Computer security methods no longer effective

IN MY OPINION

SATNAM PUREWAL

In 1977, a computer security expert noted that "as society becomes more dependent on computers, computer crime is becoming not only more disastrous in its potential impact, but also more attractive to the criminal." How right he was.

Information security breaches are on the increase, and are not limited to any country or industry. Last year, hackers broke into the web site of the U.S. department of justice and changed the name to department of "injustice."

This year, an American hacker broke into school computers and changed his brother's grades, and the U.S. Foreign Agricultural Service was forced to shut down its World Wide Web site because a hacker was launching attacks from it.

In the U.K., a computer hacker was recently charged with the theft of 100,000 credit-card numbers and enough related information to use them.

Russian hackers robbed a major financial institution of $400,000 by using fraudulent wire transfers.

Until recently, an organization's greatest challenge to security came from its own employees: approximately 80 per

cent of all security breaches originated from within an organization. Many computer crime incidents consisted of automated "trapdoors" and "time bombs" installed by disgruntled employees.

Remote dial-up and Internet access was very limited, and external security threats were not a major concern.

They are now. According to a recent survey conducted by the Computer Security Institute and the FBI, 66 per cent of the respondents reported one or more attacks from the outside and 55 per cent of the respondents reported one or more in the past year from the inside. Significantly, many did not know whether they had been attacked either internally or externally.

In 1996, the Internet was cited as the most frequent point of attack by 38 per cent of respondents. This year, that figure rose to nearly 50 per cent. The total losses for 59 per cent of the respondents were over $140 million. Nearly all said that information stolen would be of interest to competitors.

These figures reflect the increased use of the Internet and remote access. External security breaches will continue to increase, and many of these attacks will be undetected until it's too late.

We are rapidly approaching the point in time where every corporate user will be connected to a single global network. Traditional methods for securing a modern enterprise are no longer effective.

Information security officers must ensure their organizations can deal with both inside and outside intrusions and that policies and procedures are in place to detect and respond to an incident.

According to the CSI/FBI survey, 60 per cent of organizations do not have written policies on dealing with intrusions, and only 62 per cent have emergency response teams. Seventy-three per cent don't have policies for preserving evidence.

Modern risks need a modern approach. People with call-display units review the list of callers even if they have an answering machine: knowing who has called gives an upper hand. In the same way, regardless of whether it is rejected by a firewall, all Internet traffic should be tracked and reviewed for patterns. You need to know who's rattling your door.

Organizations that are playing catch-up with their security programs will not thrive. Today we exchange data with business partners, sell products on the web, and provide remote access for telecommuting and travelling employees.

All of these present security challenges that traditional methods can't effectively address. As business methods becomes more sophisticated, the counter-measures employed to reduce risk must match that sophistication.

It costs much more to respond to a security breach than it does to prevent one in the first place.

Satnam K. Purewal, Bsc, 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