

How Secure is Your Storage?

Protecting critical systems and data with regular backup images and recovery processes

By Steve Fairbanks, Symantec Corp.

According to Strategic Research Institute, companies that aren't able to resume operations within ten days of a disaster hit are not likely to survive. Many factors can cause data loss, including: fire, power outages, employee theft, viruses and hackers, as well as modern tragedies that can leave companies without access to buildings and important documents.

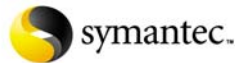
Data back-up is no longer just "IT's problem." The business costs associated with network downtime and data loss make secure backup and recovery an economic necessity. IT professionals and their businesses have learned the hard way in recent years that is not a matter of "if," but a matter of "when" disaster recovery is needed. A recent study by Pepperdine University states that 40 percent of data loss stems from hardware failure and 29 percent from human error.

At some point, every company is going to be faced with some type of data loss. Regardless of the cause, those that are prepared have a much better chance of overcoming the loss with minimal damage. Specific procedures for creating backups and a plan of action for recovery are essential to any modern business in order to secure storage.

Upwards of 60-70 percent of companies begin a disaster recovery plan, but don't finish because the plans seem too complex, overwhelming, or get put on the back burner. However, this is something that cannot be overlooked. Below are some of the best practices that should be included in every company's processes.

The Importance of Creating Regular Backups and Verification

It is essential for companies to regularly create backups of their systems. This may seem obvious to most, but often times the problem is not so much that companies are not creating backups, but that they are not verifying their recoverability. This results in "false backups" where they think their data is secure, only to find in an emergency that the backups failed and the data has been lost. This is especially true with tape backups as tapes can be more easily corrupted, damaged, worn out, or employees can forget to change the tapes. In either case, it is too late and data is already lost which can often take weeks, or even months for these systems to be restored, if ever. Therefore, it is extremely important for companies to follow best practices and create policies and procedures for creating regular backups and for testing their recovery environments. Among these policies should be regularly scheduled test recoveries in order to ensure that backup



policies and procedures are working properly. It is suggested that these recovery events be conducted at least once a quarter to make sure backups are running as planned.

Proactive Protection

Companies should also use preventative measures to ensure that systems are safe guarded as much as possible. This includes the use of antivirus software, firewalls, and intrusion detection software. Intrusion detection is important because it is much like an alarm system that will further protect vulnerable data from both internal and external threats because it monitors critical files for tampering and checks network traffic for “attack signatures.” If it detects an anomaly, an alarm notifies the administrator for further investigation or action. With intrusion detection, if an attack should occur, companies will have early warning and can quarantine the threat and their current backup data, before damage can be done to critical systems and result in data loss or corruption. It is also important to consider using products and best practices for integration from the same vendor, so that continuity planning can result in a comprehensive solution that is easily managed.

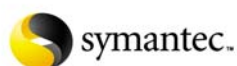
Recovery Plan

Along with backups, companies must also implement fast recovery plans in the event of data loss or systems interruption. The first step in planning for recovery is the assessment of your environment. When assessing what to include in a disaster recovery plan, companies should keep in mind the following:

- What network resources are most important?
- What is the value of those resources, monetary, or otherwise?
- What possible threats do these resources face?
- What is the likelihood of those threats being realized?
- What would be the impact of those threats on the business, employees, or customers, if those threats were realized?
- Which resources do you need to bring online first?
- What is the amount of time each one of these resources can be down?
- Set an allowable downtime for each resource.
- Set decontamination process for viruses, worms, etc.

When determining the value of an asset, organizations must consider both its monetary value and intrinsic value. Monetary value can be determined by considering what would happen if the asset was unavailable for any reason. Intrinsic value is the loss of data, privacy, legal liability, unwanted media exposure, loss of customer or investor confidence, and the costs associated with repairing security breaches. Once information assets are identified and valued, threats to those assets must be evaluated.

Although types of sensitive data can be quite broad and vary from organization to organization, there are a few key types of information that every business should plan to protect. These include all data related to strategic plans, business operations, and



financial data. Damage to or loss of any of this information can result in decreased sales, reduced competitive advantage, and decreased profits for the victimized company.

Companies also need to make sure that their backup, retention and recovery policies comply with industry standards and government regulations when thinking about the security of their storage. Industry guides such as the International Standards Organization (ISO) 17799 and government regulations such as the Gramm-Leach-Bliley Act (GLBA), the Health Insurance Portability and Accountability Act (HIPAA), and the Sarbanes-Oxley Act help provide a framework for improved corporate governance and controls. Accurately written and enforced, information security policies enable organizations to not only demonstrate their adherence with these critical regulations and standards but also articulate their own.

Conclusion

Disaster recovery is something every company needs to consider—now. In today's unpredictable and often times unstable world, no longer can companies sit back and wonder if something will happen, but rather must think about what to do when something does happen. The only truly secure infrastructure is a managed infrastructure. The only way to make sure companies are protected as much as possible before an attack, is to integrate security policies with regular and effective backups of their systems and important data. Additionally, they must have a recovery plan in place for when a disaster strikes. While putting together a systems continuity plan can seem like an overwhelming process, trying to recover from a disaster quickly is near impossible without such a plan. While disaster recovery is unique to each company and its environment, the guidelines mentioned above can serve as a solid foundation. While an often difficult and easily put off task, strong backup and recovery plans are essential for survival in the modern business world.

For further information please contact:

Symantec UK Ltd
Hines Meadow
St Cloud Way
Maidenhead
Berkshire SL6 8XB

Tel: +44 (0) 1628 641803
Internet: <http://sea.symantec.com>