

Taking steps to help secure your mobile environment

Published: March 28, 2006

Summary: *One expert discusses how workers can benefit from mobile connectivity and how to help minimize security risks.*

Taking steps to help secure your mobile environment

Sales of mobile devices are expected to soon rival standard desktops. Featuring extended battery life, lower price points and ever-growing power, the flexibility these devices provide workers is giving rise to the mobile workforce.

Properly used, they can also boost staff productivity by an estimated 20 to 50 per cent, and reduce reliance on office infrastructure.

But businesses considering a mobile computing strategy must have a plan to offer such services securely. Mobile computers will likely store sensitive business data, and if a third party gains access to this information it can leave organizations vulnerable to theft or privacy breaches. Stephen Ibaraki, a veteran IT analyst and recent recipient of the 2005 *Computing Canada* Lifetime Achievement Award, says one out of every three businesses have experienced problems due to inadequate security measures. Ibaraki has some advice on how to help protect the business network.

On This Page

- ↓ [1\) Manage network access](#)
- ↓ [2\) Guard your VPN](#)
- ↓ [3\) Install Virtual Machine software](#)
- ↓ [4\) Educate users](#)
- ↓ [5\) Protect against theft](#)
- ↓ [6\) Standardize](#)

1) Manage network access

Only authorized business systems, not a personal device, should ever be granted receive access to the corporate network. Also, Ibaraki advises that IT staff establish clear guidelines to detect rogue devices and deny them access.

↑ [Top of page](#)

2) Guard your VPN

Employees working from home, even over a secure VPN, still pose security risks. The network can be exposed to anything the employee downloads at home, which may contain spyware, viruses or Trojans. These dangerous applications can breach the internal business network through VPN.

↑ [Top of page](#)

3) Install Virtual Machine software

Virtual Machine software, such as Microsoft Virtual PC 2004 or Microsoft Virtual Server 2005, creates a controlled, policy-managed environment on the laptop or mobile computer and helps prevent unwanted material from entering your network. Unmanaged systems are the greatest risk to create open doors for hackers to enter the business network, says Ibaraki.

A worker browsing the Internet remotely and opening up attachments may unknowingly receive hacker-generated programs along the way. These programs now reside on the unmanaged computer waiting for access to core systems. When the user logs into the business network, the hacker may be granted access and can steal information on both the unmanaged computer and all systems on the network.

↑ [Top of page](#)

4) Educate users

If employees routinely carry sensitive business or client data on their mobile computers and are connecting to wireless networks outside of the office, they need to be concerned about public access to sensitive information on their mobile hard disks. "Evil twin" or "Wireless Phishing" are techniques specifically designed to steal information from unsuspecting wireless users who access "hotspots" to do their email. Most free wireless connections are legitimate – some, however, are designed to help malicious attackers steal information from employees.

↑ [Top of page](#)

5) Protect against theft

Businesses need to ensure that in the event a mobile device is stolen, data on the hard disks cannot be easily breached. Encryption, passwords, locked devices, Virtual Machine software and remote deletion applications can help safeguard valuable data.

↑ [Top of page](#)

6) Standardize

Ibaraki recommends that businesses stick with a one-vendor solution whenever possible. Choose a solution that integrates well with desktop and server software. Microsoft, for example, is committed to helping protect customers by keeping up with changing standards, and implementing any changes in its software automatically. Also, make sure your devices are compatible- check that your potential vendor's hardware is compatible with the latest security standards.

For More Information

- [Microsoft TechNet Security Topics](#)
- [The Microsoft Security Assessment](#)

↑ [Top of page](#)

[Manage Your Profile](#)

©2006 Microsoft Corporation. All rights reserved. [Terms of Use](#) | [Trademarks](#) | [Privacy Statement](#)
