



- JOHN BREAKEY, NETWORK INDUSTRY COLUMNIST -

Are You Secure in 2002?

John Breakey is President of UNIS LUMIN



Are You Secure in 2002?

Security for information systems is not a new topic. It has been part of any system or network design since the earliest computing environments. But the concept of secure access to information databases should not be considered a place at which you arrive and then "it's done". Security is an ongoing vigil, supported with an attitude of persistence. As new methods of data access are implemented and additional applications are brought on-line, they disrupt the integrity of existing security policies, practices and technologies designed to protect these valuable assets.

If you're like most organizations, you are in the process of implementing a number of changes to your IT infrastructures to accommodate broader access and usage. Some of these include:

- Giving clients direct access to specific transaction information.
- Employees using the Web to access data resources from home and elsewhere
- Deployment of wireless networks
- User of PDA's (e.g. Palm hand-helds) and phone interface messaging systems
- Users accessing multiple data applications (your intranet is also an application when it is serving up customer, employee or financial data)

What Are Others Doing To Solve The Problem?

A healthcare organization implemented a wireless network to augment their wired one to offer more mobility to laptop users. They insisted that the product they bought implemented the highest level of encryption that was available. Here's a novel concept, they actually turned the encryption function on. Well done!

An industry association opened up critical competitive statistics and reports to their members via a web browser environment. They didn't want to trust or infringe on the security practices of their member firms so they issued Security Tokens (dynamic personal, password devices) to only those member employees who were authorized to search the site. This guaranteed that Post-it notes with passwords were not hanging off of monitors. (Editor Note: Most high-function web sites are much more than "brochure wear" sites and need to be viewed with a more critical eye.)

The Multiple Password Dilemma

All of us have endured the need to maintain a separate password for every system or web site to which we log-on. While the software companies are trying to deal with this universal problem - Microsoft hopes people will subscribe to Passport and others are introducing alternatives - these solutions are designed for the general web surfer and may not be advanced enough to trust a third party with your password keys just yet. Single sign-on software, once the domain of the rich, has moved down market and is now available at less than \$50 per seat. This is a great way to improve security and simplify a user's life at the same time. Historically user convenience and security were at opposite ends of the spectrum.

What Should You Do?

Here are some steps you can take to ensure you maintain your vigil and persistence:

- Annually, take stock of all changes you have already made to the IT infrastructure to increase availability or new applications that may have been added; do a post mortem of possible breaches that may have crept in
- Have an independent audit conducted on a regular basis, perhaps once or twice a year, to validate configuration integrity and policy currency
- Occasionally make it a topic of discussion at management meetings
- Ensure that all new IT projects contain an analysis or commentary on "system security impact"
- Finally, make system and network security a priority before it becomes a crisis.

Implementing and maintaining excellent system security can be tough. As an investment it suffers from not having a direct or immediate payback like most other technology expenditures, and it's therefore difficult to get mind share. Security is like insurance. It's a gamble, with some betting that an "incident" won't happen and someone else betting it will. Place your bets.

