A Holistic Approach for Managing Spyware

Xin Luo

In the past, the main anti-malware targets for IT were viruses and worms. Yet, information privacy and security control are being increasingly challenged by the mushrooming emergence and propagation of spyware, which is one of the perilous cyber-threats confronting the IT community in terms of privacy violation. In general, most people regard spyware as a stealthy transmitter gathering and passing sensitive personal information to a third party over the Internet without awareness or permission. Stafford and Urbaczewski refer to spyware as "a ghost in the machine" [1] due to its surreptitious nature compared to viruses and worms. Warkentin et al. [2] further expand the description by arguing that "spyware is a client-side software component that monitors the use of client activity and sends the collected data to a remote machine." The rapid penetration of broadband Internet connections, coupled with a wide variety of free software downloads and weakly managed peer-to-peer (P2P) transmissions, has provided a hotbed for the pervasion of spyware. Notwithstanding, in the early development stage, spyware has the potential and specificity to surreptitiously trigger more severe calamities than viruses and worms if we don't have comprehensive management and prudent control.

The launch of vicious spyware mainly stems from the search for valuable information. As such, spyware is designed and implemented to stealthily collect and transmit information such as keystrokes for usernames and passwords, Web surfing habits, e-mail addresses, and other sensitive information. Additionally, spyware is able to trigger system resource misuse and bandwidth waste, thereby posing grave security, confidentiality, and compliance risks. Further, spyware infection, including adware, key loggers, Trojan horses, and tracking cookies [1], is a de facto worldwide phenomenon. Kingsoft, a leading anti-virus company in China, reports that spyware has become one of the top five threats to the Internet and accounts for 23 percent of the overall menaces. It is estimated that, in 2004, spyware grew rapidly, increasing to 2.5 times its 2003 level [3]. More recently, according to Webroot, more than 55 percent of corporate PCs contain unwanted spyware programs, resulting in an average of 7.2 non-cookie infections per PC.

XIN LUO(XL96@msstate.edu) is a doctoral student in Business Information Systems at Mississippi State University. His research interests center around information security, mobile communications, and global IT adoption and management. His research has appeared in Communications of the ACM, Journal of Internal Banking and Commerce, Encyclopedia of Multimedia Technology and Networking, *and international and national conference proceedings.*

SPYWARE THREATS TO BUSINESS

The spyware problem is sizable and growing. According to Dell, 12 percent of its technical support calls are spyware related. Although both home and enterprise computers currently face spyware infections, the scenario is magnified in the latter, owing to the wide scale of computer and network implementation and installation. Despite spyware infiltration in record numbers, the overall negative aftermath of spyware infection for enterprises varies from mild to wild — occasional harassment, productivity loss, resource waste, and threat to business information integrity [1,4,5]. The human factor is a main consideration when security is at issue in this scenario because the problem confronting business managers is that most spyware infections stem from unwary or novice employees browsing spyware-affiliated Web pages and downloading free software bundled with spyware programs. For example, Kazaa, a free P2P information exchange program, is bundled with several adware programs. The tradeoff, however, is always ease of use versus security, leading to the dilemma that more secure environments are generally less convenient.

Organizations such as financial institutions and insurance and health companies that must comply with government legislative regulations for information security are especially at risk if spyware penetrates the corporate computing environment. The dreadful aftermath is that confidential business information can be transmitted to outsiders, causing immeasurable loss. Even in computing environments that encrypt data, spyware remains a threat to the security of corporate data because its keystroke-logging components capture input before it can be encrypted. In addition to data theft, hacking, zombie attack, and network damage are also of great danger to business organizations. Despite the technological endeavors made toward the mitigation of spyware pervasion [6], the infection rate keeps skyrocketing per se. For this serious scenario magnified in the business domain, a mere technical effort, such as relying on anti-spyware software, cannot radically and sufficiently thwart the rapid spyware penetration. The most recent spyware research only shed light on spyware identification and elimination in the arena of information security defense [1,5–9], leaving managerial efforts relatively unnoticed. The limited spectrum of research agenda therefore needs to be further broadened and proactively revamped. A more comprehensive and effective method for spyware management and control, including deterrence, identification or detection, prevention, and elimination or correction, is urgently needed.

The overall negative aftermath of spyware infection for enterprises varies from mild to wild.

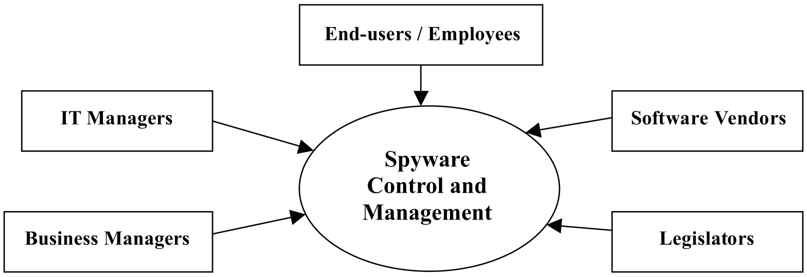
PROPOSED FRAMEWORK

The contribution of this article is that, in an effort to align both technical and managerial endeavors, a comprehensive framework for spyware management and control is proposed. Five different groups (see Figure 1), including end users or employees, IT managers, business managers, software vendors, and government legislators, are identified. Recommendations are provided for each of these five unique yet interdependent groups. This framework could arm the IT community with instrumental ordinance to more efficiently and effectively fire back, as spyware continues to become a mainstream global computing issue.

SPYWARE CONTROL AND MANAGEMENT

The core of this proposed framework is spyware control and management for businesses. Because more businesses depend on IT to enhance business operation efficiency, sustain competitive advantage, and survive in the keenly competitive market, information security and assurance is inevitably an important issue relating to business performance and success. According to IDC, spyware is currently the fourth greatest threat to companies' network security. It is estimated that approximately 88 percent of all computers are infected with some form of spyware. To comply with the emerging laws regarding information collection, such as the Health Insurance Portability and

FIGURE 1 Proposed Framework for Spyware Control and Management



Accountability Act (HIPAA) ensuring the privacy of patient information, Sarbanes–Oxley Act ensuring that financial statements are resistant to fraud, Gramm–Leach–Bliley Act safeguarding customer information, and the California Data Privacy Law (California SB 1386) protecting the confidential information of state residents, businesses should more cautiously and proactively control and manage their computing resources to thwart spyware penetrations.

Spyware control and management is not merely a technical issue to be easily handled. Instead, businesses should look beyond the technical spectrum for more efficient methods of spyware mitigation and elimination. Although some businesses have not yet ranked spyware as a serious cyber-threat, those companies will have to prioritize spyware remedies when they have experienced and fully perceived the information security impact and menace, such as loss of critical business data and even system failure, triggered by the surreptitious specificity of spyware.

Currently, there is no panacea to deter and eradicate the spyware threat because spyware becomes increasingly challenging to define and classify and there is no mutually agreed standard for spyware in the IT industry [2,8]. Different parties perceive spyware in a diverse manner — some regard spyware as an absolutely evil tool for malicious hackers to remotely steal sensitive information without the knowledge of the user, whereas others show less concern or even perceive convenience. For instance, user-tracking cookies frequently have been grouped with spyware, although cookies themselves are not applications for malicious use. Instead, they are researchware designed for Internet marketing purposes. Also, supportware, such as remote-access programs, can be used by IT administrators to monitor and control network systems.

Given the serious scenario in the business domain, asking IT people for one-click removal of spyware from machines is not effective enough for spyware deterrence, identification or detection, prevention, and elimination or correction in business organizations. Instead, this is a challenging business strategic problem consisting of internal and external support. It requires seamless cooperative effort and communication among five groups including end users or employees, IT managers, business managers, software vendors, and legislators.

End Users or Employees

Users are typically exposed to spyware as a result of their behavior [10]. The growing number of companies that value IT as their necessary strategic weapon and the increasing amount of time employees spend on the Internet performing job tasks have served to amplify users' exposure to spyware. The prevalence of spyware has been motivated by the ease of installation with default settings, its low cost, and its intrinsic rewards (bundled with freeware) that often target users who lack appropriate guidance and awareness. Spyware penetrates into an enterprise mainly through unwitting employees' computing behavior, such as downloading interesting or fun programs from the Internet, installing freeware bundled with a wide variety of unknown programs and files, and browsing Web sites embedded with malicious code.

Spyware can also circumvent perimeter firewalls through P2P instant messaging, streaming multimedia, and other routes that employees use. When residing in the system, spyware opens a direct data pipeline to the outside world without the user's knowledge. Outside the firewall, rapidly increasing numbers of mobile and at-home workers are picking up spyware downloads from various sources and then introducing them to the enterprise when logging in to the company network portal.

Therefore, a series of recommendations are provided for corporate users, as follows:

□ Users should first carefully study and thoroughly understand the company's information security and privacy policy to ensure their computing activities are in compliance with organizational requirements.

□ An automated report system (via either internal e-mail messages or enterprise instant messaging) should be implemented to regularly make users aware of the system patches or updates to protect their computers. In turn, users should carefully follow the instructions of the report.

□ Users should pay closer attention when interacting with the Internet and should more properly and responsibly manage their computing resources by uninstalling unnecessary programs and ignoring and blocking pop-up messages. They must have control over what programs are installed on their computers and set security settings on their computers acceptably high to avoid "drive-by downloads," through which spyware can penetrate when users visit a certain Web site or view an HTML e-mail message.

□ To safeguard their computing resources, users should install anti-spyware programs under the guidance of IT professionals, update the program definitions, and scan their machines regularly.

□ Users must more carefully read the end user licensing agreement (EULA) before installing any unknown software and should report to IT managers if they feel the EULA information is misleading.

□ Users should never accept downloads from unknown Web sites or pop-up windows and should avoid using P2P programs. As with the anti-virus countermeasure, users should not bring in and run unknown CDs or USB drives without the IT administrator's permission and guidance.

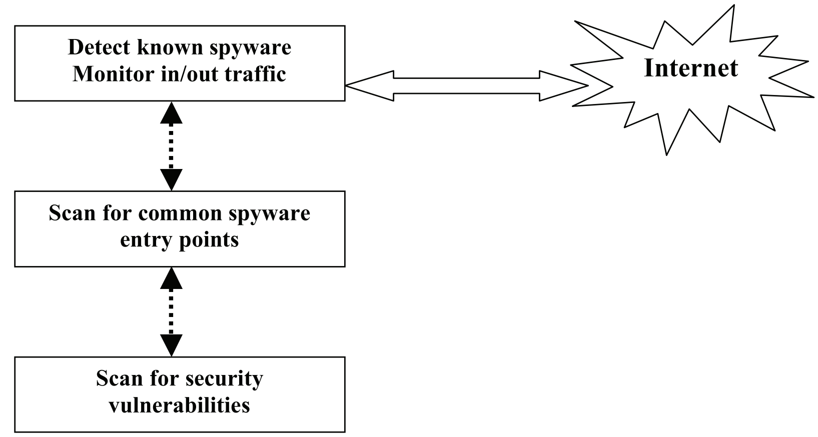
When residing in the system, spyware opens a direct data pipeline to the outside world without the user's knowledge.

IT Managers and Business Managers

At the organizational management level, IT managers and business managers should perceive spyware as a serious cyber-threat even if their business hasn't experienced severe aftermaths. Further, they should regard spyware threat as a business strategic issue because spyware impacts business productivity and efficiency. They cannot merely rely on employee vigilance as a defense against spyware. Spyware-related vulnerabilities and risks are enterprisewide, thereby calling for comprehensive treatment. As a part of a security strategy, with mutual agreement, IT and business managers should first institute an information security and privacy policy to regulate and minimize the occurrence of spyware corruption triggered by unwitting employees. Moreover, they should provide security training to cultivate spyware awareness and educate employees about how spyware penetrates, to make them realize that careless downloading and Web surfing could lead to enterprisewide spyware infestation.

As IT managers, they should authoritatively enforce the security policies to prohibit P2P file sharing and downloading freeware throughout the entire IT structure. Further, the key to thwarting enterprisewide spyware infestation is to centralize IT structure by

FIGURE 2 Multi-Layer Anti-Spyware Defense


Detect known spyware
Monitor in/out traffic
Internet
Scan for common spyware entry points
Scan for security vulnerabilities

deploying an effective multi-layer anti-spyware solution that can be managed by IT professionals with no action required by employees. The anti-spyware solution consists of three main layers (see Figure 2). The first layer serves to block all unnecessary ports and known spyware sources and destinations on firewalls or IDSs (intrusion detection systems) and IPSs (intrusion prevention systems) and to carefully monitor incoming and outbound traffic by means of a variety of anti-spyware programs along with existing anti-virus applications. The majority of known spyware can be screened and filtered via this defense. The second layer proactively scans for common spyware entry points, such as the system registry of the operating system. Thus, the new spyware variants can be identified before sneaking into systems. The third layer provides for frequent identification and analysis of the possible security vulnerabilities and promptly fixes them.

Based on the multi-layer anti-spyware solution, a centralized spyware management console concentrates the responsibility, maintenance, and troubleshooting, making it easy for the inexperienced to utilize computing. Centralized management provides the levels of accountability and functionality reporting to meet business continuity and protection goals and to prove regulatory compliance of mandated security measures required by security strategies as well as legislation. Additionally, IT managers should consider other technical alternatives in terms of operating systems and Web browsers, such as Linux and Firefox, which are less vulnerable than Microsoft Windows and Internet Explorer, respectively.

Although IT managers are mainly responsible for technical solutions for spyware, business managers should provide strong support for IT managers to implement and enforce security strategies and policies. This requires business managers to regularly communicate with IT managers via an IT–business alignment scheme, which must have the ability to respond to a dynamic network and business environment. As organizations grow, deployment or redeployment must be rapid for optimized protection at all times via this alignment approach.

Software Vendors

Unlike in the anti-virus market, current spyware definition is vague and there is no established industry standard because different anti-spyware vendors have different views for classifying software as insidious spyware or useful researchware or supportware. The dissonance amid software vendors makes spyware identification and eradication almost impossible to implement. It is recommended that, with government's strong support and permission as well as organizations' cooperation, anti-spyware vendors could be more cooperative by communicating with each other to share spyware information, such as the new definition and countermeasure methods, and designing commonly acknowledged treatments instead of launching an arms race of spyware signature identification. With such a cooperative effort, a mutually acknowledged spyware signature depository, where spyware can be classified with relevant definitions, could be established and maintained by these vendors with one voice.

The recommended spyware taxonomy would be able to articulate the various specificity of spyware, ranging from malice to mildness to usefulness, and publicize spyware findings to inject awareness for businesses. In addition, if provided communication channels, businesses could report new signatures by submitting suspicious spyware-infected files to the databases for software vendors to further analyze and create counterattack methods together.

This recommendation could alleviate dissent among vendors and minimize false-positive spyware alerts, which create unneeded stress and extra network traffic for IT managers as well as end users. Many spyware protection databases are loaded with harmless signatures that get in the way of productive protection and management. Also, definitions need to be specific enough to catch frequent revisions of spyware routines.

Many spyware protection databases are loaded with harmless signatures that get in the way of productive protection and management.

Legislators

The current difficulty of defining spyware makes it hard to draft legislative actions that could directly address and remedy the problems. Even though the U.S. government has recently paid attention to the effects and legitimacy of spyware, the insidious specificity of spyware has not yet caused widespread public outcry because most users are unaware that their systems have been compromised [10]. Although a series of emerging pieces of U.S. federal legislation, such as the Internet Spyware (I-SPY) Prevention Act of 2004, the Software Principles Yielding Better Levels of Consumer Knowledge (SPYBLOCK) Act, and the Piracy Deterrence and Education Act of 2004, are under consideration and several states have already signed into law the anti-spyware legislation, ultimately all legislative actions will strictly address the issue of privacy and self-regulation. For software installation, for instance, users will be presented with articulate notification before downloads or data collection and with direction for ease of install or removal of unwanted programs.

Warkentin et al. [2] argue that some actions are more consumer oriented and some are oriented toward the technology industry, which fears legislation could outlaw certain existing practices. Creation of legislation is a slow process that could prohibit legitimate software practices and stifle technical innovation such as researchware and supportware. Consequently, legislators should make concerted efforts with software vendors and enterprises to carefully balance the beneficial use of spyware as a legitimate marketing or administrative tool and the insidious programs targeting sensitive business information. As mentioned above, legislators should provide strong support for spyware taxonomy among software vendors to alleviate the problem of misleading spyware information. As technical progresses outrun the legislative endeavors, it is important that legislators need to be consistently aware of the extensive specificity of spyware because people often merely perceive the literal meaning of spyware and thereby incorrectly make judgments.

CONCLUSION

There is no panacea for spyware control and management which is now becoming a serious business strategic issue. Vicious spyware has the ability to compromise the crucial information of enterprises by turning desktops into zombies to the outsider world. Inside the enterprise, spyware has a significant impact on employee and IT productivity because it can degrade desktop system performance and halt a network with unwanted traffic. The proposed comprehensive framework has identified five key groups involved in spyware management and control and respective recommendations are provided. Efficient and effective spyware management and control requires all these groups to make concerted efforts to cautiously cope with spyware.

ACKNOWLEDGEMENT

A number of people have generously given valuable time and effort towards this article. The author appreciates Dr. Kirk Arnett, Dr. Merrill Warkentin and Dr. Gary F. Templeton, Professors of Management Information Systems at Mississippi State University, for their research directions and suggestions. Also, the author thanks Dr. Ray Vaughn, Professor of Computer Science, for the support of CCSR. ■

References

[1] T. F. Stafford and A. Urbaczewski, "Spyware: The Ghost in the Machine," *Communications of the AIS*, vol. 14, pp. 291–306, 2004.

[2] M. E. Warkentin, X. Luo, and G. F. Templeton, "A Framework for Spyware Assessment," *Communications of the ACM*, vol. 48, 2005.

[3] Kingsoft, "The Report of Internet-based Danger," 2004.

[4] G. Goth, "Spyware: Menace, Nuisance, or Both?" *IEEE Security & Privacy*, vol. 1, pp. 10–11, 2003.

[5] A. M. Hormozi, "Cookies and Privacy," *Information Systems Security*, vol. 13, pp. 51–60, 2005.

[6] S. S. M. Chow, L. C. K. Hui, S. M. Yiu, K. P. Chow, and R. W. C. Lu, "A Generic Anti-spyware Solution By Access Control List at Kernel Level," *Journal of Systems and Software*, vol. 75, pp. 227–234, 2005.

[7] W. Ames, "Understanding Spyware: Risk and Response," *IEEE Computer Society: IT Pro*, vol. 6, pp. 25–29, 2004.

[8] P. J. Bruening and M. Steffen, "Spyware: Technologies, Issues, and Policy Proposals," *Journal of Internet Law*, vol. 7, pp. 3–8, 2004.

[9] G. Lawton, "Invasive Software: Who's Inside Your Computer," *IEEE Computer*, vol. 35, pp. 15–18, 2002.

[10] S. Saroiu, S. D. Gribble, and H. M. Levy, "Measurement and Analysis of Spyware in a University Environment," presented at 1st Symposium on Operating Systems Design and Implementation (NSDI), San Francisco, California, USA, 2004.