PROVEN SECURITY TECHNIQUES FOR DATA PROTECTION IN CLOUD

By Claire Kirk, Technology and Compliance Writer

Data protection is one of the leading security concerns for many organizations in the cloud. Without it, the transferring of private data to remote machines just wouldn't be possible. Because of the magnitude of keeping your company's data safe from loss or harm, we have developed this complete list of proven security techniques to give you peace of mind in the measures you put in place.

Protecting data in the cloud can be similar to safeguarding data within a traditional data center. Authentication and identity, access control, encryption, secure deletion, integrity checking, and data masking are all data protection methods that have applicability in cloud computing.

Basic data encryption shouldn't be the only solution you depend on when it comes your organization's cloud data security. In this article, we will compare the various methods of data protection in the cloud, offer up tips for smooth implementation, and touch on some additional ways to make your cloud migration as seamless as possible.

THE STATS ON DATA PROTECTION IN THE CLOUD

Even though public and private clouds are highly secure environments for your data and applications, your organization is still responsible for ensuring data protection and rapid recovery of the workloads you migrate to them.

Whether you're hit with a natural disaster, an outage, or human error, you need fast, reliable, and comprehensive data recovery and protection ready at all times. Data recovery starts with reliable backups. In a recent survey of IT leaders, 75 percent indicated that data protection and backup in the cloud was the most impactful project on their business.

According to Gartner, by 2020, archived personal data will represent the largest area of privacy risk for 70 percent of organizations. By 2021, organizations that are caught lacking in privacy protection will spend more than double the compliance costs of their prepared competition.

Building the necessary framework of trust online requires an identity check to confirm that the individual actually exists and the data provided is valid. Essentially, making sure the person actually is who they say they are.

Authentication relies on data that is difficult to produce, except by that specific person. Full name, social security number, or driver's license number are all personally identifiable information (PII). Physical authentication methods like a badge, fingerprint, and facial recognition are also commonly used.

Single-factor authentication is a great starting place, but it is strongly advised to implement multi-factor authentication whenever possible. Multi-factor typically involves 2-3 verification methods – commonly, your password paired with a one-time passcode (OTP) SMS. Many organizations have also applied Single Sign On (SSO) for their teams, especially in today's highly remote world. SSO allows users to login to multiple applications through one authentication source.

One potential problem to be aware of is using traditional identity methods when partnering with multiple cloud service providers. Make sure they have the proper security and compliance guidelines in place to keep your protected information secure. They should undergo annual third-party audits and be able to show you their completed certifications.

ACCESS CONTROL TECHNIQUES

Access control is a method of guaranteeing that users are who they say they are and that they have the appropriate level of access to company data. At a high level, access control is a selective restriction of access to information. It consists of two main components: authentication and authorization, says Daniel Crowley, head of research for IBM's X-Force Red, which focuses on data security.

Enterprises must assure that their access control technologies are supported consistently through their cloud assets and applications, and that they can be smoothly migrated into virtual environments, like private clouds. The access control mechanism is crucial when supporting complex IT environments at many layers of the stack.

Organizations must determine the appropriate access control model to adopt based on the type and sensitivity of data they are processing. Older access models include discretionary access control (DAC) and mandatory access control (MAC). Role-based access control (RBAC) is the most common model today, and the most recent model is known as attribute-based access control (ABAC).

ENCRYPTION TECHNIQUES

Data encryption in the cloud is the process of transforming or encoding data before it is moved to cloud storage. Typically, cloud service providers offer a range of encryption services to the clients they support. A comprehensive platform should deliver robust access controls and key management capabilities that enable organizations to practically, cost effectively, and comprehensively leverage encryption to address security objectives.

Secure encryption is essential to protect data at rest in the cloud, especially for data that has a long lifespan of value. If your cloud service does not automatically encrypt data before it's uploaded, make sure to do so yourself beforehand. The simplest way to do this is by applying passwords and encryption to files as soon as you are finished editing.

Companies and organizations need to take a data-centric approach to protecting their sensitive information in order to guard against advanced threats in today's complex world of virtualization, cloud services, and mobility.

SECURE DELETION TECHNIQUES

Did you know hackers can still locate data that you have deleted and exploit it? Not properly deleting data on devices and in the cloud can lead to a serious vulnerability for your personal and professional information.

- **Designate a data disposal point person:** Make sure it's someone who knows the lifecycle of data, the policies behind deletion, and how it is managed.
- **Set up policies you adhere to:** Document the process for secure data deletion – what should be done, when it should be done, and who is responsible for it.

A RECOVERY TECHNIQUES

s important each system using cloud services performs an automatic backup at least weekly. For systems storing sitive information, this should happen even more frequently. The overall backup procedure should include the operating system, application software, and data on the machine. Another rule of thumb is to implement multiple backups over time in accordance with regulatory compliance.

Once a quarter, a testing team should evaluate a random sample of system backups by restoring them on a test environment. Systems that are restored should be confirmed to guarantee that the operating system, application, and data from the backup are all functional and intact. If there is a malware infection, restore procedures would use the backup version which predates the original infection.

This can be a daunting task, so it may be worthwhile to tap into the expertise of your cloud service provider and their team of experts.

MIGRATING TO A COMPLIANT AND SECURE CLOUD

While businesses have a high level of control and customization with private clouds, using services on a public cloud could present compliance challenges. All data that is being migrated must meet compliance standards. Thankfully, cloud hosting providers are starting to focus heavily on helping their customers achieve these guidelines.

ORGANIZATIONS ARE NOT COMPLIANT UNLESS THEIR HOSTING PROVIDERS ARE

Recently, regulatory agencies and standard institutions have recognized the value of cloud services. Because of this, new guidelines and compliance updates are continually making the cloud a safer place to store your data.

An example of this includes the additions made to HIPAA. In 2013, HIPAA designated cloud service providers as business associates of covered entities, which means that the cloud service providers must also be HIPAA compliant. The PCI Security Standards Council also released a document that addresses cloud service providers in a PCI compliance context.

FINDING A COMPLIANT CLOUD SERVICE PROVIDER

Every organization may have different standards and attest to their compliance. This is because organizations may be structured to serve industries differently. Despite organizational differences, compliance standards like ISO 20000-1 and ISO 27001 help ensure there are controls implemented.

CLOUD MIGRATION BEST PRACTICES

Customers often wonder what some of the best practices are to quickly and confidently move their data to the cloud. Although each business is different and has varying goals and processes, there are certain patterns in migration strategies that ring true for every kind of company. Here is a short list of some best:

- **Identify the division of roles and responsibilities:** Consider access levels, separation of duties, and decide who is in control of what. Does this job fall on the shoulders of your cloud hosting provider? Is it an internal matter? A great cloud hosting provider will help to clearly define these roles with an enterprise.
- **Outline who owns each IT applications and where applications are being migrated:** Make the distinction of who owns what and where they will be held helps measure the success of your cloud migration.
- **Embrace technology change:** Your company's security and leadership team has already made up their minds to migrate to the cloud. Instead of hesitating and fearing this migration, adjust your internal processes so that they can embrace this change.

LightEdge also utilizes Vision Solutions' MIMIX real-time replication tool designed specifically for IBM Power and IBM i OS, providing a unique backup and disaster recovery solution to the iSeries world.

ntEdge is well known for our ISO 20000 and ISO 27001-validated infrastructure and operations, and constant ierence to reference architecture. LightEdge services are audited regularly to assure compliance with HIPAA, PCI S, SSAE 18, HITRUST, and more.

r highly-trained experts are also knowledgeable about achieving compliance standards like NIST and FISMA. Partner with us to comply with archival and disaster recovery compliance standards.

Data protection best practices recommend maintaining three copies of data, on two types of storage, with at least one in a remote location. This strategy greatly enhances the availability of business-critical apps and data, but it requires separate storage infrastructure.

Ready to put your data protection in the hands of LightEdge's highly trained engineers? Contact one of our data protection experts to get started or to schedule your private tour of any of our data center facilities. We have disaster recovery, colocation, and business continuity experts standing by to answer any of your questions.

If you would like to get more information on disaster preparedness and threat prevention, download our free Guide to Disaster Preparedness or our Cyberattack Threat and Prevention guide.

RELATED POSTS

- Cloud Audits And Compliance: What You Need To Know
- Getting Started with Data Protection Planning
- Workplace Recovery: Getting Your Business Prepared For Success In Any Condition
- How To: Crisis Communication During Disaster Recovery
- Disaster Recovery: An Enterprise Guide Infographic
- What Successful Disaster Recovery Plans Should Cover
- Enterprise Guide to an Effective Disaster Recovery Plan
- How to Make a Business Continuity Plan
- 5 Ways to Prevent Cloud Outages
- The Five Greatest Risks Every Hosting Customer Must Navigate
- Cybersecurity Awareness Month: A Guide to Help Prevent Data Breaches
- Ten Tactics to Protect Against Insider Threats for Cybersecurity

Share this Article

CLAIRE KIRK

With a background in compliance & security, cloud hosting, colocation, and business continuity, Claire uses her knowledge and experience to create educational content for end users. A creator at heart, she specializes in B2B marketing with a focus in content creation and technical literacy.

See Full Bio

Secure and dependable disaster recovery services

Ready to work with LightEdge?

Get A Quote

OUR SECURITY STANDARDS

HIPAA COMPLIANT

AICPA SOC

HITRUST CSF Certified

NIST