

“Did you know that over 60% of businesses that suffer catastrophic data loss close their doors, and go out of business within two years?”

Data is your most critical asset: Protect it with

eSecure Backups

Easy to Start

Free Client Software
User Defined Pass Codes
User Defined Scheduling

Easy to Use

No Disk or Tapes
Incremental Invisible Backups
Regular Backup Reporting

Easy to Maintain

Full Technical Support
Full Data Accessibility
Full Data Versioning

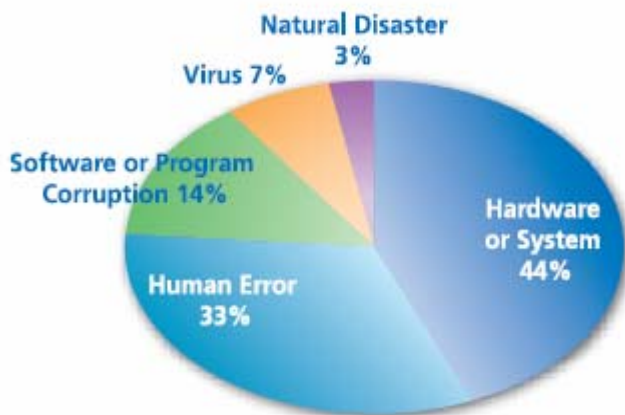
Call for your free consultation today



Data at Risk— How We Lose It

Without an adequate backup and recovery plan, your business is at risk. Because your company relies on its data and mission- critical applications, the cost of downtime is exorbitant, potentially exceeding thousands of dollars per hour for such expenses as recovering data and system files, replacing equipment, losing productivity, and losing customers. A recent study reveals the “precarious position” of small business backups: 30% lack formal data backup and storage procedures, 39% review their storage procedures only after a problem occurs, 34% admit to only fair or poor performance in storing backup data offsite, 17% don’t consistently perform incremental data backups, and 55% rate their disaster recovery plan as fair or poor. According to a disaster recovery study, nearly half of the companies that are unable to fully restore their data after a disaster will go out of business entirely².

http://www.exabyte.com/support/online/documentation/whitepapers/PDF%20to%20HTML/basicbackup/html/BackupGuide_3.html



The most common disasters suffered by respondents included hardware failure (22 per cent) and utilities failure (18 per cent), followed by deliberate or malicious damage (14 per cent).

<http://news.zdnet.co.uk/itmanagement/0,1000000308,39119002,00.htm>

Here is a startling statistic, courtesy of research company IDC: 40 per cent of small and mid-sized businesses never back up their data. Here’s another that puts the first one in perspective: 70 per cent of small businesses go belly up within a year of suffering a major loss of data.

<http://www.theglobeandmail.com/servlet/story/LAC.20070517.TWDATABACK17/TPStory/Business>

Two situations have to occur in order to lose data: (1) the data is not backed up, and (2) the original copy is lost or corrupted. Human error accounts for fully a third of data loss occurrences (see chart above).

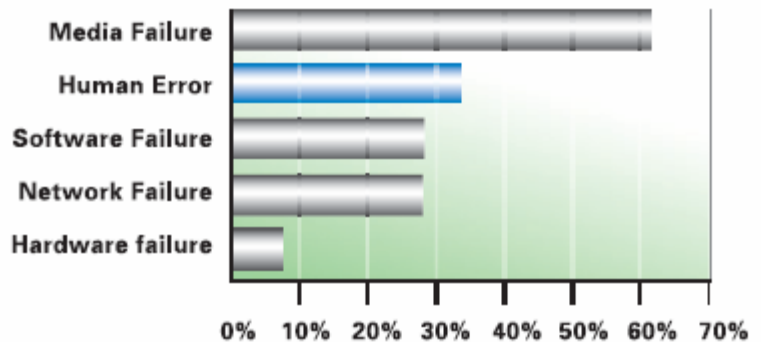
Here is a startling statistic, courtesy of research company IDC: 40 per cent of small and mid-sized businesses never back up their data. Here’s another that puts the first one in perspective: 70 per cent of small businesses go belly up within a year of suffering a major loss of data.

<http://www.theglobeandmail.com/servlet/story/LAC.20070517.TWATABACK17/TPStory/Business>

As evidence of data loss devastation, 90% of all companies that experience data loss because of disaster are out of business within two years, and nearly 50% never reopen <http://www.exabyte.com/support/online/documentation/whitepapers/affordabletapeautomation.pdf>

*Exabyte's own documentation shows the primary reason for data restoration failure is bad media:

Reasons for failed data restoration:



Data Storage Facilities and Equipment

eSecure Backup Data Center

The eSecure Backup system is designed to a secure, reliable, efficient, scalable, modular, and portable data backup solution. Our facilities are located in Atlanta, GA in a secure Tier 4 datacenter location . The servers are maintained by 4 Main, State of the art, UPS Systems, powered by 3 Generators with in ground 5000 gallon fuel tanks (each rated 1.5 megawatt and 800 KVA) to ensure power if there is an outage, and a connection to the most reliable power grid in the state of Georgia through quad vaults on 4 feeds. Eight 22-ton Redundant Liebert Air systems providing consistent temperature and humidity range in the datacenter. This grid protects the main hospital in Atlanta so it is on a last outage program for critical services and was extensively upgraded for the Olympics. For the last 5 years the generators have only been used for testing.

Security and Protective Systems

The site is protected by a state of the art data center ID system and security which includes video surveillance and recording. All entrances to the Data Center have biometric scanning in combination with card key to prevent unauthorized access. It utilizes FM200 Fire suppression and active monitoring with VESDA early smoke detection. Redundant Cisco BGP routing and switching infrastructure with cold spares on site. In the event of equipment failure, there is no interruption of service. Our systems use 10 Gig Metro Ethernet ring for the core routing. Dual feeds of all aggregation routers ensure 100% uptime. State of the art Avaya ANS BGP management system optimizing routes on the 6 gig network in real time, 7000 times per minute based upon trace route performance, ensuring servers have the highest performance routing vs. a simple BGP configuration. We also employ state of the art monitoring system for all servers and network devices with instant failure notification.

Network Backbone

Our network infrastructure consists of 6 basic backbone providers who are publicly peered with 12 major ISP providers including Earthlink. Our current network consists of Gigabit links to Abovenet, XO, PCC-BTN, SAVVIS, Telia, Level 3 and the Atlanta Internet Exchange public peering point. The Network depends on a few large pipes from quality providers to handle spikes in traffic and occasional DoS attacks as well as unknown traffic patterns in the case of a primary link failure. The network minimum Internet backbone connection is a 1 Gig pipe.

Data Encryption

Information encrypted by our client program uses the AES-256 symmetric encryption algorithm. The 256-bit encryption key (as well as another 256-bit HMAC key) is generated by running the PBKDF2 algorithm on the pass phrase as described in RFC 2898. Each file is divided into 2K blocks. Each block is compressed using zlib deflate and is encrypted using AES-256 in CTR mode (each block uses a different crypto-random nonce), and an HMAC (using SHA-256) is appended (to guarantee integrity upon restore). The data is fully compressed and encrypted before it ever enters the network. Encrypting the data on the client is more secure, and it makes the server more efficient and scalable. Filenames are currently not encrypted. Encryption of file and directory names is a planned future enhancement, and can be done by upgrading the client software – no changes need to be made by the server.

Revision Management

The use of compression and encryption precludes the possibility of performing file delta calculation at the server. Performing the delta calculation at the client also increases server scalability and efficiency. As each block is stored on the server the client stores a 64-bit CRC (two 32-bit CRCs generated from different polynomials) associated with

that block. During the next backup if a file has been changed (its modified date/time stamp has changed or its size has changed) then the client will compare the new 64-bit CRC with the stored CRC. If the CRC has changed the client will upload the new compressed and encrypted block. Otherwise the client will tell the server that block has not changed. The CRC block fingerprints and other data are protected by transactions such that if the backup of a file fails, all 64-bit CRCs and other information are rolled back to the consistent state.

Pass Phrase Recovery

The pass phrase is central to the system's security. A strong pass phrase is vital for sufficient encryption strength. However, a strong pass phrase can be hard to remember, and all data would be worthless without the exact pass phrase. Thus, a secure pass phrase recovery system has been implemented.

Client/Server Protocol

Each end user is given an account username and password (which can be changed). The client connects to the server via a TLS (SSL) connection (providing confidentiality and integrity), and requires the server's certificate to be issued by the eFolder Repository root certificate authority (to prevent spoofed servers from stealing login credentials). The client authenticates to the server with its username and password. At this point the server may redirect the user to a different server and port. This greatly increases scalability, as all clients point to the same login server, but can be redirected to their data server according to need. Data servers can be added on demand, and an account's data can be moved to larger servers as the account grows. The end user is not aware of this complexity and never needs to change anything. The communication protocol itself is an endian-independent, flexible protocol designed to support changes without breaking backwards compatibility.

Data Repository

All data is stored as files within the server's file system. The server is portable and runs either in Win32 or Linux. Servers currently run on SuSE 9.3 Linux using the ReiserFS 3.0 file system with the tea hash function. ReiserFS is a modern journaling file system supporting multi-terabyte partitions, 64-bit file sizes, and millions of files per directory, making it preferable over NTFS. RAID-6 is used for all repository partitions. Each account is assigned a subdirectory and contains subdirectories for root backup folders. Each root backup folder contains the following subdirectories:

data: Current versions of files

meta: Historical versions of files

deldata: Deleted versions of files

delmeta: Deleted, historical files

index: mirrors the directory structure so the directory list can be generated quickly

The current version of the file always stores the complete file (encrypted and compressed). Historical versions store data blocks that differ from the next (more recent) version. Thus, to restore the 5th version of the file you apply the deltas from the previous 4 versions and then apply the 5th delta. This is done as the file is downloaded and is very efficient. Also, this method makes uploading new versions efficient, as all previous versions need not be changed. When the client detects that a file has been deleted it notifies the server during the next backup. The server annotates the filename with the deleted date/time and moves it to the deleted data area. The client program will enumerate and destroy old deleted data once a week. An end user can use the file manager to destroy data. When data is destroyed it is moved to a parallel repository designed to hold the "destroyed" data. Destroyed data is held for an additional 30 days, in case the destruction of data was unintentional. Because all repository data is stored as files within the native file system, an account's data can be managed easily using the native operating system's utilities. Additionally, existing technologies and utilities to mirror file systems (such as rsync) can be used to provide additional protection against data loss.

Account Management

All account information is stored in a PostgreSQL database. The login server and the data server must connect to the same database, or replication must be employed to keep the databases consistent. The database also contains billing information and a detailed audit trail.