Global datavault
A DATAPRISE COMPANY

veeam | CSPPARTNER Platinum

Cybersecurity Guide for Cloud Data Management: Backups and Disaster Recovery

Companies face many challenges when considering security for information technology resources and systems. To guard edge-facing (those that provide access to networks outside of an internal network) and core-facing infrastructure technologies, they must protect all data at all times, and in all locations. Now more so than ever, this includes backup data and systems located in disaster recovery (DR) facilities, as the hope is that these have not been properly safeguarded or maintained and are vulnerable to attack.

Why is the security of backups important?

Primarily, this is answered with the "CIA triangle" for security: Confidentiality, Integrity, and Availability.

Confidentiality

Proprietary company data, and really all company internal data, should be kept confidential. Backups and disaster recovery instances are copies of production data and should be treated with the same stringency. In previous years, companies lost confidential data due to theft of a backup tape. While still possible today, most attacks target the data directly, given the large amount of personal information that exists in a digital state.

Integrity

Just like the integrity of production data, backup data should be kept in a pristine state with the least level of permissions possible given to users, and administrative access should be limited and monitored. Backup data should not be modifiable once written, and it should be tested for integrity. When sending backup data offsite, be sure it is encrypted in flight and at rest.

Availability

Availability is the ability for users to access data and applications when they need them. Backups and disaster recovery exist with this in mind, so it is important to treat them as the only way to ensure availability for your organization. Bad actors and hackers know the importance of backed up data and will target backups and offsite locations in order to prevent restores to get around their malware and ransomware efforts. In addition, they will use 'time bombs' to sit quietly and hopefully infiltrate backup files without alarm until they are activated.

What can my company do to prepare?

The majority of a company's security budget goes to hardware and software solutions that monitor and prevent external access to and from internal network(s). These solutions are usually expensive and complex, but a high-quality door and lock will go a long way in keeping out unwanted guests.

These devices include:

- Next-generation firewalls
- Intrusion detection and prevention devices, specifically with deep packet inspection capabilities
- Email and web filtering and scrubbing systems
- VPN connectivity with multi-factor authentication

Internal policies and procedures must accompany the door and lock. In order to maintain the CIA triangle, internal data and systems must be safeguarded from insider threats, proliferation of malware, and accidental modifications or deletions. Ideally, networks should be segregated, with a separate network for backup traffic both for performance and security reasons.

Other best practices are:

- Implementation and enforcement of strong passwords
- Least-privilege access controls
- Consistently apply software and security patches and updates across all devices
- Antivirus software and scans across all devices
- Administrative privileges removed from computers
- Disable remote access services such as RDP when possible
- BYOD policies
- User education

These apply to internal production systems and data, disaster recovery systems, and all backup systems and data.

Standards and Regulations

Organizations and companies operate in different ways and therefore have different compliance requirements. By default, all backup and DR data should meet these requirements as well.

PCI

The Payment Card Industry Data Security Standard (PCI DSS) is not a law but is a thorough set of rules put forth by the five major issuers of credit cards. The PCI Data Security Standard specifies twelve requirements for compliance, organized into six logically related groups called “control objectives.”

- Build and maintain a secure network and systems
- Protect cardholder data
- Maintain a vulnerability management program
- Implement strong access control measures
- Regularly monitor and test networks
- Maintain an information security policy

HIPAA

The Health Insurance Portability and Accountability Act of 1996 (HIPAA), Public Law 104-191, mandates that all covered entities fulfill certain requirements for data backup, data storage, and data recovery. It was created to protect Personally Identifiable Information and regulate the use and disclosure of protected health information (PHI). These requirements are listed in the Security section of the Administrative Simplification Act.

NIST

NIST SP 800-53 stands for the National Institute of Standards and Technology Special Publication 800-53, Security and Privacy Controls for Federal Information Systems and Organization. NIST is a non-regulatory agency of the U.S. Commerce Department which encourages and supports innovation and science through the promotion and maintenance of the NIST SP 800-53 industry standards and guidelines. These standards help federal agencies and contractors meet the requirements set by the Federal Information Security Management Act (FISMA).

Sarbanes-Oxley (SOX)

The Sarbanes-Oxley Act of 2002 (SOX) ushered in a new era of business rules regarding the storage and management of corporate financial data. Sarbanes-Oxley Compliance holds many publicly held companies and all registered public accounting firms to a rigorous set of standards. These rules set guidelines for how data should be stored, accessed, and retrieved.

Other regulations exist and may or may not be requirements for your company. Discuss these requirements with all third-party vendors, data center providers, and managed service providers to understand their participation or compliance related to your needs.

User Education

Ongoing education of users by a company’s own IT department is an effective defense for human-related cyberattack tactics such as phishing and recognizing suspicious websites and behaviors. The internal IT department is recognizable and knowledgeable of the systems users access on a daily basis. Many people are simply unaware of the sophistication of malicious emails and websites and need to be educated on proper use of corporate systems for transmitting data.

Additionally, education around the use of social media, if your company allows access to it, is important. Hackers will use any method they can to gain access to internal resources, even going as far as creating fake websites and links that look official in order to gain credentials.

Finally, users should know that reporting suspicious activity is encouraged, even if that user may have inadvertently caused an issue. Fear of repercussions could prevent users from coming forward about something that could have disastrous impacts on a company.

Create a Cybersecurity Incident Response Plan

Possibly the most important thing a company can do for cybersecurity preparedness is to have a plan, such as a security event response checklist. No plan or list will be able to cover every potential threat or issue that may arise, but it is the best option for calm, organized action during what may be a stressful situation.

Keep a record of assets

With cloud mobility and multi-cloud workloads becoming more prevalent, cloud data management is more important than ever. It can present its own challenges when understanding the effects of geographical outages, compliance, application and database performance needs, and data protection and recovery options. Understanding the location of workloads is key to security and availability.

Identify the risks and business impact for outages

An inventory of IT assets shows which data and systems could be at risk if the event of an incident. You can identify which assets pose the greatest risk if compromised and prioritize how you will respond and protect them. Additionally, a business impact analysis can give you an in-depth look at the data that you need to protect. You should also work out what an attack could potentially cost you, as these events will likely have an immediate financial impact and could also have long-term effects on your reputation and image as an organization.

Identify threats

Realizing and identifying threats as quickly as possible is key to preventing problems from developing fully. While a security operations center is beneficial for the overall management of security performance, many of these tasks can be better performed by hardware or software solutions.

Determine courses of action

Consider how to respond to a security incident determine relevant action items and who will be responsible for doing them. These should not only address the immediate IT issues at hand, but also include the operations of the rest of the business. For example, you might need to have a plan for how to communicate any technology problems that could affect services for your customers. Identifying which systems are most important and determining the order of recovery is important to be able to return service. If using a backup-as-a-service or disaster recovery-as-a-service provider, discuss these items on a regular basis to will eliminate confusion. Incident response and recovery tasks should be specific and assigned to specific people. Everyone should know what they need to do so that all tasks can be carried out as quickly as possible without panic.

TEST THE PLAN

Test the response plan on a regular basis to ensure all components are captured and covered, all parties are identified and familiar with their tasks, and all portions work as intended. Adapt the plan as necessary to keep it workable and efficient.

UPDATE THE PLAN

Allowing a plan of this sort become outdated is possibly worse than not having a plan at all. If information is missing or incorrect, it will be difficult to tell what needs to be fixed or recovered, so be sure to update the plan when changes are made to the environment. At a bare minimum, the plan should be updated quarterly, but a better solution would be to update it whenever MACD (move/add/change/delete) events occur.

Considerations for Cloud Backup Repositories and Backup-as-a-Service (BaaS)

Using cloud resources for offsite backup storage is a cost-effective method for protecting data. When coupled with a managed service provider, the challenges and risk of cloud storage can be reduced, if not eliminated. The BaaS provider will review your security needs versus what they offer—identifying systems and security requirements prior to this is important and will save time, but your BaaS provider may assist with this process.

When looking for a cloud provider, and specifically a cloud and service provider combined, you should look for:

- Physical facility security and data center audit compliance
- Background checks on provider staff
- Data encryption practices
- Shared responsibilities
- Controls and regulations – Compliance
- Customer data integrity and testing practices
- Network segregation
- Security monitoring and response practices

The Global Data Vault Perspective

At Global Data Vault, our business is providing services specifically tied to customer data. We understand the importance of the CIA triangle and have built a reputation on delivering what our customers expect and more. To us, all customer data is secret and confidential. If we allowed the integrity of your data to come into question, we would not be performing adequately, and we will guarantee the availability of your data within all defined SLAs.

Most of our internal security framework is based on programs from the SANS Institute.

GDV Security Ops Center-as-a-Service solution for our data centers, which we extend to our touchpoint into a customer environment. This provides automated incident response at an expert level and is attuned to our BaaS and DRaaS offerings.

We also continuously innovate and develop technology such as Enhanced Data Protection for our customers.

Security incidents can be stressful times. Global Data Vault is committed to take responsibility for assisting your company during any issue, and return you to operations as quickly and easily as possible.