



*Caution: you might have already tripped into a serious security gap created by the type of networking equipment you use.*

Digital Vision/Punchstock

## Home Computer Equipment Is Not Useful For The Business World

By Jerry Irvine

**I**t's a little-recognized hazard. To save money, smaller and medium-sized businesses buy consumer plug-and-play networking equipment over robust enterprise-grade gear, only to end up surrendering higher levels of security, reliability and performance.

Why do businesses make this mistake? Familiarity with networking equipment has risen with American's web access. Companies that traditionally provided enterprise level network devices purchased home networking companies to get a part of this

growing market. Their recognized brands are widely available at low cost, leading business owners to falsely assume that the home devices are just as effective as their higher cost siblings. Some enterprise equipment starts at \$300, but home wireless devices can be had for as little as \$39.

### Where The Threats Are

Using home networking over enterprise equipment is like deciding to use a simple dead bolt to protect your business instead of an alarm system. Both devices provide the same basic functionality. But the alarm system assures everything will be there in the morning and alert you should something happen.

Home devices are organized into four prevalent types. Routers/Gateways connect to cable or DSL internet providers; hubs and switches tie multiple computers in the home via a wired network; wireless access points unite computers via WiFi; and NAS (Network Addressable Storage) devices provide shared storage for users. These products supply the minimum features and benefits necessary to support the average home network, but functionality for businesses falls woefully short.

The average home router/gateway device provides firewall services and allows for automatic configuration allowing PCs to connect to the Internet. For businesses with their own Internet Web pages and email servers, connections from the Internet have to be allowed back in to the businesses' internal network. This is a major security concern since viruses and malicious applications, like adware, are spread through the Internet. As a result, it is industry best practice to configure a separate network called a DMZ (Demilitarized Zone) to redirect traffic coming from the Internet so it can be scanned and checked for dangerous content. When using the aforementioned devices, here's where your business network could fall down by failing to trade up.

Home quality hubs and switches generally require no configuration. But they also don't support security devices which can eliminate malicious applications. While easy and convenient, many users try daisy chaining multiple switches together without understanding the limitations and connectivity problems. Institute of Electrical and Electronics Engineers (IEEE) standards and configuration requirements limit the number of devices and work stations connected together. Exceed these limits and you'll impact communication and even

cause a complete outage. Moreover, connected workstations can transmit viruses and other malicious applications to other devices on the network.

Home based wireless network devices provide basic security configurations using WEP (Wireless Encryption Protocol) and even WPA (WiFi Protected Access). But automatic configurations frequently fail when connecting PCs to the access points. Upon set up, basic configuration is recommended with advanced security configuration performed later. But, as with most things, this never happens and systems are left wide open.

Wireless connectivity invites potential dangers. Applications with automated scripts lurk on the Net designed to breach WiFi devices and give access to your network. Home devices aren't designed to monitor for unauthorized users or rogue devices.

Home-based NAS devices allow users a centralized method to store files and share them with one another. This may be easy to manage and main-

*Using home networking over enterprise equipment is like deciding to use a simple dead bolt to protect your business instead of an alarm system. Both devices provide the same basic functionality. But the alarm system assures everything will be there in the morning and alert you should something happen.*



**Diamond Wire Spring Company**  
Designer and manufacturer of precision springs since 1939

# STOCK and CUSTOM SPRINGS

**STOCK SPRING CATALOG**  
Includes small, medium & jumbo springs with loads from 1.5 lbs. to 2000 lbs. • PLUS Full line of Die Springs

Toll-Free: 1-800-424-0500 • Fax: 412-821-1642  
email: [catalog@stocksprings.com](mailto:catalog@stocksprings.com)

Visit our website: [www.diamondwire.com](http://www.diamondwire.com)

tain with a small user base, but security features are limited and difficult to configure to insure private file access. Centrally located files are another high vulnerability. Without a standard antivirus solution performing real-time access protection, files can be corrupted or destroyed, leaving no backup or ability to salvage.

### Gaining Control

While home networking equipment shortcomings may not present a significant vulnerability, it's what they won't do when viruses, malicious applications, and programs or scripts try to invade your network. Run accidentally or intentionally, these can affect a device, groups of devices or any device connected to a network or the Internet.

Enterprise devices can configure layers of security, giving more access control options that limit users, devices and types of applications that can communicate on the network. Enterprise level devices also allow configuration of secondary devices which

*While home networking equipment shortcomings may not present a significant vulnerability, it's what they won't do when viruses, malicious applications, and programs or scripts try to invade your network.*

can automatically replace primary devices in case of a failure.

Enterprise level devices will do something else home devices can't: monitor the productivity and efficiencies of all the devices tied to your network. With this information, IT professionals can regularly review the systems to assure the business is achieving the levels of service required from its infrastructure.

When designing a business network, use only enterprise-grade gear and research and follow industry best practices to get the highest

levels of services at the best price. While cheap and easy to configure, home networking devices could cost you far more than they're worth. ♦

**Jerry Irvine is CIO/COO of Prescient Solutions, a virtual Information technology services company that helps global business clients, local municipalities, schools and governmental agencies maximize technology resources and minimize IT expenditures. Jerry holds many technical designations, including MCSE, MCNE, CCNA, CCNP, CCDA, CCDP, Cisco Wireless Professional. He can be reached at [jirvine@prescientdev.com](mailto:jirvine@prescientdev.com).**

# NESMA 29th Table Top Expo

## April 14, 2009 - 1 Day Only

### and **YOU'RE INVITED**

This is your invitation to attend the Northeast's largest show for the Spring Manufacturers, Metal-Stamping and Suppliers to our Industry.

The New England Spring & Metal-Stamping Association welcomes you to visit with suppliers and manufacturers that are leaders in our industry.

The show is the convenient place to introduce you and your employees to the new machinery and systems on the market. It also acts as an educational tool for you to ask questions about new technologies and services.

We encourage you to register as soon as possible. For registration information please contact Cindy Scoville at (860)314-2010 or visit us at [www.NESMA-USA.com](http://www.NESMA-USA.com) for a copy of our registration form.



200 MAIN STREET - BRISTOL, CT 06010  
PHONE (860)314-2101 \* FAX (860)584-4722  
[C.SCOVILLE@BRISTOL-CHAMBER.ORG](mailto:C.SCOVILLE@BRISTOL-CHAMBER.ORG)  
[WWW.NESMA-USA.COM](http://WWW.NESMA-USA.COM)