

# For Small Business, Minimum Effort Means Maximum Security

by Kate de Gutes

You've seen the headlines: "40 million Credit Cards Exposed." "Hackers Gain Access To Corporate Network." "Average Data Breach Costs Company \$5 Million." Given the increasing threat posed by everything from hackers and packet sniffers to worms and viruses, advanced security protection is a business necessity, not a luxury. But don't these problems only affect large enterprises? Small business needn't worry, right?

Wrong. For the small-business user, infection is chronic. In June, 2006, Microsoft revealed the results of a 15-month test of its Malicious Software Removal Tool on home and small-business PCs. The utility, used to scan and clean 5.7 million PCs, found backdoor Trojans, or programs that let hackers gain entry, on about 62% of them. And during the 15-month period, 20% of PCs that were cleaned were reinfected. In addition, a recent survey of 455 small and medium businesses (SMB) by international software developer GFI found 32 percent of companies experienced a security breach in the past year, most often due to a virus attack. And forty percent of these businesses say their networks are not secure, even though almost all have firewalls and anti-virus software installed. For these very reasons, hackers are targeting smaller companies. They know that IT systems at small and medium businesses are less protected. Welcome to the world of SMB, the new frontier for security challenges.

Considering the plethora of problems out there – from network security to virus protection to firewalls to customer identity theft – how can your company easily identify and implement simple, cost-effective security measures that provide maximum protection against malware and viruses? And don't forget the fines that often come with data breaches. With government regulations, the fines are often steep for businesses failing to comply with security, even though compliance is not particularly difficult or costly.

## Step One: Assess Your Risk

The first step is to examine your current infrastructure, making sure to anticipate upcoming changes and additions. What data do you need to protect? What are the entry points to your network? Which government or corporate regulations do you need to follow? Several online sites can help you assess your current security risk and what hardware or software you should consider to help secure your business. One, the National Cyber Security Alliance (NCSA) provides resources for cyber security awareness and education for small businesses. It includes a quiz to test your basic cyber security knowledge, and a guide to staying safe online. Others, such as the Internet Security Alliance, have security information and real-life



---

**Do you know ALL  
the entry points to  
your network?**

examples for SMBs. Going through the basic assessment from any one of these resources can help an SMB gain a better understanding of hackers, viruses, and system failure, and how to quickly and cost-effectively enhance their data security.

## Step Two: Update – and Use – Your Anti-virus Software

Viruses and worms are malicious programs that get more prolific — and more sophisticated — daily. Despite these dangers, many small businesses often overlook the importance of investing in or running virus protection. All of your company’s desktop and laptop computers should already have anti-virus (AV) and anti-spyware protection, which needs to be updated regularly. And that free software that comes with your computer? Upgrade to a not-for-free version.

“By their very nature, small businesses don’t employ the same level of virus protection that large businesses do,” says Rob Enderle, president and principal analyst at the Enderle Group. “One of the problems that exists in small businesses today is a tendency for people to turn off their anti-virus and anti-spyware products when they degrade performance. But you can run them in the background.”

However, even running this software in the background won’t completely close the gates to viruses. What to do?

## Step Three: Invest In Security 24/7

As noted in Businessweek.com, the most popular AV products fail to prevent 80% of new viruses, because most AV vendors have built “burglar alarms” that alert you only if a known intruder tries to compromise your system. Malware that they don’t recognize can easily get in unopposed. In fact, virus writers test their viruses against the popular AV products before unleashing them on the world. And once a new virus is unleashed, those companies who have 24/7 monitoring stand the best chance of discovering – and blocking – the intrusion. By choosing an IT security provider such as Techchex, who aligns with all the major AV vendors, you can hedge your bets: each AV vendor (Symantec, McAfee, etc.) will find – and automatically patch – different viruses at different times.

Just remember: IT security begins with the basics, like identifying points of entry. Protect your business from financial and time loss by regularly updating your antivirus software, implement best Web practices in your company, and providing regular system backup (including your operating systems, Web browsers, and VoIP implementations). Be aware of laws and Government regulations that affect you. Safely and routinely back up your data onto a server or other safe device. Use the best virus protection you can find, 24/7. Finally, once you know that security is an investment of time rather than money, you’re on your way to a more secure business. A cost-effective IT service plan makes good business sense: a professional takes care of your computers and you take care of business.

---

*Kate Carroll de Gutes is a technical writer based in Portland, Oregon whose work centers around the technology challenges faced today by small and medium-sized businesses. Her work has appeared in Fast Company and INC. magazines and on numerous blogs.*

**Techchex<sup>SM</sup> Inc.**

ARTICLE REPRINT COURTESY OF TECHCHEX INC.

Techchex can be reached at 503.227.1772 | [www.techchex.com](http://www.techchex.com)