STATE OF INTERNET SECURITY

Protecting Small &
Medium Businesses

webroot
SOFTWARE

TABLE OF CONTENTS

EXECUTIVE SUMMARY

The definition for the Small and Medium Business (SMB) sector varies globally; however, there is consensus that these companies are significant contributors to the world's economies in terms of both revenue generation and employment.

The Internet provides opportunities in the form of access to information and potential customers that help SMBs get off the ground, flourish and grow. However, SMBs are also exposed to a complex Internet security landscape.

In this context, Webroot Software conducted a survey of companies with five to 999 computers in six countries: Canada, France, Germany, Japan, the United Kingdom and the United States. This report highlights the survey results in the context of Internet security threats, SMB business realities and the policies and technology that can mitigate these risks.

Most industrialized countries report that SMBs make up 97 to 99 percent of all companies. More importantly, U.S. SMBs produce half of the private, non-farm GDP and companies fewer than 500 employees account for half of all private-sector workers. In the UK, SMBs account for almost 60% of all employment.

A 'perfect storm' is brewing in the world of IT security. As companies grow and add remote workers, IT departments are not keeping pace in terms of staffing while also struggling to maintain security for a mobile workforce. Furthermore, most SMB IT groups do not have in-house security expertise nor policies to manage employees' personal use of work computers. Add to that the growing number and complexity of malware threats and the increasing volume of sensitive customer data that is being stored and an environment is being created where cyber criminals and malware could have considerable impact on the global economy.

Other highlights of the report include:

- Over half of SMBs surveyed feel that online threats are becoming more serious (page 4).
- In all six countries, SMBs report viruses and worms as more of a threat than spyware, but in every country (but Japan) the percent of SMBs affected by spyware is higher than those affected by viruses (page 5).
- In Canada, the United Kingdom and the United States the number of SMBs that had spyware infections in the past year was second only to those that experienced spam (page 5).
- Ninety five percent have an antivirus solution installed, yet viruses are still identified as a top concern and high rates of adware, spyware, Trojan horse and virus infections are reported. (page 7).
- 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. (page 11).
- SMBs have few IT personnel to help them address these challenges. Three-fourths of these companies have fewer than 10 people in their IT departments, and many have no IT department at all (page 12).
- Specialized technology solutions are needed to secure SMBs' computers and networks (page 19).

Most industrialized countries report that SMBs make up 97 to 99 percent of all companies.

DEFINING SMBs

Different organizations vary in the way they define SMBs. In the U.S., the Small Business Administration (SBA) defines "small business" as a company with fewer than 500 employees. This definition is often used as the basis for U.S. government statistics about small business; however, few legislative and regulatory proposals have relied on this definition. For example, the Family and Medical Leave Act defines a small business as employing 50 or fewer employees. The Savings Incentive Match Plan for Employees, created to provide small businesses with an opportunity to create an employee pension plan that has fewer administrative burdens than traditional pension plans, applies to companies with fewer than 100 employees.

In the European Union and international organizations such as the World Bank, the United Nations and the World Trade Organization, the term small and medium enterprise, or SME, is used more commonly than SMB. The SME definition can vary from country to country. The European Commission defines "small enterprises" as companies with fewer than 50 employees, and companies with between 50 and 249 employees are defined as "medium-sized enterprises."

Industry Canada defines SMEs as all businesses with fewer than 500 employees. In Canada, companies that produce goods are considered small enterprises if they have fewer than 100 employees, and service companies are defined as small if they have 50 or fewer employees. Companies that fall above the small enterprise definitions, yet have under 500 employees are considered medium-sized enterprises.

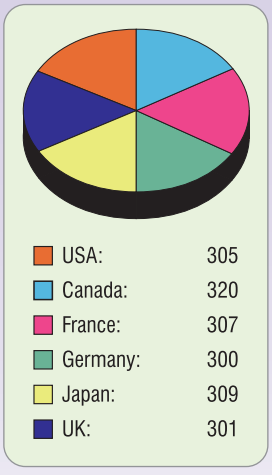
In Japan, the number of employees defining a SMB also varies by sector. Manufacturers are considered SMBs if they have 300 or fewer employees, wholesalers and service companies with 100 or fewer employees are SMBs, and resellers with up to 50 employees are SMBs.

Many private sector companies, including some prominent industry analyst firms, such as Forrester, Gartner and IDC, define small businesses as those with fewer than 100 employees. These same firms define mid-size or medium businesses as those with 100 to 999 employees.

The Webroot SMB Survey

Webroot provides industry leading security software for consumers, enterprises and SMBs worldwide. For the past several years, Webroot has been issuing quarterly reports about trends and research related to Internet security. In September of 2007, Webroot conducted a survey of security software decision makers in companies with five to 999 computers in Canada, France, Germany, Japan, the United Kingdom and the United States. The results of this survey are discussed in this report.

Webroot SMB Survey Respondents



THE ECONOMIC IMPORTANCE OF SMBs

While the precise definitions vary somewhat, there is global consensus that SMBs and SMEs comprise a significant part of the economic landscape. These companies are significant contributors to the world's economies in terms of both revenue generation and employment.

According to the SBA, 99.7 percent of all employers are companies with 500 or less employees. In April 2007, the SBA issued its report "The Small Business Share of GDP" finding that small businesses produced half of the private, non-farm gross national product in the United States. In addition the SBA has found that businesses with fewer than 500 employees account for half of all private-sector workers, and pay more than 45 percent of the U.S. private payroll.

U.S. SMBs produce half of the private, non-farm GDP.

The most recent national statistics issued by the Department of Trade and Industry (DTI) in the United Kingdom found that 99.9 percent of all UK companies have fewer than 250 employees. These small and medium enterprises also account for 58.7 percent of employment in the UK.

According to the Small and Medium Enterprise Agency within the Japanese Ministry of Economy, Trade and Industry, 99.7 percent of corporations in Japan are classified as SMBs.

The government of Canada web site states that companies with fewer than 100 employees comprise 95 percent of all business entities. These small businesses represent one third of the gross domestic product and employ about 40 percent of all working Canadians.

As these statistics indicate, most companies in the world are small and medium-sized businesses. Although larger corporations tend to get more attention, small and medium-sized companies are truly the lifeblood of the global economy and are significant economic contributors that have valuable financial and information assets. Computer and data security is one of the most pressing issues facing SMBs around the world.

SMBs account for 58.7 percent of employment in the UK. 99.7 percent of all companies in Japan are SMBs.

SMBs AND INTERNET SECURITY THREATS

Many CEOs and owners at small and medium-sized companies may think that large, global corporations are the primary targets for cyber-criminals. While large corporations certainly must be vigilant to protect themselves, SMBs must be equally vigilant as there are several factors that put SMBs at significant risk of being impacted by data security threats.

- Criminals will focus on targets that are easy to find and there are many more SMBs than large corporations in the world.
- Large enterprise networks typically have a layered defense system in place that is likely to be more difficult for criminals to penetrate.
- Many SMBs hold sensitive personal information about their employees and customers, and while there may be fewer records than in large computer systems, this information is equally as valuable.
- SMBs have fewer financial and human resources than larger companies, and thus rarely have the same level of expertise and technological protection.

Cyber-criminals will concentrate on the easiest marks.

SMBs face a complex Internet security landscape that includes:

- Growing Web threats
- Underestimation of certain threats
- Regulatory requirements

This combination makes for a potentially high-risk environment for many SMBs.

Growing Web Threats

"The Growing Web Threat" issued by Gartner in April 2007 found that Web sites and Internet applications will be the primary source of malware infections in 2008. According to Gartner, the private, personal, sensitive information held by companies large and small can be "easily monetized" by would-be Internet criminals. In addition to stealing information that can be easily sold or used in identity theft and similar crimes, many spyware infections also aim to gain control of a PC so that it can be exploited, without the user's knowledge, to distribute adware and spam. Whether distributed via a Web site, e-mail, instant messaging or some other means, all seek to then use the Internet connection as a way to communicate back to the source and/or to download additional spyware onto the computer.

Web sites and Internet applications will be the primary source of malware infections in 2008.

When respondents to Webroot's SMB survey were asked if online threats are becoming more serious, over a third felt strongly that they are, and in Germany over half of the respondents felt strongly that online threats are becoming more serious.

Are Online Threats Becoming More Serious?

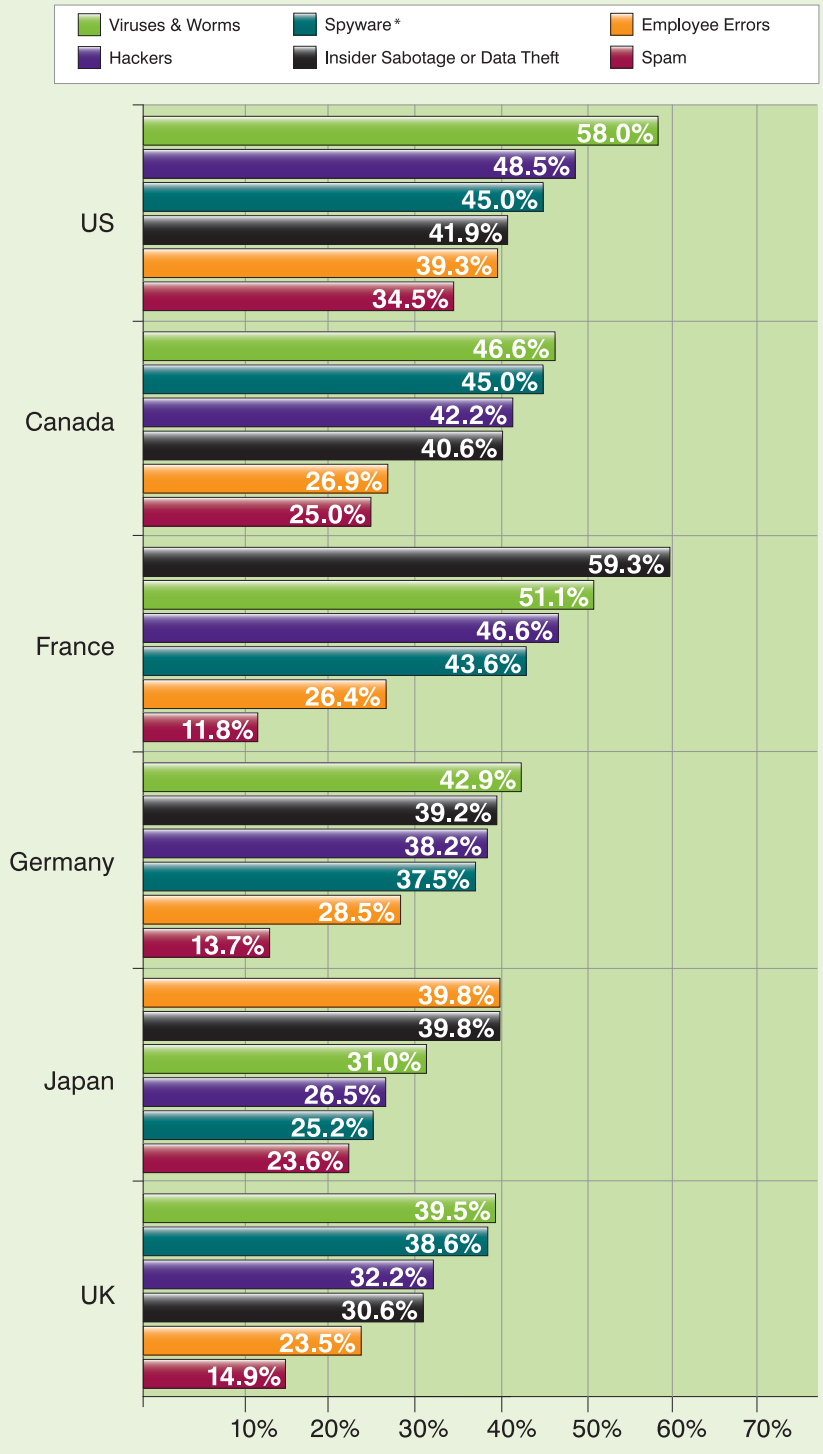
	US	Canada	France	Germany	Japan	UK
Strongly Agree	43.3%	39.1%	27.7%	54.5%	36.6%	35.5%
Agree Somewhat	44.3%	38.8%	50.8%	30.6%	39.8%	44.5%

Source: Webroot SMB Survey, September 2007 (N=1842)

Survey respondents also provided their perspectives about what they see as the most serious threats to their organization's online security.

SMBs Rating Threat as Very or Extremely Serious

Rating Listed by Percentage by Country



Source : Webroot SMB Survey, September 2007 (N=1842)

** Defined for this question as keyloggers, system monitors, Trojans, rootkits, browser hijackers and dialers*

The SMBs surveyed have experienced many of these threats firsthand over the past year. Across the six countries surveyed, spam was the most prevalent issue experienced. In each of the countries, the top three greatest number of infections after spam were a combination of adware, spyware, Trojan horses and viruses. These results reflect reported or known infections and do not take into account any infections that have gone undetected.

SMB Infections Experienced in the Past Year

	US	Canada	France	Germany	Japan	UK
Adware	65.9%	67.5%	50.8%	28.3%	– *	47.5%
Keylogger	18.4%	12.8%	7.5%	2.7%	2.3%	8.0%
Phishing	49.8%	41.7%	17.9%	22.3%	3.2%	35.9%
Pharming	17.0%	11.9%	3.9%	4.7%	1.0%	6.0%
Rootkit	18.4%	12.8%	6.2%	7.0%	1.0%	4.0%
Spam	86.2%	84.1%	84.0%	78.3%	35.3%	76.1%
Spyware	71.5%	70.9%	32.6%	37.0%	17.5%	51.2%
System Monitor	22.6%	17.8%	6.5%	9.0%	1.9%	8.0%
Trojan Horse	42.3%	48.4%	49.2%	38.7%	11.3%	33.9%
Virus	61.3%	62.8%	60.6%	50.7%	30.1%	45.5%

** Adware was not included as a category in the Japanese study*
Source: Webroot SMB Survey, September 2007 (N=1842)

These high infection rates occurred even though almost all of the SMBs surveyed have an antivirus solution installed.

SMBs That Have an Antivirus Solution Installed						
	US	Canada	France	Germany	Japan	UK
Have an Antivirus Solution Installed	96.4%	97.8%	96.7%	96.3%	92.4%	96.3%
Source: Webroot SMB Survey, September 2007 (N=1842)						

While antivirus protection is an important piece of an overall Internet security solution, it often lacks the detailed intelligence needed to deflect the diverse threats evident on the Internet today. SMBs face a spectrum of threats beyond viruses, some of which may not yet be well understood.

Underestimation of Certain Threats

In some cases, SMBs may be underestimating the consequences of certain infections. For example, while most would agree spam by itself is more of a nuisance than a serious threat, often spam is a carrier for more serious threats, such as spyware, viruses and worms.

Spam is cheap for companies. There is almost zero cost associated with mass junk mailings. This makes it an easy and cheap delivery mechanism for malicious attacks. Users who click ads in spam, or even look at a spam e-mail in their preview pane, may be at risk of downloading spyware – commonly referred to as a drive-by download.

A particularly harmful type of spam is phishing. The appearance of these e-mails and fake sites they link to are made to look identical to valid, trustworthy companies, however the scam then asks for personal information, such as credit card, bank account, PIN, or Social Security numbers.

According to the 2006 Annual Report of the Internet Crime Complaint Center, a partnership between the U.S. Federal Bureau of Investigation and the National White Collar Crime Center, of all the fraudulent acts reported in 2006, 73.9 percent used e-mail as the mechanism of contact, and 36 percent used a Web page.

Spyware is another threat that SMBs may be underestimating. The Anti-Spyware Coalition defines spyware as technologies deployed without appropriate user consent and/or implemented in ways that impair user control over:

- Material changes that affect their user experience, privacy, or system security;
- Use of their system resources, including what programs are installed on their computers; and/or
- Collection, use, and distribution of their personal or other sensitive information.

Nearly 74 percent of fraudulent acts reported to the Internet Crime Complaint Center in 2006 used e-mail as the contact mechanism.

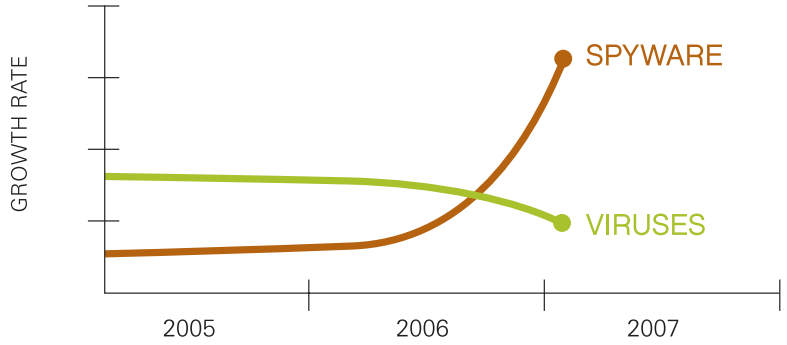
Spyware is another threat that SMBs may be underestimating.

While spyware and Trojan horses were among the most highly reported infections in the Webroot SMB survey, less than 50 percent across all the countries surveyed consider spyware a very or extremely serious threat. This is particularly concerning. Spyware purveyors are constantly releasing new programs designed to defy detection, resist removal and morph frequently.

In contrast to viruses, that typically make their presence known by spreading across many systems simultaneously and impacting machine functionality, the success of spyware programs depends on their stealth nature. Given the significant financial incentives for 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. The potential for financial reward is a strong incentive for the ongoing proliferation of spyware at higher rates than viruses or other types of malware.

Spyware purveyors are constantly releasing new programs designed to defy detection, resist removal and morph frequently.

A 2006 report from ScanSafe indicated that the number of new spyware threats increased by 254% last year while viruses were on the decline.



Regulatory Requirements

In addition to the business risks associated with these security threats, SMBs may also face legal and regulatory compliance issues. Governments in many parts of the world have instituted additional data protection measures to compel companies to adequately protect the sensitive customer data in their possession. While legal and regulatory compliance can often be expensive, it is a cost of doing business in that given jurisdiction. Even more costly is the potential liability for a company that fails to comply with the appropriate legal requirements to safeguard sensitive information.

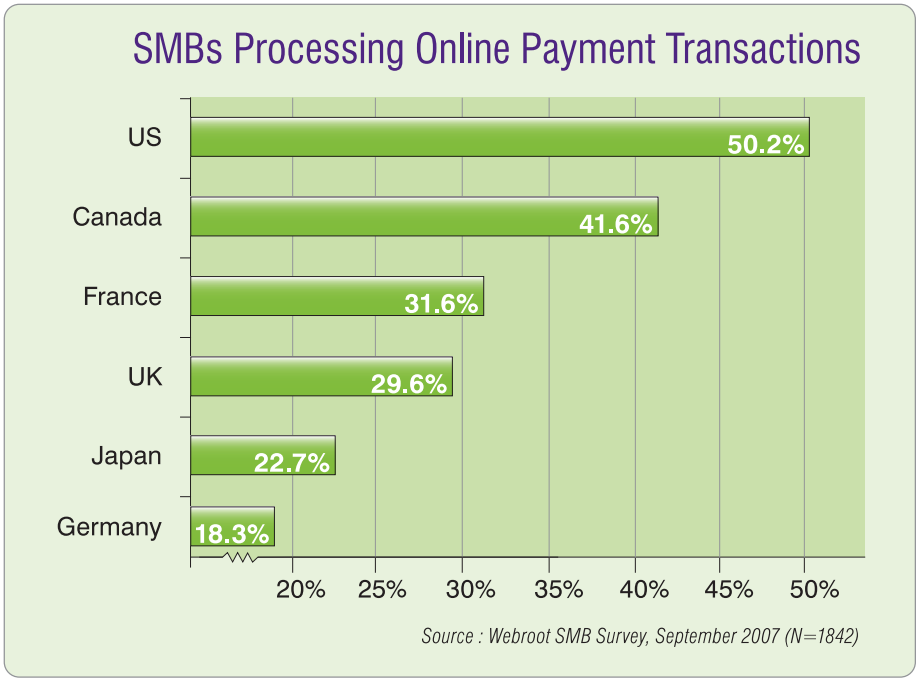
Even more costly is the potential liability for a company that fails to comply with the appropriate legal requirements to safeguard sensitive information.

One of the most well known laws in this regard is the European Union's Data Protection Directive. This Directive sets out the guidelines on which European countries have crafted their laws. Article 17 of the Directive requires:

> *Member States shall provide that the (data) controller must implement appropriate technical and organizational measures to protect personal data against accidental or unlawful destruction, alteration, unauthorized disclosure or access, in particular where processing involves the transmission of data over a network.*

Japan enacted a similar measure, the Personal Information Protection Law, in May 2003. In the United States several laws set out data protection requirements. For example, the U.S. Health Insurance Portability and Accountability Act requires that the privacy of medical records be adequately protected against unauthorized access and misuse. In the financial sector, the Gramm-Leach-Bliley Act requires that organizations which maintain credit information for customers be held accountable if that data is accessed or compromised by an unauthorized third party. Incidents of unauthorized network access and spyware, such as system monitors or Trojans, raise concerns about noncompliance.

Beyond country laws, there are also globally recognized guidelines, such as the Payment Card Industry (PCI) Data Security Standard, which applies to all companies that process any credit card information whether from consumer or businesses customers. This standard is directly applicable to many SMBs around the world, including approximately half of SMBs in the United States.



HEIGHTENING THE RISKS FOR SMBs

Beyond the external threats and regulatory requirements facing SMBs, there are several internal factors that heighten the Internet security risks for SMBs, including:

- Pervasive Internet use
- Home-based and remote workers
- Lack of policies or restrictions for employee Internet use
- Storage of valuable customer and employee data
- Limited in-house expertise
- Budget and resource constraints

At least 66 percent of all businesses in the UK use the Internet.

Pervasive Internet Use

Over recent years, the trends of widespread network access, declining costs of bandwidth and the expanse of Internet resources have made it easier for entrepreneurs and business owners to launch and grow their companies.

The Annual Small Business Survey published in November 2006 by DTI reported that at least 66 percent of all businesses in the UK use the Internet. Most common uses cited were e-mail, purchasing and marketing.

Network connectivity enables SMBs to more easily:

- Communicate with customers and suppliers
- Market their services to a broader geographic audience
- Gather business and product research
- Access Web-based distribution channels, such as Amazon.com and eBay

Increased reliance on the Internet has served as a key driver in the growth and vibrancy of the SMB sector. In the "SMB State of the Union Study" issued in December 2005, 83 percent of SMBs surveyed strongly agreed that the Internet helps them run their companies. The November 2006 Everon Technology Insider newsletter reported that a subscriber survey found that 77 percent of small businesses said their success depends on the Internet. At the same time, those network connections that bring all the benefits of the Internet also expose SMBs to new security threats.

Seventy-seven percent of small businesses said their success depends on the Internet.

Along with the many growth opportunities that have been realized as a result of pervasive Internet use, SMBs must also face the risks that accompany an interconnected world.

Home-Based and Remote Workers

Home-based and remote workers pose security challenges for all companies and this is particularly true for small and medium-sized enterprises. Many SMBs start out or remain home-based businesses. Internet connectivity allows employees to work more easily from their homes and remote locations. SMBs can on-board home-based and remote employees more rapidly by minimizing the need and overhead costs of large office spaces.

While working remotely has become the norm in many companies, it is generally more difficult to maintain security on remote PCs. It's common for employees to use unauthorized mobile devices to access sensitive corporate data, or to rely on open, unsecured wireless networks to connect to work. This creates even more routes for malicious software to infect computers and company networks. Network-level controls are insufficient. Every machine needs to be secure as well.

Lack of Policies or Restrictions for Employee Internet Use

A significant number of the respondents to the Webroot SMB Survey categorized employee errors and sabotage or data theft by insiders as very or extremely serious threats to the organization. In fact, insider sabotage or data theft ranked higher than any other potential threat for the SMBs in France and Japan.

Forty to sixty percent of SMBs lack a policy or technology to restrict or monitor employees' personal use of work computers.

Rated as Very or Extremely Serious Threats to the Organization

	US	Canada	France	Germany	Japan	UK
Employee Errors	39.3%	26.9%	26.4%	28.5%	39.8%	23.5%
Insider Sabotage or Data Theft	41.9%	40.6%	59.3%	39.2%	39.8%	30.6%

Source: Webroot SMB Survey, September 2007 (N=1842)

To mitigate the risks of intentional sabotage and data theft by employees, SMBs must consider appropriate technological tools to monitor and protect their company computer and network assets. Concerns about employee errors are exacerbated by the fact that often employees are unaware the potential harm that their Internet surfing and downloading can cause to their work computer and company network. The negative impacts of employees who inadvertently infect the business with spyware and other harmful programs can be mitigated by employee education along with the establishment and enforcement of an Acceptable Use Policy.

Yet, in spite of these serious concerns, 40 to 60 percent of SMBs in the same survey lack a policy or technology to restrict or monitor employees' personal use of work computers.

Percentage of SMBs Without a Policy or Technology in Place to Restrict or Monitor Employees' Use, by Category

	US	Canada	France	Germany	Japan	UK
Downloading Music	36.4%	36.8%	52.1%	56.5%	67.3%	42.5%
Personal E-mail	49.8%	55.2%	67.1%	60.8%	57.0%	53.2%
Personal Instant Messaging	43.0%	45.7%	57.1%	58.5%	71.2%	44.9%
Visiting Non-Work Related Web Sites	44.9%	48.3%	55.0%	63.1%	62.8%	51.2%

Source: Webroot SMB Survey, September 2007 (N=1842)

Particularly in organizations that do not have any formal policy or restrictions, it is likely that personal use of company computers and network access is pervasive. Not only does this represent significant security risks to the organization, it can also be a significant loss to productivity. The Office of the Inspector General at the U.S. Department of Interior conducted an investigation in 2006 and found that the personal Internet use of their 80,000 employees was costing the Department almost $39,000 per week and over $2 million a year.

Storage of Valuable Customer and Employee Data

All of these trends are particularly disconcerting, considering the volume of sensitive data held by small and medium-sized companies around the world. In March 2007, the National Federation of Independent Businesses (NFIB) and Visa USA announced the results of a survey of companies with fewer than 250 employees. Fifty-two percent said they keep at least one type of sensitive customer information, such as social security numbers or credit card numbers. Yet, an alarming 61 percent said they have never sought information about how to properly handle and store customer information. In the same survey, 57 percent did not see securing customer data as something that requires formal planning, and 39 percent said they simply rely on "common sense" to keep data safe. These results indicate that many SMBs may be underestimating the value that external entities put on the sensitive customer information they hold.

Fifty-two percent of SMBs keep at least one type of sensitive customer information.

In the United States, government offices responsible for protecting consumer interests, such as the U.S. Federal Trade Commission (FTC) and several U.S. state Attorneys General have become increasingly proactive in filing complaints against companies for lax computer security measures. For example, the FTC filed a case against DSW, Inc. (FTC File No. 052-3096) stating the company created unnecessary risks to the personal information collected about consumers in its stores by failing to use readily available security measures to protect its computer networks nor employing sufficient measures to detect unauthorized access.

Limited In-House Expertise

One likely reason so many SMBs indicate they have not sought information about how to properly handle and store customer information is a lack of in-house data security experts to drive these efforts. SMBs have few information technology (IT) staff personnel to support their computer and network needs and often lack personnel and resources dedicated to data security.

Sixty-one percent have never sought information about how to properly handle and store customer information.

In the Webroot SMB survey, approximately three-fourths of the respondent companies have fewer than 10 people in their IT departments to staff all their IT needs – desktop, software and server support – as well as Internet security matters. In Japan, 39.8 percent of the companies have no IT department at all. Even SMBs with larger, mature IT organizations, often lack a dedicated or centralized security team.

Three-fourths of SMBs surveyed have fewer than 10 people in their IT department.

IT Staff for SMBs						
	US	Canada	France	Germany	Japan	UK
None / No IT Dept.	8.9%	8.8%	20.2%	26.9%	39.8%	26.9%
1-2 Total IT Staff	22.3%	29.7%	26.4%	24.6%	19.1%	29.6%
3-9 Total IT Staff	26.6%	30.6%	28.7%	29.6%	19.1%	29.6%
Total SMBs with Fewer than 10 Staff	57.7%	69.1%	75.3%	81.1%	78.0%	78.1%
Source: Webroot SMB Survey, September 2007 (N=1842)						

Budget Constraints

Compounding the issue of small IT staffs typical in SMBs are smaller IT budgets. Forrester Research's "2007 SMB IT Budget Outlook," issued in February 2007, found that SMBs will average only a two percent rise in IT budgets, and SMBs expect to spend only nine percent of their IT budget on security.

Almost 40 percent of the SMBs in Japan have no IT department at all.

Smaller IT budgets available at SMBs directly impact their ability to attract and retain qualified IT personnel since they often have less money available for compensation. The April 7, 2007 issue of CIO Insight magazine included an article by Allan Alter entitled, "Unequal Pay for Equal Experience" that reports chief information officers at companies with less than $500 million in annual revenue "earn 58 cents for every dollar earned by CIOs at larger organizations." While their salaries differ significantly, the report found that the smaller company CIOs and larger company CIOs varied little in terms of experience and other factors.

SMBs expect to spend only nine percent of their IT budget on security.

THE BUSINESS IMPACTS FOR SMBs

There are many Internet security risks that can have numerous negative business effects for SMBs, including:

- Loss of sensitive information
- Theft of intellectual property/trade secrets
- Slowed system performance
- Employee downtime
- Costly computer repairs
- Legal fees due to lawsuits
- Brand/reputation damage
- Company closure

Unfortunately, there are numerous incidents and stories of organizations who have been the victims of Internet crimes. Often companies try to keep these incidents quiet, attempting to avoid the negative publicity that they can generate. One incident that received considerable media attention in the U.S. happened to the government of Carson, California in June 2007. According to the Los Angeles Times, a hacker installed a keylogger on the city treasurer's computer and was able to capture bank passwords. The hacker then attempted to steal $450,000. In this case, the city government official quickly noticed the unauthorized transfers and working with the banks was able to head off most of the loss. Many organizations are not this fortunate and as a result most will never be willing to talk to reporters about such incidents.

Direct financial loss is only one of several business impacts facing companies today. The Webroot SMB survey found that spyware and viruses affected organizations by:

- Causing lost sales
- Compromising confidential information
- Disrupting business activities
- Draining IT resources
- Reducing employee productivity
- Slowing system performance
- Threatening sensitive online transactions

A hacker using a keylogger to gather bank passcodes attempted to steal $450,000 from the local government in Carson, California.

In five of the countries surveyed, an even greater number of SMBs were affected in these ways by spyware than by viruses. Japan was the exception where more SMBs were affected by viruses. This reinforces the earlier point that SMBs, who across the board rated viruses and worms as a more serious concern than spyware, may be underestimating the seriousness of the spyware threat.

How SMBs are Affected by Spyware and Viruses

	US		Canada		France		Germany		Japan		UK	
	Spyware	Virus	Spyware	Virus	Spyware	Virus	Spyware	Virus	Spyware	Virus	Spyware	Virus
Caused Lost Sales	47.2%	47.5%	32.9%	32.9%	24.4%	33.0%	17.9%	22.4%	8.1%	16.1%	19.3%	17.0%
Compromised Confidential Info	57.7%	52.5%	43.1%	40.3%	37.8%	39.4%	34.4%	35.4%	5.1%	11.9%	25.0%	25.3%
Disrupted Business Activities	79.1%	73.4%	67.5%	60.6%	66.4%	62.6%	47.9%	48.0%	24.9%	57.0%	53.8%	46.2%
Drained IT Resources	80.7%	74.2%	74.0%	67.2%	54.4%	51.8%	44.6%	45.3%	16.1%	33.4%	60.4%	55.5%
Reduced Employee Productivity	82.6%	74.1%	77.5%	67.2%	58.0%	55.0%	45.6%	48.7%	19.1%	36.6%	56.8%	47.8%
Slowed System Performance	86.5%	76.4%	82.9%	73.2%	68.3%	62.6%	61.0%	55.1%	28.8%	52.8%	69.6%	57.8%
Threatened Sensitive Online Transactions	61.0%	53.4%	40.9%	39.7%	35.6%	32.9%	27.0%	27.3%	10.3%	27.0%	27.0%	23.2%

Source: Webroot SMB Survey, September 2007 (N=1842)

MITIGATING THE RISKS FOR SMBs

Given all the risks and challenges outlined, network security can seem overwhelming to SMBs. Even before selecting the best technology product, there is a strong consensus about the kinds of steps companies should take to establish effective policies and educate employees.

While only 50 percent or less of the SMBs surveyed by Webroot indicated they are processing online payment transactions, the guidelines provided by the PCI Data Security Standard are very applicable and useful for all companies to follow. The PCI provides these objectives:

- Build and maintain a secure network
- Protect cardholder data
- Maintain a vulnerability management program
- Implement strong access control measures
- Regularly monitor and test networks
- Maintain an information security policy

The PCI standard provides details about how to best fulfill each of these objectives. Specific elements of the standard, such as ensuring that antivirus programs can protect against other forms of malicious code such as spyware and adware, offers important guidance for all companies, even those that do not accept credit cards as a form of payment.

Another set of guidelines that can be broadly applicable are issued by the U.S. Federal Deposit Insurance Corporation (FDIC). The FDIC letter of guidance recommends:

- Restricting users from downloading software not previously approved
- Expanding the risk-assessment process to consider threats from spyware
- Expanding security and Internet use policies to include risks associated with spyware and acceptable user behavior
- Taking steps to enforce these policies and reprimand employees or contractors who fail to comply
- Installing and configuring firewalls to monitor both inbound and outbound traffic. If possible, block outbound ports that are not necessary for business functions
- Implementing tools to scan e-mail for spam and either block the e-mail or designate it as spam
- Implementing tools to restrict or prevent pop-up windows

The Anti-Spyware Coalition (ASC) assembled a set of tips for organizations to protect their networks and mitigate spyware. To educate employees and other network users the ASC recommends:

- Require network users to agree to an Acceptable Use Policy indicating that unauthorized programs can be blocked.
- Teach employees and other computer users to understand that many "free" programs and services on the Internet install spyware that drastically slows PCs, installs annoying pop ups, and steals private and corporate information.
- Ensure IT support staff is trained to recognize the less overt spyware symptoms, including very long boot up, slow and erratic application performance, frequent computer crashes so that proper remediation can be taken.

The ASC offers these additional tips to protect company computers and networks:

- Maintain up-to-date detection patterns and software updates
- Select desktop security software that can be centrally deployed and managed
- Maintain current operating system and browser patches to minimize vulnerability to security exploits
- Ensure Web browsers are set to at least "medium" in the security and privacy settings
- Do not allow users to surf the Internet while logged on with "administrator" privileges to the network
- Maintain a list of allowable software and/or executable files and run a weekly scheduled check against PCs in the network. Check results for non-standard entries and take appropriate actions to remove unapproved programs
- Consider re-imaging chronically spyware-infected PCs
- Configure gateway proxies and firewalls to prevent
  - "drive by" downloads (non-approved CAB and OCX files)
  - executable downloads from known spyware sites (identified by content filtering lists)
  - executable downloads from suspected/high-risk sites (sites in categories with high incidents of spyware)
  - PC communication to known spyware "phone home" sites and report which PCs are likely infected with spyware
- Scan files at the gateway for known spyware code files at the gateway for known spyware code
- Maintain strong anti-spam protection

Require an Acceptable Use Policy agreement with all network users.

Implementing strong Internet security policies and processes is critical to ensure that the technological tools utilized are fully effective.

FINDING THE BEST TECHNOLOGY SOLUTION

In addition to establishing best practice policies and educating employees, SMBs need to fight technical threats with technology. The time and effort required to effectively battle online security threats can be daunting for a growing business - not to mention the importance of selecting a solution that will continue to support your company as it grows.

Critical to a company's security infrastructure is a centrally managed desktop threat solution. Most effective will be those SMBs that remain focused on these Internet security priorities, and select industry-leading solutions to address these needs:

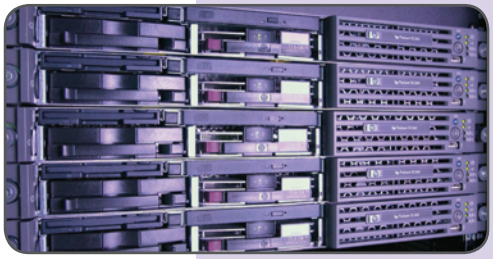
- Prevent the installation of unauthorized software
- Monitor network use and abuse
- Block inappropriate content on the Web
- Remove useless files to free up disk space (temp files, memory dumps)
- Set custom policies to manage employee Internet, network, and application use

Critical to a company's security infrastructure is a centrally managed desktop threat solution.

Additionally, SMBs require seamless, scalable deployments that provide centralized, customizable user management, including coverage for laptops and remote employees. Internet security infrastructure solutions need to provide proactive, accurate threat detection that minimizes false positives and provides comprehensive removal in real-time.

In evaluating options, SMBs should consider:

- One size does not fit all
- Freeware is not really free
- Firewalls and antivirus are only part of the solution
- Specially designed products best address the problem



One Size Does Not Fit All

Security software programs that claim to do it all for all kinds of companies can not deliver the specialized expertise needed to address the most serious threats. Spyware in particular is uniquely developed to bury itself in a computer file structure, making it both hard to detect and even harder to remove without causing other damage to the computer. Extensive experience and dedicated research teams are critical to the development of the most effective solution.

Freeware is Not Really Free

Freeware is a software program that can be downloaded free of charge. While this approach may be tempting to SMBs with tight budgets, the adage, "you get what you pay for" comes to mind. Typically, organizations offering freeware rely on voluntary contributions to create and update their software. These programs lack robust functionality, centralized management capabilities and daily updates – all critical to ensuring an effective level of protection.

Freeware can create additional burdens for IT staff, as it often lacks centralized management, making definition updates and sweeps manual and more time consuming. There may also be legal implications for companies relying on freeware. Many of these solutions are intended for individual consumer desktops, and are not intended for deployment on multiple company computers. Often the user agreements reveal that using the software in a corporate environment does require a licensing fee.

In addition, software offered for free lacks the quality and sophistication that business organizations require to protect their IT resources.

Firewalls and Antivirus are Only Part of the Solution

While gateway protection in the form of firewalls can help to block certain kinds of attachments and some types of malicious code, they leave a very significant vulnerability. Spyware is typically embedded in legitimate traffic, such as e-mail or on Web sites with other valid purposes. Further, once installed on a system most spyware programs disguise themselves as trusted programs, allowing them to communicate freely with the Internet over ports that are often left unprotected by firewalls.

Likewise, antivirus software is only a part of the technological solution required. Antivirus products, particularly those promoted as a one-size-fits-all package, lack the detailed intelligence needed to deflect the diverse threats evident on the Internet today.

Specially Designed Products Best Address the Problem

Sophisticated threats require specially designed products. Spyware and other malicious programs can infect a computer from a range of entry points including Internet-based applications, peer-to-peer sharing channels and removable media. Regardless of how it arrives, spyware must execute on the desktop or laptop to infect the computer. Thus, to detect, block and remove spyware and prevent damage to the network and other computers in the company, there should be antispyware software on every desktop that is part of an overall, centrally managed enterprise solution.

To ensure that SMBs are fully protected, their Internet security solution should include an antispyware program that provides:

Regular definition updates -- Many free antispyware software downloads do not provide adequate protection against spyware programs because they are not supported by ongoing threat updates. This leaves PCs open to attack from evolved or newly introduced malicious spyware programs. Regular updates to the threat database protect companies from new rapidly-evolving or changed applications, as well as the latest worms and its family of variants.

Refined spyware detection -- Some software scans yield false positives to make customers think there are more detections of traces than competitor products. If the software isn't capable of detecting and effectively removing malicious spyware programs, privacy is at risk. Truly useful and beneficial antispyware software only finds and removes spyware, and does not impact other programs or files.

Proactive protection -- Detection and removal of spyware programs is only half of the antispyware software solution. It's equally important to stop spyware programs before they reach computers. Smart Shields prevent spies from installing real time on PCs. This proactive protection defends system and browser elements while simultaneously guarding information and privacy.

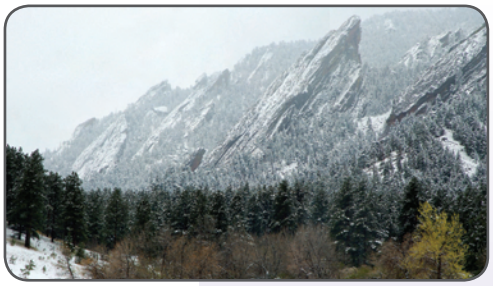
Designated threat research team -- Often, it's not financially possible for companies that offer free antispyware software to house a team of dedicated threat researchers. Updates may be erratic, poorly programmed or non-existent. A threat research team knows what to look for, and how to most effectively find and remove spyware from a users PCs.

Customer service -- Most free antispyware software is not backed by expert customer support, e-mail support or online help sections. The best software providers offer reliable support to their customers.

Easy-to-use interface -- It takes several versions to determine the best and most user-friendly interface. Like research teams, interface improvement is not always an area of focus for all antispyware software providers.

Stable company to back up the software -- It's important to identify credible software that is backed by an established company so you have recourse if you encounter a problem with your purchase or software functionality.

ABOUT WEBROOT SOFTWARE



Webroot Software provides industry leading security software for consumers, enterprises and small and medium-sized businesses worldwide. Globally recognized for its award-winning Spy Sweeper® line of antispyware and antivirus products, Webroot security software consistently receives top review ratings by respected third-party media and has been adopted by millions globally. Webroot AntiSpyware Corporate Edition (formerly Spy Sweeper Enterprise) is a comprehensive, centrally managed solution that aggressively blocks, detects and eradicates spyware on desktops across the network. Webroot AntiSpyware Corporate Edition with AntiVirus offers combined protection for spyware and viruses. Available either as branded solutions or on an OEM basis, Webroot products can be found online at www.webroot.com and on the shelves of leading retailers worldwide. Webroot global headquarters are located in Boulder, Colorado.

To find out more visit www.webroot.com or call 1.800.772.9383.

About the Research

In August and September 2007, Webroot sponsored online surveys of companies with five to 999 seats in Canada, France, Germany, Japan, the United Kingdom and the United States. Survey Sampling International invited panel members who are desktop security decision-makers to participate. Three hundred or more responses were received from each country. The margin of error for each study is ±5.7 percentage points.

Certain data is available upon request.

APPENDIX

Appendix I: The Symptoms of a Spyware Infection

Some common visible symptoms of a spyware infection include:

- A barrage of unsolicited pop-up ads
- Browser hijacking so that the Web site that appears is not the one typed in the address bar
- Sudden or repeated changes to the computer's Internet homepage not made by the user
- New, unexpected or unrequested toolbars
- New, unexpected or unknown icons appearing on the desktop or in the tray at the bottom of the screen
- Problems with keys malfunctioning or not working at all
- Random error messages
- Performance degradation with long delays in opening programs or saving files
- Antispyware or antivirus software is turned off, or malfunctioning
- Unidentified toll charges on your phone bill

It is important to note that often the most dangerous forms of spyware will not display and visible signs, as they are designed to be stealth and remain on the computer unnoticed by the user.

Appendix II: Glossary

Adware

Adware is advertising-supported software that displays pop-up advertisements. Adware is usually available via free downloads from the Internet. Adware is often bundled with or embedded within freeware, utilitarian programs like filesharing applications, search utilities, information-providing programs (such as clocks, messengers, alerts, weather, and so on), and software such as screensavers, cartoon cursors, backgrounds, sounds, etc. Although seemingly harmless, some adware programs may track your Web surfing habits. Deleting adware may result in the deletion of the bundled freeware application.

Antispyware software

Antispyware software protects a PC from spyware infection. Spyware protection software will find and remove spyware without system interruption.

Botnet

A botnet is a collection of computers running remote control software programs and under a common command and control infrastructure via a public or private network. Botnets can be used for sending spam remotely, installing more spyware without consent, and other illicit purposes.

Browser Hijackers

Sometimes called Home Page Hijackers, browser hijackers have the ability to change your default home page as well as other Web browser settings. Common behavior also includes adding advertising, pornographic, or other unwanted bookmarks, creating pop-up advertisements, and redirecting mistyped or incomplete URLs. Additionally, browser hijackers may redirect your searches to "pay-per-search" Web sites.

Cookie (or Adware Cookie)

Cookies are pieces of information that are generated by a Web server and stored on your computer for future access. Cookies were originally implemented to allow you to customize your Web experience. However, some Web sites now issue adware cookies, which allow multiple Web sites to store and access cookies that may contain personal information (surfing habits, usernames and passwords, areas of interest, etc.), and then simultaneously share the information with other Web sites. Adware cookies are installed and accessed without your knowledge or consent, and in some cases this sharing of information allows marketing firms to create a user profile based on your personal information and sell it to other firms.

Dialer

Dialers have the ability to disconnect your computer from your local Internet provider and reconnect you to the Internet using an expensive pornographic, toll, or international phone number. They do not spy on you, but they may rack up significant long distance phone charges. They have the ability to run in the background, hiding their presence.
Worst case scenario: Dialers may rack up significant long distance phone charges.

Distributed Denial-of-Service (DDoS) Attack
A means of burdening or effectively shutting down a system by bombarding it with an overwhelming amount of traffic. DDoS attacks are often launched using botnets. A vulnerability in one computer system can be exploited to make it the DDoS master.

Drive-by download
When programs are downloaded without the user's knowledge or consent. Most often accomplished when the user clicks to close or eliminate a random advertisement or other dialogue box.

Encryption
Encryption is the scrambling of data so it becomes difficult to unscramble and interpret.

Exploit/Security Exploit
A piece of software that takes advantage of a hole or vulnerability in a user's system to gain unauthorized access to the system.

Firewall
A firewall prevents computers on a network from communicating directly with external computer systems. A firewall typically consists of a computer that acts as a barrier through which all information passing between the networks and the external systems must travel. The firewall software analyzes information passing between the two and rejects it if it does not conform to pre-configured rules. Firewalls provide effective protection against worm infection, but not against spyware like Trojans, which hide in legitimate applications, then install secretly on a user's PC when the application is launched.

Hijackers (Home Page Hijacker or Browser Hijacker)
Hijackers have the ability to change your default home page as well as other Web browser settings. Common behavior also includes adding advertising, pornographic, or other unwanted bookmarks, creating pop-up advertisements, and redirecting mistyped or incomplete URLs. Additionally, home page hijackers may redirect your searches to "pay-per-search" Web sites.

Information Privacy
The interest an individual has in controlling, or at least significantly influencing, the handling of data about themselves.

Host File
The host file stores the Internet Protocol address of a device connected to a computer network. Some spyware can change a host file in order to redirect users from a site that they want to visit to sites that the spyware company wants them to visit.

Keylogger
A keylogger is a type of system monitor that has the ability to record all keystrokes on your computer. Therefore, a keylogger can record and log your e-mail conversations, chat room conversations, instant messages, and any other typed material. They have the ability to run in the background, hiding their presence. In some cases, a third party may be able to obtain private information such as usernames, passwords, credit card or Social Security numbers.

Operating System
The operating system (OS) is usually the underlying software that enables you to interact with the computer. The operating system controls the computer storage, communications and task management functions. Examples of common operating systems include: MS-DOS, Mac OS X, Linux and Windows.

Personally Identifiable Information (PII)
Information such as name, address, phone number, credit card information, bank account information, or social security number.

Privacy
The interest that individuals have in sustaining a 'personal space,' free from interference by other people and organizations.

Privacy Policy
A privacy policy outlines the responsibilities of the organization that is collecting personal information and the rights of the individual who provided the personal information. Typically, this means that an organization will explain why information is being collected, how it will be used, and what steps will be taken to limit improper disclosure. It also means that individuals will be able to obtain their own data and make corrections if necessary.

Registry
A computer registry is a database integrated into certain operating systems which stores information including user preferences, settings and license information about hardware and software installed on a user's computer. Spyware often changes registry values in order to take control of parts of the system. These changes can impair the regular function of the computer.

"Remove Me"
Remove me is an option often included in spam which is fake. That is, if you respond to request removal, you very well may be subjecting yourself to more spam, because by responding, the sender knows that your e-mail account is active. A 2002 study performed by the FTC demonstrated that in 63 percent of the cases where a spam offered a "remove me" option, responding either did nothing or resulted in more e-mail.

Rootkit
A rootkit is a program that fraudulently gains or maintains administrator level access that may also execute in a manner that prevents detection. Once a program has gained access, it can be used to: monitor traffic and keystrokes; create a backdoor into the system for the hacker's use; alter log files; attack other machines on the network; and, alter existing system tools to circumvent detection. Rootkit commands replace original system command to run malicious commands chosen by the attacker and to hide the presence of the rootkit on the system by modifying the results returned by suppressing all evidence of its presence.

Shareware
Software distributed for evaluation without cost, but that requires payment to the author for full rights is commonly called shareware. If, after trying the software, you do not intend to use it, you simply delete it. Using unregistered shareware beyond the evaluation period is "pirating."

Spam
Spam is the common name for unsolicited commercial e-mail. It is sent, usually in bulk, through "open-relays" to millions of people. Spam is cost-shifted advertising. It takes a toll on Internet users' time, their resources, and the resources of Internet Service Providers (ISP). Most recently, spammers have begun to send advertisements via text message to cell phones.

Spyware
Spyware is any application that makes potentially unwanted changes to your computer while collecting information about your computer activities. This information may then be sent to a third party for malicious purposes, without your knowledge or consent. Spyware can be distributed by bundling with freeware or shareware, through e-mail or instant messenger, as an ActiveX installation, or by someone with access to your computer. Unlike traditional personalization or session cookies, spyware is difficult to detect, and difficult (if not impossible) for the average user to remove without the use of an effective antispyware program.

System Monitor
System monitors have the ability to monitor all computer activity. They range in capabilities and may record some or all of the following: keystrokes, e-mails, chat room conversations, instant messages, Web sites visited, programs run, time spent, and even usernames and passwords. The information is gathered via remote access or sent by e-mail, and may then be stored for later retrieval. In some cases, a third party may be able to gain access to private information such as usernames, passwords, credit card numbers or Social Security numbers.

Trojan Horse (also known as Trojan or Backdoor Trojan)
A Trojan horse is a program that allows a hacker to make changes to a computer without the user's knowledge. Unlike a virus, a Trojan does not replicate itself. It is generally disguised as a harmless software program and distributed as an e-mail attachment. Once you open the attachment, the Trojan may install itself on your computer without your knowledge or consent. It has the ability to manage computer files, including creating, deleting, renaming, viewing, or transferring files to or from the computer. It may utilize a program manager that allows a hacker to install, execute, open, or close software programs. The hacker may have the ability to open and close your CD-ROM drive, gain control of your cursor and keyboard, and may even send spam by sending mass e-mails from your infected computer. Trojans have the ability to run in the background, hiding their presence.

Virus

A program or code that replicates, infects another program, boot sector, partition sector or document, that supports macros by inserting itself or attaching itself to that medium is a virus. Most viruses just replicate, many also do damage.

Worm

A program that replicates itself over a computer network and usually performs malicious actions such as using a computer's resources and, possibly, shutting the system down. The name is an acronym for "write once, read many." A recent example of a worm is the Sasser worm (or W32.Sasser.A and its variants) that infected millions of corporate and private computer systems. Earlier in 2004, the Netsky worm (or W32/Netsky) spread by mass e-mail using addresses obtained from an infected computer. It also spreads via local networks by trying to copy itself to shared folders on drives C: to Z:.

Zombie

A zombie machine is one that has been taken over using remote control software. Zombies are often used to send spam or to attack remote servers with an overwhelming amount of traffic (a Distributed Denial of Service Attack). A collection of many zombies comprise a botnet.

SOURCES

Government

Annual Small Business Survey
Small Business Service
UK Department of Trade and Industry
London, United Kingdom USA
November 2006
http://www.berr.gov.uk/files/file38237.pdf

Directive 95/46/EC of the European Parliament and of the Council
(The 'Data Protection Directive')
Official Journal of the European Communities
Brussels, Belgium
October 1995
http://ec.europa.eu/justice_home/fsj/privacy/law/index_en.htm

Decision and Order in the Matter of DSW, Inc.
File Number 052-3096
Federal Trade Commission
Washington, D.C. USA
March 2006
http://www.ftc.gov/os/caselist/0523096/
0523096c4157DSWDecisionandOrder.pdf

Excessive Indulgences: Personal Internet Use at the Department of Interior
Office of the Inspector General
U.S. Department of Interior
Washington, D.C. USA
September, 2006
http://www.doioig.gov/upload/FINALInternetreport1.pdf

Guidance on Mitigating Risks From Spyware
Document Number: FIL-66-2005
Federal Deposit Insurance Corporation
Washington, D.C. USA
July 2005
http://www.fdic.gov/news/news/financial/2005/fil6605.html

Internet Crime Report 2006
Internet Crime Complaint Center
Federal Bureau of Investigation
U.S. Department of Justice
Washington, D.C. USA
January 2006
http://www.ic3.gov/media/annualreports.aspx

SME Definition
European Commission
Brussels, Belgium
May 2003
http://ec.europa.eu/enterprise/enterprise_policy/
sme_definition/index_en.htm

Gramm-Leach-Bliley Act of 1999
Public Law 106-102
U.S. Congress
Washington, D.C. USA
November 1999
http://banking.senate.gov/conf/confrpt.htm

Health Care Insurance Portability and Accountability Act of 1996
Public Law 104-191
U.S. Congress
Washington, D.C. USA
August 1996
http://aspe.hhs.gov/admnsimp/pl104191.htm

New Personal Information Protection Act
Japan External Trade Organization
Tokyo, Japan
November 2005
http://www.jetro.org/content/296

SMEs, Growth and Poverty
Note Number 268
The World Bank
Washington, D.C. USA
February 2004
http://rru.worldbank.org/Documents/PublicPolicyJournal/
268-private.pdf

Small Business Research and Policy
Industry Canada
Government of Canada
Ottawa, Canada
June 2004 – April 2007
http://strategis.ic.gc.ca/epic/site/sbrp-rppe.nsf/en/Home

The Small Business Share of GDP
Office of Advocacy
U.S. Small Business Administration
Washington, D.C. USA
April 2007
www.sba.gov/advo/research/rs299tot.pdf

Small and Medium Enterprise Agency Web Site
Japanese Ministry of Economy, Trade and Industry
Tokyo, Japan
http://www.meti.go.jp/english/aboutmeti/index.html

Private Sector

NFIB and Visa partner to educate small businesses on security in 2007
National Federation of Independent Businesses
Washington, D.C. USA
March 8, 2007
http://www.nfib.com/object/IO_32561.html

2007SMB IT Budget Outlook: North America
Michael Speyer
Forrester Research, Inc.
Cambridge, Massachusetts USA
February, 2007
http://www.forrester.com/Research/Document/
Excerpt/0,7211,40826,00.html

Annual Global Threat Report
ScanSafe
San Mateo, California USA
March 2007
http://www.scansafe.com/__data/assets/pdf_file/3717/gtr_mar2007_v4.pdf

Definitions
Anti-Spyware Coalition
Washington, D.C. USA
June 2006
http://www.antispywarecoalition.org/documents/documents/ASCDefinitionsWorkingReport20060622.pdf

The Growing Web Threat
Peter Firstbrook
Gartner, Inc.
Stamford, Connecticut USA
April 2007
http://www.gartner.com/DisplayDocument?ref=g_search&id=503458

Protecting Your Network: Mitigating Spyware in Organizations
Anti-Spyware Coalition
Washington, D.C. USA
April 2006
http://www.antispywarecoalition.org/documents/documents/ProtectingYourNetworkflyerA4.pdf

SMB State of the Union study
AllBusiness.com
San Francisco, California USA
December 2005
http://www.allbusiness.com/services/business-services/3996110-1.html

Small Business Information Security Readiness
Andrea Peiro, Patrick Cook, Hassan Beydoun
Small Business Technology Institute
Santa Jose, California USA
July 2005
http://www.sbtechnologyinstitute.org/

Payment Card Industry (PCI) Data Security Standard
PCI Security Standards Council, LLC
Wakefield, Massachusetts USA
September 2006
https://www.pcisecuritystandards.org/tech/index.htm

News Stories

"77% of Small Businesses Agree Job Success Depends on Internet"
Technology Insider
Everon Technology Services
Boston, Massachusetts
November 2006
http://newsletter.everonit.com/index000149058.cfm

"Computer hackers steal Carson funds"
By Hector Becerra
Los Angeles Times
June 1, 2007
http://pqasb.pqarchiver.com/latimes/advancedsearch.html

"Unequal Pay for Equal Experience"
By Allan Alter
CIO Insight
April 7, 2007
http://www.cioinsight.com/article2/0,1540,2121441,00.asp

The Best Security
in an Unsecured World™

Webroot Software, Inc.
P.O. Box 19816
Boulder, CO 80308-2816
USA
www.webroot.com
Phone: 303.442.3813
Fax: 303.442.3846
Consumer Sales & Support: 866.612.4227
Consumer Sales & Support: www.webroot.com/support

Printed with soy-based inks on post-consumer recycled paper.