CYBERSECURITY

Do You Have Effective Data Backup Procedures in Place?

By Jake Omann, CIC, CPCU
Management Liability Segment Leader

www.usi.com

THE USI ONE ADVANTAGE®

Your company's data is one of the most precious resources you have. Loss of data, especially with no viable backup, can have catastrophic consequences. Cisco's 2018 Security Capabilities Benchmark Study shows that 40% of mid-sized employer experienced at least eight hours of system downtime due to a security breach. According to the 2019 Cost of a Data Breach produced by IBM with the Ponemon Institute, the average cost of lost business as the result of a breach—including business disruption and system downtime—is $1.42 million, over a third of the total cost of a data breach.

A solid data backup strategy is a critical component of your business resumption plan. Developing an effective backup plan requires an investment of time and money, but the cost is far less than the burdensome task of recreating data for which no backup exists. Backups ensure that your critical data can survive most hazards. Too many individuals and companies have suffered from having their hardware lost or stolen, infected with malware or corrupted by ransomware attacks. Common sense dictates that all hard drives will eventually fail. The question is whether or not you are prepared for the worst-case scenario.

Prepare with a playbook

Having a plan to protect critical data on the front end is only half the battle. It is also essential to have procedures in place if and when a security crisis occurs so you can respond quickly and effectively. Timing is important, because a number of regulations and laws require notifications to take place in a defined period of time. Security incidents can be confusing, especially if you don't practice your response. Running through a playbook of strategies for handling multiple scenarios can help you stay grounded and minimize damage if you face a real crisis. Having this information well-planned in a playbook format allows you to respond appropriately and in a timely way.

The 3-2-1 backup rule

Multiple computer systems, especially virtual environments containing thousands of devices and access points, makes protection and recovery much more complicated. A comprehensive data protection plan should include the 3-2-1 backup rule. This backup rule is a common approach to keeping your data safe in almost any failure scenario. The rule is simple: keep at least three copies of your data, and store two backup copies on different storage media, with one of them located offsite.

- Keep at least three copies of your data: one primary and two backup.
- Store two backup copies on different devices or storage media, so you always have access should one storage method fail. Use a combination of internal and external storage options such as an external hard drive or cloud storage. Another good option is a Network Attached Storage (NAS) device, a smart hard disk box that connects directly but acts independently from your network infrastructure.
- Protect against physical perils such as theft, fire, flood or natural disaster by keeping at least one copy of your data in a remote location, such as offsite storage or the cloud.

Having a business disruption plan and an effective backup procedure ensures that your operations can get back to normal as quickly as possible following an interruption. A comprehensive cyber liability policy can help provide additional coverage and support in the event of a data breach or other cyber event.

For more information about effective data backup procedures, please contact us at 800-258-3190 or MNWI.Info@usi.com.