



Electronic Security: Protecting Your Resources

This document describes some of the threats your organization faces when it provides Internet access to its members. It includes information on the types of threats, and how WebSpy software can be used to protect your organization.

The Security Problem

Everyone has heard stories of computer security problems within various organizations, with consequences ranging from loss of corporate secrets to significant financial loss. Unfortunately, many organizations still feel that running anti-virus software and implementing password-controlled network security secures their electronic resources from malicious attackers. The reality of modern Information Technology is that achieving impenetrable electronic security is virtually impossible. No one can afford to regard electronic threat as a simple problem with a simple solution.

Organizations may believe they are too small, and do not have any thing of interest or of value to an attacker. The fact is that all organizations have something of interest, such as hard disk space, bandwidth and processing power. The increased use of IP address scanning tools, denial of service tools and IIS worms implies that electronic security is an issue every organization should be concerned with.

There are three main areas of electronic threat:

- **Unauthorized External Access**
Any organization connected to the Internet is subject to this threat. Implementing network security measures help to reduce this threat, however determined individuals can usually find a way to get through these security measures. Financial details, intellectual property, trade secrets, and confidential information are the main targets of this type of threat.
- **Unauthorized Internal Activities**
Trusted users of a network may either maliciously or unintentionally disclose valuable or confidential information to a third party. This security threat can often go unnoticed as the user is operating within their assigned level of security.
- **Malware**
Software designed to infiltrate or damage a computer system, such as viruses, worms, trojans, spyware, backdoors, rootkits and some adware, can infect your organization when connected to an external network such as the Internet. The risk is intensified through irresponsible or unaware staff.

The possible consequences of these threats include:

- Diminished competitiveness due to the loss of crucial corporate information
- Financial loss due to the theft of proprietary information and through fraudulent activity
- Loss of time and resources when dealing with security breaches
- Lost productivity and wasted investment
- Legal proceedings resulting from the exposure of confidential information
- Negative publicity

These consequences can have severe impacts. All organizations must ensure their electronic resources are secure.

A Growing Concern

Organizations around the world are recognizing their vulnerability. The 2007 Computer Security Institute Survey highlighted the growing problem:

- 46% of respondents detected computer security breaches within the past 12 months, with 26% having more than 10 incidents occur
- The average annual loss reported was over \$350,000

This survey also identified the two largest threats as internal:

- 59% detected employee abuse of Internet access privileges (for example, downloading pornography or pirated software, or inappropriate use of e-mail systems)
- 52% detected computer viruses

Other areas of concern include:

- 18% of respondents reported a 'targeted attack' – a malware attack aimed exclusively at their organization
- Financial fraud was the source of greatest financial lost with an overall cost of over \$20,000,000
- 29% of organizations reported computer intrusions to law enforcement agencies

Electronic Security Approaches

There are two main approaches to security: *active* or *passive*. An *active* approach to security covers all actions designed to prevent a breach of your system's security model. A *passive* approach refers to the actions taken to monitor the security of your system based on that security model.

All users should employ both active and passive approaches to security. Each of these approaches strengthens the other. Using monitoring products such as those developed by WebSpy Ltd. may provide you with information from server logs about a particular user abusing the organizations electronic resources (passive approach to security). This information may lead you to install an application that prevents or discourages them using the network in this way (active approach to security).

How do you determine your risk?

Every organization has different needs and priorities. So how do organizations determine the level of security they need? Organizations can employ a number of approaches to assess the level of security they need.

- **Qualitative risk assessment**
Many techniques have been developed attempting to qualitatively assess the risk of electronic threat, such as multiplying a risk threat frequency by a loss amount and comparing the result with the value of the protected asset. The main problem with this method is that the figures used in calculations are often highly subjective and inaccurate. Monitoring products such as those developed by WebSpy Ltd. help organizations assess how their systems are being used, in order to increase the accuracy of data used in risk assessment calculations.

- **Best practices**
Commonly accepted baselines for security protection are often employed by organizations to avoid the uncertainty of conducting a formal risk analysis. This approach offers better protection from liability lawsuits, however unique security threats may be overlooked unless the organization conducts a comprehensive analysis of their situation. The International Standards Organization (ISO) has developed security standards (namely the ISO17799 standard) that organizations can adopt to secure their systems from malicious attack. Another organization that develops common guidelines on all areas of security is GASSP (Generally Accepted System Security Principles).
- **Scenario analysis approaches**
The scenario analysis approach involves the creation of various scenarios in which computer security can be compromised. An appropriate mitigation procedure is then developed in attempt to prevent the security threat from occurring. The main disadvantage with this approach is the vast number of scenarios that exist. It is virtually impossible to attend to them all, therefore only threats that pose a significant risk to the organization are addressed.
- **Cost-benefits analysis**
Cost benefit analysis attempts to base the choice of security safeguards on the cost of the protected asset. For some organizations, the loss of information may not have a large financial cost. The benefits of implementing an expensive system security solution will not justify the cost in such situations.
- **Insuring all risks**
For organizations that cannot afford to design an electronic security solution, simply insuring all assets against risk may be a more viable solution. When this approach is taken, electronic security procedures often need to be assessed by an insurance company.

A combination of any of the above methods is often the best approach as it results in a more comprehensive analysis, and the implementation of a more effective security solution.

The WebSpy Approach

When determining your security requirements, no approach will be successful unless you have a clear understanding of how your electronic resources are used. Monitoring your Internet and network usage over a period of time provides you with information required to make important decisions regarding your organizations electronic security.

In an environment of evolving threats, it is important for an organization to have the ability to identify and adapt to new threats quickly. The capture and analysis of electronic resource usage at any point in time enables organizations to quickly respond to new threats. This flexibility is not available when using a purely predictive approach.

Monitoring does not prevent the users of a network from accessing certain content. This means that the benefits of online research tools are not affected.

In addition, monitoring also helps prevent one of the three main electronic threats: unauthorized internal activities. When an organization's members know they are being monitored, they are less likely to use electronic resources in a way that is against the organizations acceptable use policy.



WebSpy Ltd. develops an integrated suite of products designed to monitor Internet and network usage in both small and large organizations. The software is highly configurable, powerful and yet easy to use. The WebSpy suite of products can therefore satisfy the needs of system and network administrators as well as non-technical managers.

- **WebSpy Live**
[WebSpy Live](#) monitors network traffic in real time. Using this tool, managers are alerted to events such as users spending too much time on the web or viewing unacceptable content. These alerts are based on customizable profiles that can be created to suit your organization. Live enables managers to take immediate action when and where problems occur.
- **WebSpy Analyzer**
[WebSpy Analyzer](#) is a powerful reporting package that uses server or firewall log files to analyze web and email activities. You can create comprehensive reports on email and Internet usage, and export these reports to a variety of commonly used formats. Analyzer incorporates a 'drill down' facility allowing in-depth interrogation of data using customizable profiles.
- **WebSpy Vantage**
[WebSpy Vantage](#) is an award-winning software product that provides you with a common reporting window into all the key functions of your network and its usage within your organization. The comprehensive information provided by Vantage can assist in identifying and resolving network problems, reducing security vulnerabilities, as well as maximizing employee productivity by encouraging responsible usage of system resources.

WebSpy Vantage Giga also comes with an additional Web Module that enables administrators to securely distribute reports and information throughout an organization. Employees can log into the Web Module to view their reports, and conduct ad-hoc drilldowns into their storages, providing up to date information whenever they need it. Access to information is controlled through customizable permission levels, ensuring employee and company privacy.

Internet and network monitoring is a cost effective method of combating unauthorized internal activities. WebSpy products provide managers with relevant timely information to assist educated decision-making relating to the security of electronic resources.

Resources

There are many useful resources on the web to help you find out about electronic security. However, it is always good practice to verify any information you find.

WebSpy Resources

WebSpy Ltd. website
<http://www.webspy.com>

Live, Analyzer and Vantage Downloads
<http://www.webspy.com.au/download/index.aspx>

Organizations and Interest groups

International Standards Organization

<http://www.iso.org>

Computer Security Institute

<http://www.gocsi.com/>

Generally Accepted System Security Principles (GASSP)

<http://web.mit.edu/security/www/gassp1.html>

Useful Information

Approaches to choosing the strength of your security measures

http://www.linuxsecurity.com/feature_stories/feature_story-98.html

ISS' Top Ten Vulnerabilities

<https://gtoc.iss.net/topten.php>

Big-picture approaches to security - Network World Fusion

<http://www.nwfusion.com/newsletters/wireless/2002/01162807.html>

ISO17799 News - Issue 2

<http://www.iso17799-web.com>

All Rights Reserved. No part of this document may be photocopied, reproduced, stored in a retrieval system, or transmitted, in any form or by any means whether, electronic, mechanical, or otherwise without the prior written permission of WebSpy Ltd.

No warranty of accuracy is given concerning the contents of the information contained in this publication. To the extent permitted by law no liability (including liability to any person by reason of negligence) will be accepted by WebSpy Ltd, its subsidiaries or employees for any direct or indirect loss or damage caused by omissions from or inaccuracies in this document.

WebSpy Ltd. reserves the right to change details in this publication without notice.

Other product and company names herein may be the trademarks of their respective owners.



Contact WebSpy Ltd

If you would like more information on managing event logs or any of the products mentioned, please contact your nearest WebSpy Office:

WebSpy North America (Servicing North and South America)

Legacy Southcenter Place
16400 Southcenter Parkway, Suite 201
Seattle, Washington 98188
[Find us on Google Maps](#)

Toll free: 888-862-4403
Phone: +1 206-575-7763
Fax: +1 206-575-7809
Email: sales@webspy.com

WebSpy Europe (Servicing Europe, Middle East and Africa)

3rd Floor, Unit 19
Angel Gate
326 City Road
London, EC1V 2PT
[Find us on Google Maps](#)

Phone: +44 (0) 207 239 7500
Fax: +44 (0) 207 239 7539
Email: europesales@webspy.com

WebSpy Australia (Servicing Australia, Asia and the Pacific)

Level 3 Mercury House
33 Richardson Street
West Perth, Western Australia 6005
[Find us on Google Maps](#)

Toll Free: 1800 801 121
Phone: +61 8 9321 3322
Fax: +61 8 9321 3377
Email: sales@webspy.com.au

Alternatively contact WebSpy support on our [support page](#).