



webroot[®]
SOFTWARE, INC.

Privacy. Protection. Peace of Mind.

White Paper

Building a Business Case for Enterprise Spyware Protection

Webroot Software, Inc.

2560 55th Street, Boulder, CO 80301

Toll Free: 800.870.8102

Telephone: 303.442.3813

Facsimile: 303.442.3846

www.webroot.com

Index:

Executive Summary	1
Measurable Impacts	2
Overview: “Cost of Not Doing Business”	4
Not Big Bangs, but Big Bucks	5
ROI for the Enterprise Anti-Spyware Investment	6
The Cost/Benefit Issue	7

Executive Summary:

All spyware and other unwanted applications can jeopardize your business operations. The least noticeable harm from spyware, adware and other potentially unwanted software programs is to slow network and desktop processing by tiny increments. Even the slightest slow-down, multiplied across the enterprise, adds up to a serious bottom line impact in decreased automated processing and worker productivity. By the time those tiny increments cause a noticeable slow-down, the unwanted programs present within your enterprise will likely require considerable time and ingenuity to remove without causing additional, more costly damage to your operating systems and applications. And that's just the best case scenario.

The worst case scenario results in loss of corporate intellectual property or confidential information about employees or customers through the transmission of tracked user activities and proprietary information back to the spyware's originator and on to the purchaser of that information – advertisers, business intelligence spies, or even organized crime. Such misdirection of corporate information compromises security and confidentiality, and poses threats to corporate integrity, reputation, and regulatory compliance. Those big-bucks risks are more difficult to predict, but they must figure heavily in the calculation of the value of protection against spyware and other potentially unwanted software.

All risks, from IT processing speed to legal exposure, carry probability and cost metrics. The more predictable types of risks—technological and human resource downtime—carry more readily measurable costs to support the ROI case because these events are far more likely to occur than the catastrophe. Sound management practices applying the efficiency principle of “lean production” to improve profitability with every possible decrease to wasteful costs clearly applies to the toll spyware takes on the performance of networks and employees.

Proceeding logically from cause (installation on corporate workstations) to effect (damage, possibly eventual catastrophic system failure or intellectual property theft), it becomes clear that the more thorough a preventive solution you implement at the technological level, the more complete a defense you have against a big-ticket, high-profile security breach.

An enterprise-level anti-spyware solution provides a thorough solution that initially disinfects your enterprise and then pro-actively defends it against re-infection. A corporate strategy to protect your operations from spyware and other unwanted software will begin with the complete removal of existing spyware programs and then ensure ongoing defense against the installation of new applications beyond the often inadequate defenses at the network gateway, with centrally controlled desktop protection.

Bottom Line for Protection:

Protect your workstations and you protect your corporate reputation.

Measurable Impacts

Spyware and other unwanted programs can cause proliferating small costs that, unnoticed and unchecked, add up over time. They may eventually cause a catastrophic breach of security that you and your employees, your customers, the media, and regulatory agencies—will notice. You don't want spyware to bypass an ineffective solution, infect your company and expose you to that much risk. The recommended approach applies preventive solutions at the lowest levels of impact in order to forestall greater impacts. Building a convincing business case for acquiring, implementing and maintaining such solutions requires that you know what to measure on both the cost and benefit sides of the ROI equation.

What levels of cost can which types of spyware and potentially unwanted software generate?

Backdoors are code that allow a hacker to have access to a computer, usually with powerful interfaces that give the hacker complete control over the machine as if they were sitting in front of it. Back Orifice, SubSeven, NetBus are some famous back doors. IRC controlled backdoors are used to kick off Denial of Service (DoS) attacks against targets. See below for more information.

System monitors (or **trackware**) include keystroke loggers, which are code that record all input from the keyboard and ship it off to the hacker. This is a useful tool for gathering usernames, passwords and other account information.

There are examples of code that will also record voice and video from a computer equipped with a microphone or camera. Results from an ongoing spy audit of enterprise systems (available on the Webroot website) indicate that more than 5% of the tested systems have system monitors on them.

Spyware is an elusive, ever changing threat that falls into several categories. At its most basic, spyware programs track your online and offline activities without your knowledge and/or consent, and share that information with a third party. Spyware can come in two broad categories:

- **System Monitoring Tools** that record everything from keystrokes and visited websites to chat sessions, instant messages and e-mail messages.
- **Keyloggers**, programs that capture every keystroke performed on a keyboard, including usernames, passwords and private data like bank account or credit card numbers.

The largest emerging supply of spyware comes from commercial sources who want to feed advertising to unsuspecting users in the form of **Adware**, spyware's more benign cousin. Adware is often bundled with or embedded within freeware – utilitarian programs like file sharing applications, search utilities and information providing programs (e.g. clocks, messengers, alerts, weather, etc)— and funware like screensavers, cartoon cursors, backgrounds, sounds, etc. Adware applications are usually advertising supported software that anonymously monitors your Internet surfing activities and typically can display targeted pop-up, pop-under, and other advertisements on your computer from time to time. You, sometimes unknowingly, agree to receive these ads in exchange for free software, but adware can cause problems beyond the distracting pop-up ads.

Your goal is to demonstrate that an ounce of spyware prevention really is worth a pound of infection cure.

Malware specifically targets the most valuable corporate information assets.

Some adware may track your Web surfing habits. Deleting adware will usually result in deletion of the bundled freeware application. Adware can produce pop-up, pop-under, floating or animated ads containing scripting that can permit browser manipulation by exploiting features and flaws the operating system, the browser itself and browser helper objects (BHOs), ActiveX, and Java. The adware's information gathering and reporting activities can cause the same network latency as cookies do. Beyond that, adware can sometimes perform such undesirable functions such as installing new utilities and features on the user's computer, modifying the user system and changing browser settings in ways that tech support must later undo – usually only after the unexpected code has caused a significant system issue or transmitted confidential information.

Trojan Horses are code that masquerade as one thing, but are actually something else, usually malicious, but sometimes just a nuisance. For instance, you can download a screen saver and unwittingly install an unwanted program through the backdoor. Trojan horses can be masters of deception. In an example of very clever opportunism, hackers created a Trojan horse that masqueraded as a controversial screen saver that Lycos was distributing. The original Lycos version launched denial of service attacks against spammers. The fake screen saver installed Perfect Keylogger, a spyware application. To avoid confusion, think of Trojan horses as disguised delivery mechanism (similar to the legendary horse used by the Greeks in the Trojan War). Do not confuse them with their payload which could be any software application. There are newer types of programs that are similar to Trojans, but that rely on user carelessness (inattention in reading end user agreements or not understanding Internet downloads, rather than pure deceit. These can trick users into downloading a program with modest utility while its primary purpose is to deliver advertising or other unwanted applications.

Malware began as the umbrella term for viruses and Trojan horses, but it now includes any secretly installed code that interferes with network performance or threatens corporate information. Malware causes the same network impacts as trackware and adware, but can also open the gate to all manner of corporate information theft – whatever the spyware developer can imagine by whatever means the developer can devise. Malware specifically targets the most valuable corporate information assets. Malware has been known to activate a webcam or microphone on the user's system – literally spying on the employee. At a corporate level, malware can install and run background processes enmeshed in the user's operating system (and potentially spread to all users on the network) in such a way that removal can be as damaging as the processes themselves if not performed properly. And proper removal can itself be a costly exercise. Another type of malware, sometimes called "scumware," binds tightly to users' operating system and can disrupt company websites necessary for mission-critical functions. Other specific types of malware include **keystroke loggers** that report user entries that may include confidential information, **backdoors** that permit unauthorized entry to corporate systems and data, and **Trojans** that deliver malware code hidden in purportedly useful download the user requests. (See detailed descriptions above.)

Overview: “Cost of Not Doing Business”

Adware programs report computer user behaviors and preferences back to advertisers. Adware installs on PCs and laptops you may think are protected behind network protections, as well as those used remotely, and then—regardless of the initial point of entry— the adware sends its reports over your network back to its source. You can measure the cost of one small transmission, and the cost of millions of legitimate business transmissions is justifiable. But that same unit cost multiplied for as many, if not more, millions of instances of adware traffic is wasted money – fat, not lean, production.

At its most extreme, spyware and other potentially unwanted applications can generate a glut of suspicious network traffic sufficient for the network administrator to shut down at least part of a company’s Internet access. Malware sneaks into computers and networks surreptitiously and carries the same productivity deterioration costs, but with a greater likelihood of catastrophic exposures. Backdoors into corporate data, Trojans and keyloggers can result in theft of employees’ and customers’ credit information, identity theft, access to confidential corporate information, and other security vulnerabilities that may breach regulatory compliance. Your company’s risk manager or a consultant specializing in risk mitigation for your industry can determine the costs of such incidents.

Intentionally malicious spyware is usually invisible to the computer user (as opposed to adware’s obvious pop-ups) and can go undetected unless network traffic reports indicate suspicious volumes of activity – and it keeps working while the administrator investigates those reports. Reliance upon the network traffic sensors in firewalls and anti-virus software may not alert the network administrator in time to stop the spyware’s activities. And even if the alert is timely, the proper extrication of malware from PC or server operating systems can be time-consuming in order to be thorough and to avoid damage to the systems to which it has become bound. A better solution identifies malware before it installs itself, quarantines it, and then enables the administrator to remove it if investigation shows that it is not a legitimate application file.

The pervasiveness of spyware and the risks posed by malware and adware alike received information security industry notice throughout 2004. Publications such as Information Security Magazine and Network World and organizations like the Cyber Security Industry Alliance sounded the alarm about the hazards spyware poses to corporate networks and employee devices.

In fact, spyware has become a serious enough matter to draw the attention of the United States Congress, where several bills are progressing toward approval. H.R. 2929, the Spy Act, places technological requirements upon spyware distributors, such as obtaining permission from users through a clearly worded licensing agreement.

You can measure the cost of one small transmission, and the cost of millions of legitimate business transmissions is justifiable. But that same unit cost multiplied for as many, if not more, millions of instances of adware traffic is wasted money – fat, not lean, production.

Intentionally malicious spyware is usually invisible to the computer user

Spyware has become a serious enough matter to draw the attention of the United States Congress

Companies need to protect themselves with every technological and behavioral resource in their power.

After being downloaded, the programs would have to be easy to disable. Abusers face increased fines imposed by this bill. Two other bills take the approach of directly criminalizing malicious software's behavior. H.R. 4661, the Internet Spyware (I-Spy) Prevention Act of 2004, and S 2145 both criminalize several types of activities: intentionally impairing the security protections of a computer; accessing a computer without authorization; obtaining or transmitting personal information for the purpose of injuring or defrauding a person or of damaging a computer. Both H.R. 2929 and H.R. 4661 were approved by the House and moved to the Senate in October, 2004. The text of S 2145 had not yet been received from the Government Printing Office in mid-December, 2004.¹ The Cyber Security Industry Alliance more strongly supports the behavioral approach taken by H.R. 4661.²

Clearly, these software distributors will continue to profit as long as legitimate businesses remain unaware of their own productivity eroding because of spyware installations. And just as clearly, companies need to protect themselves with every technological and behavioral resource in their power. Executives should consider the costs of the potential damage from spyware against the investment in preventive measures such as employee education in protective policies and the technological solutions, from firewalls to anti-spyware software.

Not Big Bangs, but Big Bucks

During the past twelve months, spyware installations on corporate desktops have yielded some significant numbers over repeated surveys and audits.

Since October, 2004, Webroot has audited more than 20,000 systems operating in more than 6,200 companies, and found an average of 15 pieces of spyware and other potentially unwanted software per corporate desktop computer, including malicious spyware installations. On the PCs audited, an average of fourteen percent had system monitors and six percent had Trojan horse programs, the two most potentially malicious—and financially hazardous—types of spyware.

Other studies also demonstrate the growth of spyware on corporate computers. IT managers, 40% of whom admit they have been hit by spyware, report that spyware installations are constantly increasing.³ An independent study in 2004 found that 92% of organizations with at least 100 employees have some sort of spyware infection⁴, which is not surprising because the National Cyber Security Alliance estimated as early as June, 2003, that nine out of 10 PCs connected to the Internet had spyware. A 2004 study by Earthlink and Webroot Software reported that the average Internet connected PC contains 27.5 traces of spyware.

¹ <http://thomas.loc.gov>

² https://www.csialliance.org/news/newsletters/news/Sept04_newsletter.html

³ Source: Adam Sehovic, *Mobile News*, June 2004

⁴ Websense *Web @ Work*

Who is taking notice of these and related info-sec numbers? According to a NetContinuum independent study, senior IT executives at Fortune 1000 companies in the U.S. are concerned about the vulnerabilities of Internet downloaded applications, spyware's playground. Ninety-eight percent of the study's respondents believed that Web application attacks represent a dangerous threat, with 62% ranking the threat at "10" on a scale of 1-10. Ninety percent reported that government regulations like as Sarbanes-Oxley, Gramm-Leach-Bliley and California Senate Bill 1386 have driven the purchase of new products specifically for Web application security. Narrowing the perspective to the type of activities that spyware performs, 60% evaluated a hacker obtaining sensitive business data from an application as worse than a mission-critical application going down for an hour; 22% of respondents called the two equally bad.⁵

Ninety-eight percent of the study's respondents believed that Web application attacks represent a dangerous threat, with 62% ranking the threat at "10" on a scale of 1-10.

ROI for the Enterprise Anti-spyware Investment

In the category of productivity impact, both technical and human, you can estimate many easily calculated cost factors. These include:

- Tech support calls – cost per minute, multiplied by average number of minute for spyware-solution calls, multiplied by the number of such calls you experience
- Workstation down time for restoring the drive to a healthy state or (worst case) entirely rebuilding the machine – non-productive labor hour cost plus lost transaction cost
- IT labor hours to perform workstation system repair removing the application, which can require delicate manual extraction of code so as to avoid damage to necessary functions
- Employee training hours in tactics for avoiding unwanted applications and identifying clues to its existence in their workstations' performance
- Workstation slowdown – cost of transactions not completed, based on the actual number of transactions versus the number completed during normal operations
- Network bandwidth/resource consumption – cost of resource per transaction multiplied by the number of unwanted transactions.

In the category of corporate risk, the cost factors carry a higher per-incident cost. You will have to derive estimates of these cost factors from your industry's standards and any corporate history with such events, which your company's risk management officer can provide. Liabilities include:

- Theft of intellectual property
- Theft of credentials
- Theft of confidential personal information about employees and customers
- Fraud committed with the personal information obtained
- Corporate espionage resulting in loss of competitive advantage
- Liability through breach of privacy lawsuits or regulatory fines and censure
- Devaluation of brand reputation because of insufficient security protecting customer information – cost per defamatory incident.

IT administrators should define a security policy that is consistent throughout the organization – and be able to manage centrally the software that implements that policy

⁵ https://www.netcontinuum.com/products/whitePapers/getPDF.cfm?n=NC_WhitePaper_FortBstPractices.pdf

In order to keep your enterprise anti-spyware solution truly cost-effective, you should ensure that it offers the broadest protection, scalable to your growing needs, with the most efficient centralized control mechanism for the IT administrator.

To avoid interference with business processing, distributed update servers may be deployed so that when a client polls for an update, it can obtain the update from the available local server with the highest resource availability.

Then you run the ROI spreadsheet.

1. ANNUAL COST OF SPYWARE AND OTHER UNWANTED APPLICATIONS ON WORKSTATIONS = (Number of exposure risks – workstations, laptops) X (reported average number of spyware programs per workstation) X (number of units of resource capability spyware uses daily to run and store the information gathered X 365) X (cost/unit of resource capability)

2. ANNUAL COST OF SPYWARE AND OTHER UNWANTED APPLICATIONS ON THE NETWORK = (Number of exposure risks – workstations, laptops) X (reported average number of spyware programs per workstation) X (average number of messages each spyware program sends daily X 365) X (cost/message of network resource)

3. ANNUAL COST OF LOST LABOR PRODUCTIVITY = ((IT employee labor cost/hour) X (number of spyware and other unwanted application related help-desk calls in the last year) X (average time of help-desk call for detection and removal by end-user during the call)) + ((IT employee labor cost/hour) X (number of spyware and other unwanted application-related help-desk calls in the last year) X (average time of IT effort to remove more complicated, embedded programs off-line from reporting end-user)) + ((average end-user labor cost/hour) X (number of spyware and other unwanted application related help-desk calls in the last year) X (average time of help-desk call for detection and removal by end-user during the call)) + ((average end-user labor cost/hour) X (estimated hours of lost productivity due to system slowness before the problem is reported))

4. SINGLE INCIDENT COST ESTIMATE FOR CORPORATE RISK ELEMENTS = (estimate must be provided by in-house risk manager or industry consultant)

How your risk manager calculates the probability of the corporate risk elements depends upon the number of employees whose workstations represent an exposure and the estimated rate of spyware infection throughout your enterprise. That is a judgment call based on industry and corporate history and the best experience of your risk management team or consultant.

The Cost/Benefit Estimate

Set the total of those four calculations against the cost of owning an enterprise anti-spyware solution, which usually includes:

- Corporate license based on number of workstations protected
- Annual subscription for updates of definitions and solution enhancements
- Tech support by telephone help-desk and email or trouble-ticketing system
- Training time for IT administrators and end-user education (both of which are less than training for entirely manual management and removal).

The value of enterprise-level protection against spyware becomes readily apparent. Of course, your company should educate employees about the hazards and avoidance of spyware and other unwanted applications in any case. But your employees should also know that you have implemented a solution to support their attention to their

primary jobs with the least disruption. In order to keep your enterprise anti-spyware solution truly cost-effective, you should ensure that it offers the broadest protection, scalable to your growing needs, with the most efficient centralized control mechanism for the IT administrator.

About Webroot Spy Sweeper Enterprise

Webroot Spy Sweeper Enterprise is an award-winning corporate anti-spyware solution that provides centralized desktop-level protection against spyware, adware and other unwanted software programs. Providing the most comprehensive detection and removal of spyware available, Webroot Spy Sweeper Enterprise offers:

- Comprehensive, corporate-wide detection and elimination of spyware and adware
- Automated deployment of spyware definitions and software updates
- Options to schedule group-based and company-wide spyware sweeps
- Ability to create and enforce customized protection policies
- Customizable, detailed reports and summaries on malicious threats
- Advanced support for remote and laptop users while outside the corporate network

About Webroot Software, Inc.

Webroot Software, a privately held company based in Boulder, Colorado, creates innovative privacy, protection and performance products and services for millions of users around the world, ranging from enterprises, Internet service providers, government agencies and higher education institutions, to small businesses and individuals. The company provides a suite of high-quality, easy-to-use software that guides and empowers users as they surf the Web, protecting personal information and returning control over computing environments. Webroot's software consistently receives top ratings and recommendations by respected third-party media and product reviewers.

For more information about Webroot Software or Spy Sweeper Enterprise, please visit www.webroot.com or call 800-870-8102.

Privacy. Protection. Peace of Mind.

2560 55th Street, Boulder, CO 80301

Toll Free: 800.870.8102

Telephone: 303.442.3813

Facsimile: 303.442.3846

www.webroot.com