Information security starts with back door

IN MY OPINION

SATNAM PUREWAL

Information security is a hot issue, as companies try to balance the advantages of doing business on the Internet with the need to protect their information systems from unauthorized intruders.

Unfortunately, while focusing on making their systems secure, management often neglects basic physical security.

Many organizations are literally locking the front door and leaving the back door open. Critical network hardware is placed in areas accessible to all employees; personal computers are left in unlocked offices.

When organizations fail to provide basic physical access controls, they leave their information systems vulnerable to theft and tampering. This can be costly, especially if the stolen equipment contains information that is confidential or proprietary.

How can companies protect themselves?

Begin by reducing the risk of intruders impersonating authorized users to gain access to secured areas.

Such attempts can be prevented through security awareness campaigns and by introducing user identification.

Employees should wear photo identification and visitors should be assigned visitor badges. Challenge those not conforming.

Some companies rely on their receptionists to "guard" the door. This is not always effective. Practiced thieves, sometimes working as teams, can easily manipulate or ignore busy receptionists.

Minimizing external access points, ensuring all entry points to secure areas are locked, and engaging the services of a security company will reduce your exposure.

Many organizations use the basic lock and key system to secure their premises. This has four weaknesses: unauthorized duplication of keys, lack of accountability of who entered an area at a given time, the loss of keys, and retrieving keys from terminated or departing employees.

Most companies feel it is too expensive to continuously change locks when one of these events occur.

A key-pad password system solves the issues of lost keys and their retrieval, but the issue of terminated or departing employees remains because most organizations fail to change the password when employees leave. In addition, passwords can be shared more easily than keys and therefore doesn't allow for accountability.

In my opinion, card access is one of the most cost-effective ways to secure access. It also allows traceability and accountability. If a card is lost or stolen, or an employee terminated, the card can be instantly disabled.

The use of biometric access security devices, such as fingerprint scanners at secured doors or on PCs is increasing. The output logs from all devices should be regularly reviewed for possible breaches of security.

Criminals don't always use doors for access.

Walls should run above dropped ceilings and below raised floors to prevent access by climbing or crawling. Communications cabling should not be readily accessible, preventing "wiretapping" through commonly available network tools.

Consideration should be given to closed circuit TV and video equipment.

All equipment should be secured to the desktop, and portable computers can be temporarily secured via cable locks. Key pieces of equipment can be fitted with more advanced theft warning, detection and tracing devices.

Theft of computer equipment is not limited to business premises. Every day computers are stolen from cars, hotels, and homes.

Corporate policy should instruct employees not to leave computers in unattended cars and hotel rooms.

While a computer is at home, unauthorized individuals should be forbidden to use it, especially when confidential information is accessible.

Physical security is the first line of defence against intruders.

Businesses must keep in mind that while it is important to have passwords and firewalls to protect against Internet or even internal intruders, attention must also be paid to the basics.

Physical security visibly demonstrates an organization's commitment to security and sends a positive message to employees and customers.

Satnam Purewal, CISSP, is a security consultant for the Management Solutions practice of Deloitte & Touche in Vancouver. She can be reached at (604) 640-3080 or spurewal@dttus.com