Computer-information confidentiality essential

IN MY OPINION

SATNAM PUREWAL

Ensuring privacy of information in the age of computers and the Internet concerns us all as the abuse of access to information systems becomes increasingly prevalent.

By abuse, I mean the use of data for purposes for which it was not originally collected. Almost 50 per cent of organizations responding to the 1997 Computer Security Institute/FBI Computer Crime and Security Survey identified some form of unauthorized use of their computers in the last year.

Both in Canada and the U.S., there have been numerous cases in which individuals have used information available to them in the workplace for personal gain.

Every day, we share our addresses, phone numbers and other personal details with organizations ranging from the corner store to all levels of government. The combination of this information exchange and the ability to use computers to merge multiple databases means extensive personal histories can be developed.

The concerns about information systems and privacy centre on the amount of information collected; the kind of information kept; the methods used to

store it; and the record of who has access to it.

Management must deal with these issues by implementing appropriate security policies and appointing information security officers. These officers can establish practices to meet policy objectives by managing the length of time that sensitive data is kept and designing techniques for storing the information. They would control access to the information and ensure it is effectively disposed of when it is no longer required.

Information security professionals can determine the access each individual needs to carry out their responsibilities. For example, everyone with access to a client database may not need to see the address and telephone fields. Alternatively, the information collection process can be re-engineered to capture "yes" or "no" answers rather than complete personal data.

As organizations design security policies, the need to meet security goals and employees' right to privacy appear to conflict. Some feel the privacy of individuals is threatened by the need to monitor e-mail and other online activity for security reasons. An appropriately designed security policies and practices can strengthen both individual privacy and organizational security.

Maintaining an activity audit trail is essential to ensure breaches of security and privacy are traceable.

Such a process is a strong deterrent to misuse, and protects employees who need to access information, the organizations which need the information for their business, and the person whose information it is.

Companies that collect information will be increasingly held accountable as the demand for individual privacy grows. Organizations that ensure security and privacy will probably be the preferred places of business for consumers in the 21st century.

Here's a checklist to help conduct a privacy-oriented audit of your organization:

- ❑ Do you question the unnecessary collection and retention of data?
- ❑ Do you ensure all private/confidential data is disposed of appropriately and that no authorized or unauthorized person can gain access to it during the destruction process to use it to the detriment of the individuals involved?
- ❑ Do you ensure databases are linked only after the source has been verified?
- ❑ Can the integrity of connected databases be preserved?
- ❑ Are there access controls to protect against unauthorized access?
- ❑ Are adequate audit controls in place to determine activity leading to an incident and assist in identifying the perpetrator?
- ❑ Do you have a security-awareness program to ensure all users understand their role in security and confidentiality of the information entrusted to them?

Only through appropriate security practices can organizations earn the right to collect personal information and the confidence of society to release this information into their care.

Satnam Purewal, CISSP, is a management solutions consultant for Deloitte & Touche in Vancouver. She can be reached at (604) 640-3080 or by e-mail: spurewal@dttus.com.