Disaster Recovery

I write this 14 days after the terrorist attacks on New York and Washington DC, and the related plane crash in Pennsylvania. Besides the coverage of the human tragedy and the intrigue of the workings of international terrorism, there are a few technological issues that are worth exploring.

The Technology of Security vs. Privacy

Now that the initial shock has warn off, it seems that some are taking advantage of our quest to avoid similar incidents by offering technological security measures - both for airport security and for monitoring electronic communications to detect future attacks.

Biometrics companies (those which identify users by measuring the body in some way) are offering their technology to scan or photograph each flyer and employee and compare it to a database to assure your identity. These devices scan either your fingerprint, your retina, or your facial characteristics and compare it to a database to identify you. The 2001 Super Bowl crowd had their faces scanned and compared to a database of pickpockets and terrorists. 19 matches were found, but no arrests made. It all seems a little Orwellian.

But as far as we can tell right now in this particular case, the suspected terrorists who hijacked the plane used in the attack were using their own names when they bought their tickets and presented their I.D.'s. For the few participants that were even suspected of ties to terrorists, It seems that a simple list of known and suspected terrorists compared against the boarding list or ticket buyer would have been quite effective.

As for monitoring, many are aware of the rumored "Echelon" system operated by an international consortium of secret government security agencies. The system reportedly monitors all telecommunications devices (phone, cellular, e-mail, and faxes) for key words (such as the word BOMB) and word patterns which are then flagged for closer investigation. The European Parliament has concluded it is more than rumor. Immediately following the attack, many Internet Service Providers have reportedly been visited to obtain permission to place monitoring devices on their systems.

But it seems as though terrorists and criminals are quite capable of encrypting their electronic communications, or avoiding them entirely through couriers and personal communications. Many experts are now suggesting the disinvestment in human intelligence in favor of hi-tech surveillance was an error in judgment.

Disaster Planning

The other issue that comes to mind after this crisis is recovering your business after a catastrophe. How long will your business be down after a fire or flood, or an electrical or communications outage?

Most stock exchanges maintain an entire duplicate facility a few miles from it's primary location, fully staffed with Information Technology staff for it's maintenance . Every transaction is mirrored (recorded simultaneously) in both locations so that nearly 100% of their information is available in both locations at any moment.

Most of the other major Financial Services companies involved in the attack also had well established backup procedures in place. Some mirror their data for complete safety, and others store their nightly backup tapes well off-site so that they can recover in another location. Those that restore from tape can lose up to one day of time while restoring the information in a new location, and would also lose any information saved since the last backup tapes were made (often up to another day's worth of information) - and that's assuming you have a server on-hand to restore your data to!

There are on-line services that can take the place of your nightly backup tapes. These services will store your information at their facilities for later retrieval, saving you the trouble of transporting tapes off-site and taking responsibility for the reliability of the backups - but they can be relatively expensive.

Some financial services companies have already distributed their physical offices within a region, and have connected the servers at each major site with high-speed network connections. This arrangement allows servers to be mirrored at different locations - with instant redundancy of any data saved on the network. These facilities work around the geographic distances between offices using teleconferencing within their network, and if properly configured will allow any employee to sit at any workstation in any office and access their own familiar desktop, applications and files.

Of course, no matter how well your disaster plan may be and how safeguarded the data, it's important to be realistic about the human factor. The enormous loss of human lives which made this act of terrorism into a national tragedy also robbed the businesses affected of a tremendous amount of experience and expertise that cannot be recovered.

Another factor is simply one of real estate and equipment. If your offices are unavailable, do you have another location for your employees to work? How long will it take for you to acquire, furnish and activate it? How long to acquire a replacement server and desktop computers? Is your infrastructure organized for remote workers to have secure access to their data from home? Is their home connectivity adequate to the task?

Of course, all of this safety and redundancy is dependent upon one vitally important factor: all important data needs to be saved on your servers - not on the local machine!

How long can you afford to be down in a crisis? Hours? Days? A week? The answer to this question will help you determine the proper level of backup and redundancy you need to build into your technology infrastructure.

Michael Hogan - at Ideate, is an Architect. He developed the first national AEC Information Exchange. He currently provides business extranet solutions and provides consulting services to the AEC industry in Chicago. He welcomes comments by e-mail at mhogan@id-8.com