

2007 Webroot® State of Internet Security Summary

Companies hold valuable information in the form of customer data, proprietary information and trade secrets in their computers, networks, servers and storage devices. As a consequence, company IT systems are under constant attack. Companies are struggling to maintain security for a mobile workforce as cyber security threats continue to increase in both number and complexity. Combine this with the growing volume of sensitive digital data that is vulnerable to attacks. The result is significant risk to the global economy.

Cyber Security and SMBs

IT security is particularly noteworthy in the Small & Medium Business (SMB) sector which according to the U.S. Small Business Administration produces at least half of the private, non-farm GNP and at least 45% of the U.S. private payroll.

Many large corporations have significantly strengthened their network security infrastructure, so cyber criminals are likely to concentrate on easier marks, making SMBs prime targets.

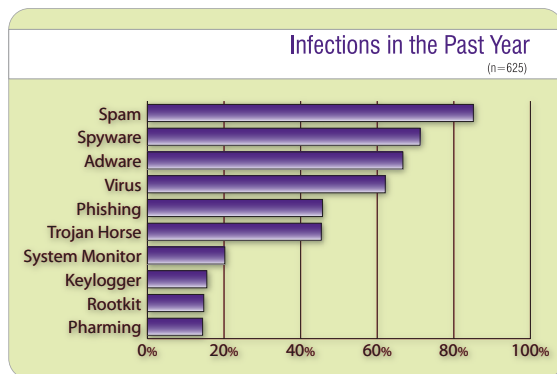
→ There are many more SMBs than large companies in the world.

→ Most all SMBs hold sensitive personal information about their employees and customers that can be monetized by cyber criminals.

→ Yet, SMBs often lack the financial and human resources available at larger companies to combat cyber threats.

According to a survey conducted by Webroot Software in September 2007:

- Over half of SMBs surveyed feel that online threats are becoming more serious.
- The number of U.S. SMBs that had a spyware infection in the past year is second only to the number that experienced spam.
- Employee errors and insider sabotage or data theft are viewed by SMBs as two of the most serious Internet security threats they face, yet most SMBs lack policies or technology to restrict or monitor employees' use of work computers for personal activities.



Source: Webroot SMB Survey, September 2007

Evolving Cyber Security Threats

Online criminals use sophisticated tools to find unprotected and vulnerable networks and computers. Today's spyware programs are more complex and dangerous than ever before. They infect machines with more registry entries and files to make removal more difficult. Further complicating removal efforts, many pieces of spyware use watcher processes, which monitor each other so that when removal is attempted the malicious code will be repopulated, or new components will be downloaded from the Internet.

In contrast to viruses, that typically make their presence known by spreading across many systems simultaneously and seriously impacting machine functionality, the success of spyware programs depends on their stealth nature. Given the significant financial incentives to stealing sensitive data or serving nuisance advertising, spyware program writers are adept at covertly infiltrating a system and installing programs deep within a computer or network.

VIRUS / WORMS



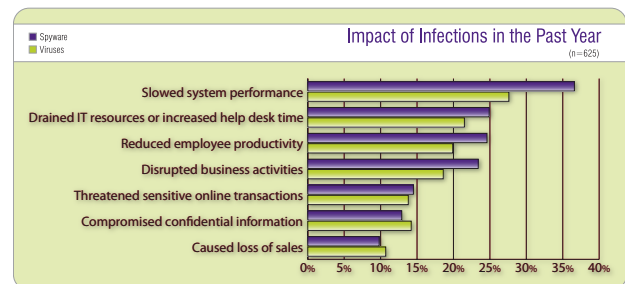
- replicates by attaching to files
- spreads quickly
- visible damage

SPYWARE



- monitors/controls
- records keystrokes
- unnoticed = more damage

Even things that may seem more innocuous like spam or pop-ups, which are generally viewed more as nuisances than threats, are increasingly dangerous as they can be used to carry more serious threats, such as spyware, viruses and worms. There is almost zero cost associated with mass junk mailings. This makes spam an easy and cheap delivery mechanism for malicious attacks that can have significant impact on both businesses and individual consumers.



Source: Webroot SMB Survey, September 2007