continuous adherence to published policies. At any given time, employees must have clear, comprehensive documentation of all policies available for reference and review.

VERITAS™ ENTERPRISE VAULT

Available on-premises and in the cloud, Enterprise Vault enables organizations to efficiently store, effectively manage, and easily discover and retrieve unstructured information as needed for business. Enterprise Vault helps customers deduplicate information, manage organization-wide retention policies, and control the costs of compliance and litigation support. ■

Product highlights

- **Proactively manage eDiscovery.** Efficient search and review can be performed in-house without manual collection, streamlining early case assessments, legal holds, and a repeatable and defensible eDiscovery process.
- **Intelligently manage information** as part of an information governance program by automating the granular retention, and defensible deletion of information.
- **Reduce storage footprint and costs** by archiving less frequently accessed information off of expensive primary storage and servers such as Exchange, Domino, Share-Point, and file servers.
- **Streamline backup and recovery** by moving older, infrequently accessed content from production sources into a centralized archive.
- **Veritas Enterprise Vault Extensions** provides a framework for partners to create archiving applications that extend the scope of what Enterprise Vault can archive. The Extensions may be viewed and managed within the Vault Administration Console.
- **Centralized administration** provides advanced reporting, monitoring, and diagnostics of the archive, helping to ensure consistent performance and availability.