

Telecommuting raises issue of security risks

Where a business is located, and where its employees live and work, no longer need to be the same.

Today's telecommunication technology gives us the opportunity to choose employees living in any part of the world or, conversely, to work for employers in and part of the world.

Organizations that offer the alternative of working from home or other locations frequently attract some of the best high-tech talent. They also benefit from the longer hours put in by people working from home and the reduced office space needed.

These benefits must be weighed against the serious security risks introduced by allowing employees to work away from the business site and must be addressed before implementing telecommuting.

One of the most critical security issues is connectivity. How will employees connect to the organization's information systems?

There are various options and each type of connection has its own set of risks.

Access via the Internet means that every Internet user could potentially gain access if precautions are not taken. How do we really know the user on the system is authorized?

Token devices provide the additional security necessary.

A "token" is a device such as a credit card-sized computer that displays a new password every minute. This password is also simultaneously generated in the organization's system. Users enter the password displayed on the face of the token into their PCs and it is matched by the company system somewhere on the other side of the Internet. Each time

Satnam Purewal

IN MY OPINION

The benefits of employees working from remote locations must be weighed against necessary security procedures.



telecommuting employees log on, a new password will be generated and required.

Once connected, users begin transmitting information across the Internet and telephone networks.

This also poses serious security risks, which can be reduced through the use of encryption. If someone intercepts the transmission, deciphering the text will prove almost impossible.

Telecommuting or not, backing up important files is always critical.

Most organizations have policies and procedures regarding backing up material on their information systems. On-site employees can back up their important files on to the office network. These are then backed up again and stored off-site. Such a system is essential.

Another crucial issue is employee termination. If telecommuting employees or contractors leave or are terminated, how will corporate data and assets be retrieved? How does an organization ensure that all confidential documents are returned?

Procedures to address this should be established in conjunction with the human resources group and legal counsel.

Confidential information on paper is usually kept in locked locations in offices or business premises.

Employees with a "home office" should have a device in which they can store secure information until it can be returned to the office. A fire-proof filing cabinet with a locking mechanism should be sufficient.

At the office, only authorized individuals are permitted to access corporate computers and information systems. When the computer is at home, children and spouses may make use of the computer.

Employees need to understand they are responsible for all activity on business computers seven days a week, 24 hours a day.

Home offices usually have a low level of security. An organization may have an elaborate intrusion-detection system whereas many homes are simply secured by lock and key. These risks must be assessed before telecommuting is permitted.

The demand for telecommuting will only continue to increase. To meet this challenge, organizations must carefully assess the risks that telecommuting will introduce and develop solutions to mitigate them. Organizations that do this successfully will thrive in the new millennium.

Satnam Purewal is a computer security consultant in the management solutions practice of Deloitte & Touche. She can be reached at (604) 640-3080 or by e-mail at spurewal@deloitte.ca.