In today's computing environment, businesses are relying on computers to perform daily business activities as well as mission critical functions. The use of computers in business is essential to maintain a competitive edge in almost any marketplace. As smaller companies begin to realize the benefits of computers for bookkeeping, customer databases, word processing, e-mail, scheduling, research and web sites, the need to have a backup copy of this data becomes more important. Research has shown that more than 80% of the businesses suffering from catastrophic data loss have gone out of business with 12 months. This is not hard to believe considering the extent computers are relied upon in businesses of all sizes.

The issue of data protection is not a new issue. Data security has traditionally been more of a large corporate concern because many smaller businesses did not have the computing systems utilized by larger corporations. Today, with the low cost of computers and easy access to the Internet, businesses of all sizes have the ability to utilize computers for many important job functions. Small businesses rely on computers to automate and simplify tasks in order to reduce the costs of running a business. As such, any loss of data is a significant business risk. With secure off-site storage capabilities offered by FirstBackup, small and large businesses alike can automatically protect their data on a daily basis to ensure business continuity.

ENCRYPTION

When proposing the benefits of off-site storage using the Internet as the communications medium, users may raise a concern about the security of their data. Whenever data privacy is an issue, some type of encryption must be employed to insure that the data can only be accessed by authorized users. Encryption allows a user to specify an access code or password which is used to make computer data unreadable to anyone without the correct password. There are hundreds of encryption algorithms available today, but a few stand out as industry leaders. The DES algorithm is a popular algorithm that has been used by the U.S. Government as the standard encryption algorithm. Another algorithm gaining popularity is the Blowfish algorithm which allows a more powerful encryption and faster performance than DES. These encryption algorithms are available in FirstBackup.

DES

Adopted in 1977, DES is based on a conventional or secret key system in which the sender and the receiver use a single key to encrypt and decrypt data. The sender uses the key to convert the data to scrambled format according to a complex mathematical algorithm, and only users with the correct key can successfully decrypt the data.

Having a key length of 64 bits, 56 are used as a key, while the remaining eight are used to check for errors. The DES algorithm will encrypt data in the same amount of space used by the original data. The user selects which one of more than 72 quadrillion transformation functions are to be used by selecting a 56-bit key. The theory behind the security of DES has been that, short of trying all 72 quadrillion combinations, there is no way to "break" the algorithm.

Triple DES

To increase the security of DES, some organizations use "triple DES" - or three operations of DES with two keys - to protect data. This method, however, requires more processing power, which may affect performance.

Blowfish

Blowfish was designed in 1993 as a fast, free alternative to DES. Unlike DES, however, the Blowfish algorithm has a variable key length, which can be extended from 32 bits to 448 bits. Blowfish continues to gain acceptance in the marketplace because it is faster and more secure than DES.

THE FIRSTBACKUP PROCESS

FirstBackup utilizes encryption in several key areas to ensure that the user's data is secure.

Communications

Since the information is transmitted across the Internet, the communications between the user and the server should be encrypted to prevent a malicious person from intercepting data as it is transmitted over the Internet. As part of the initial connection procedure, the FirstBackup client software negotiates a compatible set of encryption methods before sending any user information or data to the server. This ensures that all user communications during the entire backup and restore process are completely encrypted.

Storage on Server

When the encrypted backup data has been successfully received by the server, it is immediately stored on the disk in the encrypted format and the filenames are further encrypted to make it more difficult for someone to identify the user data on the server. Data must be encrypted while stored on the server to prevent any unauthorized user from accessing the data files. Even if the physical storage devices were damaged or stolen, the encrypted data could not be compromised.

Storage on Client

Important information such as the user's password must be stored on the client computer in order to facilitate the logon process to the FirstBackup server. This password and other important information is stored on the client system in an encrypted format that can only be read by the FirstBackup application.

User Authentication

User authentication is performed immediately after the encrypted/secure connection between the client and server has been made. The client software sends the username and password to the server to be validated against the user database. This method of user authentication provides a robust and secure method for managing users.

SUMMARY

With today's encryption technology and the accessibility of the Internet, smaller businesses and individual computer users can now take advantage or the same levels of data protection that were previously only available to large corporations. Off-site storage of data provides a safe haven to protect any computer user from catastrophic data loss. The appropriate use of security measures, such as encryption, helps to ensure users that their data remains private, secure and protected throughout the entire FirstBackup process.