Securing Employees' Windows-Based Home Computers

by **James G. Barr**

Inside this report ...

Executive Summary

[return to top of report]

Today, home computers and office computers are virtually indistinguishable. That's because many employees use office computers to store and process personal data, and home computers to store and process office, or company, data.

Since company data migrates -- often with the company's blessing -- to employees' home computers, CSOs should be concerned about the security of home systems.

While their jurisdiction may be limited relative to imposing home security standards, CSOs should at least encourage employees to follow sound security practices, especially for Windows-based systems, which are targeted far more frequently -- and effectively -- than units running either the Macintosh or Linux operating systems.

This is not to suggest that Mac and Linux home users are invulnerable, rather to emphasize the magnitude of the threat facing Microsoft personal computers.

Risks

[return to top of report]

Windows-based home computers are often subject to attack, exposing both personal and corporate data.

1. Operating System Contamination

Forget the butterfly. The Microsoft logo should be a bull's-eye. "Years of inattention to security issues in Redmond, Washington [have left Windows users] exposed to [contaminants such as] the Blaster worm, the Sobig virus, Messenger Service pop-ups, spyware"[1] and worse.

While Microsoft is finally showing signs of taking security seriously, even offering bounties on hackers who deploy viruses, the Windows operating system will remain vulnerable, probably for years to come.

2. Exposed Company Data

Attacks on home computers can affect corporations. Many employees use their home systems to perform company work, in the process downloading sensitive or confidential company data. When these home units are compromised, company data can be exposed to theft or misappropriation.

3. Catastrophic Data Loss

Home computers, just like the office variety, are vulnerable to sudden and catastrophic data loss, usually due to malicious programs or problems involving the hard disk. Unlike corporate computers, however, only a small percentage of home computer files are backed up. Months, or even years, of work can be wiped away in a matter of minutes.

Recommendations

[return to top of report]

Company CSOs should encourage employees to secure their Windows-based home computers, especially since such systems often contain sensitive corporate data.

1. Limit Storage of Confidential Company Data

While companies often benefit from employees taking their work home, home computer users should be cautioned to avoid downloading -- whenever possible -- company confidential data.

2. Keep Computers Off Limits to Family Members

Home computers used for company business should be off limits to all family members. To prevent tampering, desktop units should be deployed in rooms with lockable doors, and laptops should be stored in locked cabinets. In addition to preventing unauthorized usage, such measures reduce the likelihood of loss due to robbery, especially laptop theft.

3. Install a Personal Firewall

In addition to anti-virus software, home computers should be equipped with a "firewall". "A firewall acts like a protective gateway that shields a private computer user or network of users from external threats, such as hackers and viruses.

"Firewalls can be thought of as a pair of mechanisms: one that blocks traffic, and another that permits it. Simply put, a firewall's purpose is to keep unauthorized users out of your computer while allowing you to access the Internet and utilize public networks, helping you do your job more quickly, easily, and effectively."[2]

Windows XP users can use XP's built-in Internet Connection Firewall. In addition, McAfee provides another popular firewall product.

4. Apply Microsoft Security Updates

While home users are normally diligent in applying anti-virus updates, from suppliers like McAfee or Symantec, they often neglect to apply Microsoft security updates.

The Windows XP operating system includes an Automatic Updates feature, which can automatically download the latest Microsoft security updates while the computer is on and connected to the Internet.

5. Backup Critical Files

To safeguard against data loss, especially the catastrophic form, backup all critical files at regular intervals.

Table 1. Backup Considerations

[return to top of report]

Item	Concern

Critical Files	To be safe, backup all data. Otherwise, backup all vital records, i.e., important information that's only available on the subject PC. From a company perspective, don't forget work in progress. Nothing is more frustrating than trying to recreate just-written memos and reports.
Registry Settings	If conducting a partial backup, don't forget the Windows Registry. "This is the huge database that tells your computer how to run. Without it, you have an expensive paperweight."[3]
Off-Site Storage	Store backup media (tape, CD, DVD, etc.) off-site, i.e., away from home.
Backup Media	Using a floppy disk for backup is no longer practical. Adopt a higher-speed, higher-capacity media. Current alternatives include: ■ Tape drives; ■ CD or DVD drives; ■ Zip or Jaz drives; and ■ External hard drives.

6. Keep Used Hard Drives

Given the current state of computer forensics, it's very difficult to clean a hard drive of all data.

When discarding a home PC, remove and physically destroy the hard drive. After all, why take any chances?

7. Migrate from Windows 98 NOW

Effective January 16, 2004, "security-based hot fixes will not be generally available for users of Windows 98 and Windows 98-Second Edition."[4]

Home computer users should immediately migrate their Windows 98 (in some cases, Windows 95) systems to Windows XP, or some other security-supported version of the operating system.

Table 2. Action Plan for CSOs

[return to top of report]

Action	Purpose
Limit the Storage of Confidential Company Data	To reduce the risk to company assets from compromised home computers.
Keep the Computer Off Limits to Family Members	To avoid damage due to non-employee. i.e., family, use.
Install a Personal Firewall	To reduce the risk of virus and other contamination, particularly when used in concert with anti-virus software.
Apply Microsoft Security Updates	To benefit from the latest in vendor security patches.
Backup Critical Files	To protect against catastrophic data loss.
Keep Used Hard Drives	To prevent company data from falling into the hands of PC recyclers (and other non-trusted agents).
Migrate from Windows 98 NOW	To maintain Microsoft security support and assistance.

Resource File

[return to top of report]

CERT Coordination Center: http://www.cert.org/
McAfee: http://www.mcafee.com/
Microsoft: http://www.microsoft.com/
SANS Institute: http://www.sans.org/
Symantec: http://www.symantec.com/

References

[1] Rob Regoraro. "A year of spam, spyware and worms." WashingtonPost.com. December 30, 2003.

[2] "Personal firewalls: Don't run your PC without one." bcentral.com.

[3] Kim Komando. "Are you still not backing up your data?" bcentral.com.

[4] Peter Galli. "Windows 98 Users Face Increased Security Risk, Says Study." eWeek.com. December 11, 2003.

About the Author

[return to top of report]

James G. Barr is a leading business continuity analyst and business writer with more than 25 years' IT experience. A member of "Who’s Who in Finance and Industry," Mr. Barr has designed, developed, and deployed business continuity plans for a number of Fortune 500 firms. He is the author of several books, including How to Succeed in Business BY Really Trying, a member of Faulkner's Advisory Panel, and a managing editor for Faulkner's **Security Management Practices**. Mr. Barr can be reached via email: jgbarr@faulkner.com.