For TechWise newsletter blast by April 21, 2008 *By Rhonda Raider* *[593 words]*

Security Bloopers:
Five Common Mistakes

Wondering if you've adequately protected your network can cause sleepless nights. In the rush of your workday, what could you have missed? Sleep better by avoiding these common mistakes.

1. Being too generous with wireless network access
"Guests expect wireless access, and you can make it secure with the right policy," says Philip Stone, president of Boardwalk Communications [LINK: www.bdwalk.biz], a Cisco Premier Partner whose certifications include Advanced Wireless.

- Deploy a wireless access point that supports VLANs, such as Cisco Aironet® access points [LINK: www.cisco.com/go/aironet], and set up a guest VLAN that restricts access.
- Assign random passwords for guests and set them to expire after a specified time. Cisco 2100 Series Wireless LAN Controllers [LINK: http://www.cisco.com/en/US/products/ps7206/index.html] let your lobby receptionist do this.
- Don't broadcast your company's SSIDs, broadcast only guest SSIDs.
- Dial down the power setting. "Be sure to change the power setting so that you're not serving nearby companies," says Jerry Divino, security consultant at Boice Enterprises [LINK: www.boice.net], a Cisco Certified Silver Partner whose certifications include Advanced Security and Advanced Wireless.

2. Expecting superhero performance from a familiar duo
It's fantasy that just a network firewall and anti-virus software can do it all. "The reality is that you need a 'defense-in-depth' approach so that if a threat gets through one layer, it can be stopped at others," says Divino.

- Use an integrated security appliance instead of separate products. You'll get better protection, and spare yourself having to learn multiple interfaces. For example, the Cisco Adaptive Security Appliance (ASA) 5500 Series [LINK: www.cisco.com/go/asa] provides comprehensive content security with URL filtering, anti-phishing, anti-spam, anti-virus, and anti-spyware, all with a common interface.

3. Letting employees connect too freely from home or the road
Employees who connect from home or public hotspots can have their transmissions intercepted or leave behind information that can be used to break into the company network.

- Secure sessions with non-company-owned PCs by setting up Secure Sockets Layer (SSL) VPNs, which encrypt session data without requiring preloaded client software. Cisco IOS SSL VPN [LINK: www.cisco.com/en/US/products/ps6657/products_ios_protocol_group_home.htm] also temporarily downloads Cisco Secure Desktop to the PC to get rid of cookies, temporary files, browser history, and other cached content once the session is over.

4. Using leaky pipes to connect other sites and partners
It's easy to use the Internet to link remote offices to your central network. But how can you secure the connections?

- Spare yourself the time to manually set up VPN connections between a new office and all the others. Using the EZVPN feature in Cisco Integrated Services Routers [LINK: www.cisco.com/go/isr], you can easily configure Cisco routers to initiate VPNs between sites and clients. When a branch employee plugs in the router, it automatically gets the information it needs from the main office router. EZVPN is also available for the Cisco ASA.
- Be alerted to suspicious network activity by using an intrusion prevention system (IPS) [[LINK: http://www.cisco.com/en/US/products/sw/secursw/ps2113/index.html]. Accelerated IPS processing is available in an IOS software module for the Cisco Integrated Services Router; IPS is also available as an integrated hardware module for the Cisco ASA. Both save you from having to purchase and manage a discrete IPS device.

5. Being lured off course by a siren song
Just about everyone has opinions on security. For advice based on businesses like yours, discuss your needs with a certified technology partner who has security expertise and experience serving SMBs. Such a partner can provide solutions appropriate for your environment, ideas for minimizing costs, assistance with security policies, and other technical support and services you may need.

Next Steps
Find a partner with expertise in security and experience working with SMBs. [LINK: http://tools.cisco.com/WWChannels/LOCATR/openBasicSearch.do]

See how to secure your business, what's needed, and how to get started. [LINK: http://www.cisco.com/web/solutions/smb/need_to/secure_my_business.html]

Learn about Cisco solutions for SMBs [LINK: http://www.cisco.com/web/solutions/smb/index.html]

# # #