The Anti-Cloud Service

Anti-Cloud: Backup & Restore Regulatory Compliance Reference

The amount of data used by today's businesses continues to increase exponentially year over year. Corporate scandals, international unrest, and blatant security flaws in computer operating systems and software applications have resulted in a much more intense and detailed scrutiny of data as it enters and leaves the organization. Well-known Fortune 1000 companies have been exposed and vilified in the media for reckless data stewardship, and in some cases, of outright fabrication of financial performance reports.

Private information stores of several prestigious organizations, some of them highly sensitive and personal in nature, have been lost, misplaced, or accessed by hackers –the details of the events becoming leading news headlines.

Corporate America, already under varying degrees of competitive and performance pressure, now faces compliance legislation and disclosure requirements that seek to right some of the wrongs done to consumers, investors, and employees alike.

A summary of key regulatory compliance policies that require organizations to establish offsite backup and recovery plans is as follows:

Healthcare – HIPAA, HITECH

Health Insurance Portability and Accountability Act - HIPAA: 2003

Healthcare industry are legally obliged to securely maintain patient's health information in an effort to provide patient privacy and security. HITECH (2009) further strengthened the HIPAA regulations with criminal and civil penalties for not maintaining health information correctly. All patient's data must be accessible and recoverable. Any entity that maintains **any** information has the legal responsibility to securely maintain information in a present state and the ability to recover the information if needed. Fines can range from $100 to $50,000 per records up to 1.5 million per violation.

- All data (email, file, server) needs to be replicated offsite
- Data needs to be encrypted – 256 AES- standard
- Data needs to be easily recoverable
- Periodic recovery tests need to be performed
- Data backup and Recovery Plan (DBR) needs to be documented
- Reporting capabilities must be able to track audits, access points, incident tracking

Financial, Insurance, Banking

Sarbanes-Oxley Act (SOX): 2002
Federal law regulating the retention, management and control of electronic records and financial transactions in publicly traded companies. Public companies (specifically CEO, CFO, CTO) are held accountable for their actions and as a result need to maintain financial records physical and digital without alterations for at least 5 years (7 is the norm). The information must be held in an organized fashion and be easily reportable. Fines of up to $5million per incident and 20 years in jail can be applicable

- 256-bit encryption (government standard)
- Quarterly testing and reporting
- Documented policies and procedures.
- Applies to any document pertaining information
- Frequent retention points back up (prevent lost files) in addition to full snapshot
- Continuous monitoring of access points, recovering capabilities and changes to data

The Financial Modernization Act of 1999 - Gramm Leach Bliley Act:
Requires financial companies that offer financial products or services to explain their sharing practices and safeguard all the consumer information. Although the regulations are flexible and don't identify specific standards towards data protection, the industry typically follows the guidelines for HIPPA and SOX.

- Ensures security of customer information and records
- Protect against anticipated or unanticipated threats to their information
- Protect against unauthorized access or use of personal information that results in harm to the customer.
- Identify one policy holder to manage process

Payment Card Industry Data Security Standards (PCI): 2005
PCI is an internal regulation set by the industry itself in an effort to safeguard consumer payment card information. States that if you are storing, processing or transmitting any consumer information, regardless of where you are, you must adhere to and are responsible to the standards set by PCI. Fines vary from $5,000 to $100,000 per month for non-compliance

- Build and maintain a secure network
- Protect card holder data (256 encryption)
- Maintain reporting and quality control procedures
- Monitor access, changes and reporting capabilities
- Maintain a information security policy

Fair and Accurate Credit Transaction Report (FACTA): 2003
Provides the consumer access to their credit history but also provides safeguards pertaining to identity theft. Affects all companies that have and maintain consumer information and requires them to take all efforts to safeguard that information from potential fraud. Failure to comply with FACTA can lead to fines of $1,000 per individual per incident in addition to class action law suits.

- Prevention programs need to be put into place to identify "red flag" incidents.
- Maintain all information securely and privately
- Provide credit reporting to consumers
- Proper disposal of all consumer information

SEC Data Compliance:
Provide institutional regulations that govern compliance of data retention, protection and continuity for financial records and electronic communication

- Stored information must be encrypted and stored safely so only authorized individuals can access
- Data is securely stored in diverse and protected datacenters
- Data can be restored quickly and accurately to a specific RPO
- Must have clear reporting on access points for auditing purposes

Financial Industry Regulatory Authority (FINRA):
FINRA requires financial institutions keep and maintain business continuity and contingency plans in an effort to satisfy obligations to their customers in case of unplanned emergencies. Although FINRA refers to books and physical records the regulations should be applied to a firm's secure data storage.

- Any financial business needs to provide a solution that automatically and securely back up their data to an offsite, protected and secure facility in a different geographic location
- All businesses need to maintain a written continuity plan in case of an emergency

SSAE 18/SOC 2:
Any company that utilizes outsourced services to maintain financial information must comply with the standards of SSAE 18, which includes having a SOC 2 reports and compliant third-party vendors.

- Anti-Cloud maintains their certification for SSAE 18 and SOC 2 to provide our customers with the needed documentation for auditing purposes.