

HOW COMPLIANCE IMPACTS BACKUP STRATEGY

SCOTT BLEASDELL - PRODUCT MANAGER

IDERA, INC.

THE INTERSECTION OF COMPLIANCE AND DIGITAL DATA

Sarbanes-Oxley. Gramm-Leach-Bliley. PCI. HIPAA/HITECH. SEC. Basel II. Red Flag rules. SSAE 16.

Organizations of all sizes and shapes must comply with government and industry regulations. Some regulations are limited to public companies, while others are relevant only to certain verticals. There are many regulations that cut across type, size, and industry in their impact. In addition to legally mandated requirements, many organizations voluntarily adopt quality and process standards like Six Sigma or ITIL, or establish performance guidelines that impact employees and/or customer agreements. Adhering to these standards brings with it additional (and not always overlapping) sets of rules. In compliance with these standards, regulations and rules—or just to maintain best practices—most organizations are implementing some degree of business continuity/disaster recovery plan.

While most information can (at least in theory) be kept on paper, virtually all organizations now keep personnel, customer, financial, transactional and other records in digital format. Indeed, in this day and age, most organizations operate at the intersection of compliance and digital data. After all, compliance and digital data have become inextricably intermingled. Compliance is only manageable when information is digitized, and the proliferation of digital data makes compliance more essential. Organizations need to be following a set of rules about how to manage the growing stores of digital information they're accruing.

The bottom line: Whether legal requirements are in place, whether the rules and regulations are self-imposed, or whether there's a combination of factors in play, prudent business practice calls for backing up and securely housing digital data.

ABOUT THE AUTHOR

Scott Bleasdell is the Product Manager for Idera Server Backup. He has more than 18 years experience in the IT industry. After starting out as a network administrator for one of the largest privately owned companies in the US, Mr. Bleasdell saw a need for better software solutions to serve the IT community.

He has worked on systems management solutions for NetIQ and as a product manager for Microsoft's Systems Center division. Mr. Bleasdell later joined a small software company where he led in the creation of multiple service desk and datacenter automation products that eventually became part of the portfolios of companies such as Citrix and Quest Software (now a part of Dell).

Mr. Bleasdell earned his degree in engineering from the University of Texas at Austin.

THE INTERSECTION OF COMPLIANCE AND BACKUP

Compliance-related requirements need to drive the backup strategy, and the backup strategy needs to support whatever compliance-related requirements an organization has in place.

What does having (and enforcing) a backup strategy accomplish for an organization?

For one, it lets you demonstrate to regulators and auditors that you're capable of protecting and restoring critical data. It can also get you quickly back in business after a disaster occurs—whether from terrorist attack or hacker intrusion, hurricanes (such as recent damage from Hurricane Sandy) or a burst pipe, or just plain human error. Further, it can help protect and defend your organization when litigation arises from employees, customers, competitors, or regulators.

WHY ANY OLD BACKUP WON'T DO

It's not just a matter of if you're backing up (and you should be). It's also important how you're backing up. There is a set of technical requirements that must be satisfied if a backup solution can be used for compliance purposes. These are:

- » Encryption in transit
- » Encryption at rest
- » Access controls
- » Audit trails
- » Where backed up data is kept (off premises, in country, etc.)
- » The ability to determine what types of data get backed up
- » The ability to set frequency of backup
- » The ability to satisfy restoration time requirement

Any company that maintains personally identifiable information on employees (Social Security numbers, proof of citizenship, etc.) has obligations attached to the maintenance of this data. The same holds true for organizations holding confidential customer information (e.g., credit card numbers, banking information). These obligations revolve around keeping information private and confidential, keeping information secure from unauthorized access, and just plain keeping information for whatever the requisite retention period is.

There's no need to delve into much (if any) detail on why these requirements make the list: They're all more or less self-explanatory. Two not-so-self-evident things are worth pointing out here.

1. Tape-based backup, which requires manual intervention, is an inherently insecure process and will fail to meet the compliance threshold for regulations regarding data privacy. Tape-based backup may further fail the test when it comes to satisfying time-to-restoration requirements.
2. All automated software backup solutions are not created equal. When choosing a solution, you should be doing so with full awareness of what your organization's compliance needs are.

IDERA SERVER BACKUP

Idera Server Backup software provides compliance-ready backup for over 275,000 servers. The table that follows shows you why Idera is so well suited to meet the compliance needs of so many organizations.

| Required for Compliance | For example: | Idera "Compliant Ready" Server Backup |
|-------------------------|--|--|
| Encryption in transit | <ul style="list-style-type: none"> - Sarbanes Oxley (financial reporting data) - Basel II (financial reporting data) - Graham Leach Bliley (non-public personal information) - PCI (personal account number) | Data in transit from the agent to the backup manager are encrypted using SSL. |
| Encryption at rest | <ul style="list-style-type: none"> - Sarbanes Oxley (financial reporting data) - Basel II (financial reporting data) - Graham Leach Bliley (non-public personal information) - PCI (personal account number) | Users have the option to encrypt the data as its being written to disk, using AS 256 encryption. |

| Required for Compliance | For example: | Idera "Compliant Ready" Server Backup |
|--|---|---|
| Access controls | <ul style="list-style-type: none"> - HIPAA (unique user identification) - SSAE 16 - Red Flag Rules | Each disk safe (where data is backed up to) can have its own pass phrase, rather than rely on use of a global pass phrase. Users can't restore data to a server they're not credentialed for. |
| Audit trails | <ul style="list-style-type: none"> - HIPAA (for information systems containing protected health information) - Sarbanes-Oxley - PCI | Each time a task – backup, restore, or merge – is performed, Idera Server Backup logs information on who initiated the task, what files were involved, where information was backed up or restored to, etc. All configuration changes are also logged in an auditable file. |
| Determine what types of data to back up | <ul style="list-style-type: none"> - Sarbanes Oxley – financial reporting data - HIPAA - electronic protected health information | Users can select any combination of files and folders to be excluded from their continuous data protection policy, and can add advanced rules using patterns to exclude only certain file types. |
| Set frequency of backup, and retention times | <ul style="list-style-type: none"> - Sarbanes Oxley (sets minimum number of periods for retaining data and audit trails) - HIPAA (sets varying length requirements for adults' and children's health records) | Users can schedule server backups as frequently as every 15 minutes, and can set how many recovery points to retain. |
| Satisfy restoration time requirements | <ul style="list-style-type: none"> - Varies broadly by industry and individual organizational needs | The ability to satisfy restoration time requirements obviously depends on many factors: the size of the data set, types of files (e.g., millions of small files vs. thousands of large files) bandwidth availability, geographic distance between backup and restore site, etc. All of this should be taken into consideration when implementing your backup (and restore) strategy. That said, Idera Server Backup was designed to perform restores as fast as possible, and does so faster than virtually any competitive offering. |

There's a final way in which Idera Server Backup is "Compliance-Ready." The best intentioned compliance and backup strategy will live only "on paper" if it's difficult to implement and time-consuming to deploy on a regular basis. Unlike solutions that may take hours to install and configure, Idera Server Backup is built for "download and go," with no professional services required. Once Idera is up and running, tasks are automated, saving administrative time, eliminating the possibility of "forgetting about it," and decreasing the likelihood of human error.

Given the concurrent explosion of digital information and compliance requirements, having a sound, workable backup and restore policy is essential. So is the ability to carry through on that policy. Idera Server Backup stands at the intersection of compliance and backup with a solution that lets organizations of all shapes and sizes put compliance into practice, cost efficiently and time effectively.

About Idera

Idera provides industry-leading application and server management software for physical and virtual server platforms, including solutions for server backup, SQL Server administration and SharePoint administration. Idera's award-winning products address real-world challenges, including performance monitoring, backup & recovery, security, compliance and administration.

ABOUT HOSTWAY

Hostway Corporation is a leader in Cloud, Managed and Hybrid hosting. Hostway delivers reliable, secure and scalable Infrastructure-as-a-Service (IaaS) solutions to over 600,000 customers worldwide. Hostway services its clients from more than 250,000 square feet of state-of-the-art data center space, spanning four continents and 12 countries. Hostway has emerged as one of the largest cloud hosting and IaaS providers in the world, due to the company's expertise in developing secure, multi-tenant hosting environments and is committed to providing SMBs and large enterprises with cost-effective business solutions. Hostway's core products include Managed Hosting, Cloud Hosting and Email & Applications.

Contact Hostway:

866.467.8929
sales@hostway.com

| | |
|----------|--|
| WEB | www.hostway.com |
| TWITTER | www.twitter.com/hostway |
| FACEBOOK | www.facebook.com/Hostway |
| LINKEDIN | www.linkedin.com/company/hostway-corporation |