SYSTEMS engineering

WHITE PAPER

Data Governance and Data Protection

SYSTEMS engineering

WHITE PAPER

Data Governance and Data Protection

There are frequent articles in the news about data breaches, ransomware and identity theft which is causing many organizations to reexamine at their incident response and business continuity plans. When going through the exercise, it's important to remember that data governance and data protection, otherwise known as backup and recovery, have important roles to play.

DATA GOVERNANCE POLICIES

The definition of data governance is "the organizing framework for establishing strategy, objectives, and policies for corporate data."[1] In short, knowing where your data is, identifying which locations contain sensitive or private data, and limiting access to those who have the privilege to see it. Data is very important in allowing organizations to grow and thrive. **Deciding how to protect and store that data is the next step in what data governance consists of.** There are two types of data that most businesses are comprised of: structured and unstructured data.

- **Structured data is the critical accounting, management, and production data stored in a database. Without these important electronic items, your company would probably enter panic mode. Disarray and disorganization might ensue.**
- **Unstructured data makes up most of the work day; these consist of the daily files such as Microsoft Office and Adobe PDF documents, and might also include media files. Choosing which of these documents are the most important to keep and protect; controlling where these are stored will ensure that a businesses' data governance program is structured and well prepared.**

On a similar note, what would your organization do if there was a true disaster? Here are some questions to consider:

- **How long would it take to recover your systems?**
- **Have you tested your recovery plan to verify how long it takes?**
- **Do you have a failback plan following a disruption?**

DATA PROTECTION DEFINED

If you are in charge of organizing your company's file and systems recovery plan, there are specific items that need to remain top of mind. For example, two terms that organizations should be familiar with are "Recovery Point Objective" and "Recovery Time Objective." These two terms are defined as:

- **Recovery Point Objective (RPO): How much current data can you afford to lose? For many organizations, this is 24 hours; most have a daily backup ensuring that only one day's worth of work would be lost. Other organizations may require an RPO of hours, minutes or even seconds.**
- **Recovery Time Objective (RTO): How long can you afford to go without access to your data? Again, for many organizations this can be 24-48 hours. Other organizations may require an RTO of hours or minutes even in the case of a total loss of their offices.**

It's never a comfortable place to be when data is lost and where time lapses before it is returned, if it is able to be recovered at all.

The Scary Truth

Up to

40%

of businesses affected by a natural or human-caused disaster never reopen."[2]

PROTECTION STRATEGIES

To optimize cost and recovery time, organizations need to make a decision about how various applications and data are protected. By having the fundamental protection measures in place and by having a plan, the likelihood that an entire system will be lost will be minimized.

Data protection strategies to consider include:

- **FAULT TOLERANCE: Reduces the likelihood of data loss due to a hardware failure. All applications and hardware should be on fault tolerant systems.**
- **FILE RECOVERY: The recovery of lost or corrupted files over a minimum of the past 30 days is essential for all critical data.**
- **REPLICATION: Allows you to achieve disaster recovery time objectives of 24 hours or less at a remote site by creating replicas of your virtual environment and its corresponding data.**
- **ARCHIVING: Maintains the long-term retention of files subject to regulatory compliance and eDiscovery requirements. Having a data governance policy for document archiving is the most important step.**

At Systems Engineering, we recommend clients map their data and applications to appropriate levels of protection (keep in mind that it might take more than one solution to fit the needs and budget of the business). For example, organizations could justify the replication and rapid recovery of one or two critical applications, yet leave the remainder of systems protected by a less costly solution with higher RPO and RTO. We also recommends that all data and applications are protected by fault tolerant systems that are backed up at the file level.

This can be confusing and complex and knowing all the options, including the underlying costs, when transitioning to a replication solution is important. Understanding the past, present, and future of your data protection plan can make long-term decisions more efficient.

ABOUT SYSTEMS ENGINEERING

Systems Engineering is an IT strategy and managed services provider delivering world-class technical and business solutions to enable the exceptional within organizations. Established in 1988, Systems Engineering is a 100% employee-owned serving more than 500 legal, healthcare, financial services, and government clients nationwide. Headquartered in Portland, ME with an additional office location in Manchester, NH, the company has a team of 150+ who are available 24×7, 365 days per year to serve the needs of its clients. Known as a forward-thinking, modern technology partner, Systems Engineering seeks to enhance business by providing superior managed IT, security, cloud, and consulting and IT leadership that allows companies to grow and prosper.

To enable the exceptional within your organization, visit systemsengineering.com or call 888.624.6737.

References
[1] *www.sas.com*
[2] *Insurance Information Institute*