Security needed to guard future information

Satman Purewal

IN MY OPINION

Systems should be as carefully designed as the new information systems they're aimed at protecting.

Thousands of new information systems are implemented every year. These systems will provide more information on a more timely basis — critical for making management decisions in today's business environment.

Billions of dollars worth of corporate information will be stored in these new systems, so it is imperative that security not be an after-thought.

Effective security and control processes are critical to the success and long-term survival of the organization.

As with all specialized activities, it is obvious that you should turn to a professional for advice. Many don't, at their peril.Implementing a new system has three key areas in which information security needs to be considered:

- Conversion of information from the existing system to the new one.
- Information travelling across interfaces between the new and incumbent systems.
- The configuration of security for the new information system.

Data conversion is required when the new system is unable to read information stored in the format of the existing system. To solve this problem, the most common approach is to develop a program to rewrite the data into a format acceptable by the new system.

There are several problems with this process. Is the converted data accurate? Has it been converted? Have we simply converted incorrect information from one system to another?

Many new systems project failures have been blamed on the software when it was the result of transferring incorrect information.

Every industry needs to consider the potential issues they face. Retailers will need to ensure converted prices are correct. Manufacturers need to ensure all inventories are converted. Financial institutions need to ensure account information is correct before conversion.

There are many automated tools available to assist the security professional in the conversion process.

Often a new information system will replace only a subset of the existing, or "legacy," systems. There may still be significant information sharing between the two systems.

The interface between the new system and the legacy system needs to be designed to ensure there is no loss of information accuracy or confidentiality during the transfer.

The security professional will always look to ensure interfaces work effectively during the design phase of a new systems project, rather than waiting until the system has been installed to find out they do not work.

The existing system will contain security and control processes ensuring the accuracy of information generated by the system. The new system will likely provide much stronger security and internal control, so this could be an opportunity to improve the security of the whole organization.

The new system may also introduce vulnerabilities. At a minimum, however, you will require controls that provide at least the same level of security provided by the current system.

Finally, all access points to the legacy and new systems must be reviewed and secured.

How can information be accessed? What information is considered confidential? How much damage could be caused, either deliberately or in error? Is it possible to recover key information after such a security breach and how long will it take to recover it?

These questions must be asked of all areas of the new system, including the networks, applications, databases and microcomputers.

The information security professional will focus on making the most effective use of technology to support the security policies, confidentiality needs and integrity requirements of the organization.

Security and control processes must be considered throughout the life cycle of a new systems project. Most importantly, professionals who understand information security and control processes should be consulted during the design stage.

Too often the responsibility for security is assigned to the project team as an additional task. This sends a clear message that security is not a high priority. Information security should be a key priority with today's systems.

Satnam Purewal is a senior consultant in the Management Solutions practice of Deloitte & Touche. She can be reached in Vancouver at **spurewal@deloitte.ca**