Barracuda

The Value of Offsite Storage

White Paper

Regardless of the industry in which you operate or the size of your business, having a solid backup and recovery plan is vital. No business can afford to gamble with its data by using outmoded or high-failure backup methods. In today's world of cost-effective high speed Internet connectivity, data can be protected effectively by shipping it over the wire and storing it at secure offsite locations where it can be accessed in a time of need.

One thing is certain: data loss is inevitable. An estimated 6 percent of all PCs will suffer at least one episode of data loss per year. Indeed, 20 percent of laptops will suffer hardware related data loss in their first three years of use. A CBI/FBI survey revealed that 52 percent of respondents discovered unauthorized access to their systems, and 47 percent had experienced laptop theft.[1] A recovery plan that includes offsite storage as a fundamental component will offer a degree of protection that can not be duplicated with an onsite-only solution.

[1] 2006 CSI/FBI Computer Crime and Security Survey," Computer Security Institute / Federal Bureau of Investigation.

Disasters and Consequences

For some business owners and IT administrators, whether or not they have any data backup system at all becomes their single standard in determining disaster preparedness. In reality, every business has different backup requirements, recovery needs, and priorities, and should create a regular process to analyze and identify critical systems recovery procedures in the event of a total loss. Each business and possibly each system a business utilizes may have different requirements for acceptable recovery time and effort. These should be related to the available recovery options and their associated costs.

According to an article in Pacific Business News, "Of all businesses that close following a disaster, more than 43 percent never reopen. An additional 29 percent close permanently within two weeks."[2] There are a variety of reasons for the high failure rate, and a variety of controls that can be implemented to minimize the damage. Among those controls is a plan for your data that has it stored securely in a place other than the one being rebuilt.

[2] http://www.bizjournals.com/pacific/stories/2004/04/26/focus6.html

Disaster can strike in a variety of forms. Most commonly, the word "disaster" evokes images of earthquakes, fires, floods, landslides, hurricanes, and tornados. These typically fall into the category of natural disasters. There are a number of increasingly common man-made threats that can similarly destroy data and render a business non-functional. These directed threats include viruses, hackers, sabotage, and burglary.

Prior to offsite replication, system administrators would most commonly back up to portable media and either walk critical data offsite themselves or pay a service to vault it. A visit to the "Chronology of Data Breaches" at http://www.privacyrights.org instantly and often shockingly demonstrates the pitfalls of physically moving data. The Data Breaches list is littered with examples of lost or stolen data. This risk inherent to portable media can now be avoided with a better and more secure backup solution.

- **April 27, 2006 – Long Island Railroad (Jamaica, NY)**

  Data tapes containing personal information including names, addresses, Social Security numbers and salary figures of "virtually everyone" who worked for the agency was lost by delivery contractor Iron Mountain while en route. Data tapes belonging to the U.S. Department of Veteran's Affairs may also have been affected.

- **May 15, 2007 – IBM (Armonk, NY)**

  An unnamed IBM vendor lost computer tapes containing information on IBM employees – mostly ex-workers – including Social Security numbers, dates of birth, and addresses. They went missing in transit from a contractor's vehicle.

In addition to grave financial risks, losing data can place an organization in violation of numerous government regulations that often mandate reporting of the event. The Health Insurance Portability and Accountability Act of 1996 (HIPAA), the Sarbanes-Oxley Act of 2002 (SOX), Gramm-Leach-Bliley Act (GLBA), and Rule 26 of the Federal Rule for Civil Procedure all require secure data storage, backup, and recovery capabilities. Executives and boards of directors with fiduciary responsibilities are now often liable for proper protection of information.

Securely Stored Data

Safely stored data is both a physical and a logical consideration. Having established that offsite storage is the best way to ensure data integrity in case of a disaster, the manner in which data is stored is critically important. When the Barracuda Backup Server is installed and configured, it will perform an initial backup of all selected data and store it locally. An advanced digital cataloging system shreds data into small pieces and tracks the changes of these parts over time to make sure duplicate data is not being retained. This deduplication helps minimize storage and bandwidth costs as it prepares to send data offsite.

To create an offsite copy of critical data, the Barracuda Backup Service sends data, to one of two secure data centers via the Internet using an encrypted IP tunnel. Before data is transmitted, those shredded and cataloged parts are symmetrically encrypted (AES256 bit) then compressed for transfer and remote storage efficiency. The symmetric key to unlock those parts is in turn asymmetrically encrypted (RSA1024 bit). The United States Government has approved 192-bit AES encryption as an acceptable method for protecting Top Secret information.[3] Not only does the Barracuda Backup Service encryption method exceed that specification, but across the Internet, data is protected by three separate encryption algorithms two layers deep.

The last copy is created when replication occurs between the two data centers. All data is mirrored from one to the other and can be accessed from either. Barracuda Networks distributes data for each customer across two geographically dispersed data centers to minimize the potential impact of an event at either location. Each data center is highly secure including alarms, controlled access, fire suppressors, redundant bandwidth, and emergency power generators – everything necessary to ensure valuable data is not in danger.

Planning for Recovery

The Barracuda Backup service was designed with recovery in mind. Administrators manage the device through a Web interface. Because all critical data is kept offsite and administrative instructions are sent from the Web interface down to the Backup server, nothing critical is lost if the server is damaged. Barracuda Networks provides a number of tools and protocols to access and restore data either from the local box or from the cloud. This includes the Web interface, the Barracuda Restore Tool, WebDAV, and even FTP. A business can begin restoring data from the cloud as soon as it has connectivity. In the event that local backup server is a total loss, and there is a significant amount of data that needs to be restored quickly, Barracuda Networks Technical Support can load data on a hard drive or a replacement Barracuda Backup Server and ship it.

Don't Get Caught Unprepared

Clearly, neglecting to protect data until disaster strikes is an extremely high-stakes risk. In the event of a disaster, the likelihood for a company's survival drops dramatically without access to critical data like company financials, accounts payable records, or customer records.

The overwhelming dependence of modern businesses and organizations on information to operate and remain profitable dictates the necessity of an affordable plan that allows for full and immediate recovery. A business should never be in a position where all of their data exists on a single device or at a single location. As a result of advances in technology and design, organizations can now manage these together at an affordable rate.

[3] Lynn Hathaway (June 2003). "National Policy on the Use of the Advanced Encryption Standard (AES) to Protect National Security Systems and National Security Information" (PDF). http://www.cnss.gov/Assets/pdf/cnssp_15_fs.pdf

To learn more about Barracuda's web security solutions, please visit www.barracuda.com/products or call Barracuda for a free 30-day evaluation at 1-408-342-5400 or 1-888-268-4772 (US & Canada).

About Barracuda Networks, Inc.

Protecting users, applications, and data for more than 150,000 organizations worldwide, Barracuda Networks has developed a global reputation as the go-to leader for powerful, easy-to-use, affordable IT solutions. The company's proven customer-centric business model focuses on delivering high-value, subscription-based IT solutions for security and data protection. For additional information, please visit www.barracuda.com.

Barracuda

Barracuda Networks
3175 S. Winchester Boulevard
Campbell, CA 95008
United States
408-342-5400
888-268-4772 (US & Canada)
www.barracuda.com
info@barracuda.com