Information Security: Data Loss Prevention

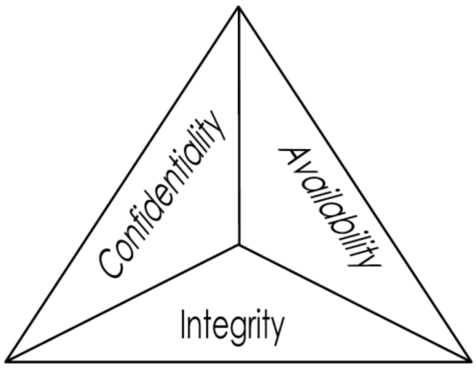
This document examines the possible threat and effect of data loss. It includes methods designed to prevent data loss and enhance system security and how WebSpy software can be used to prevent data loss and protect your organization.

Information Security

Most confidential, important or sensitive information is created, updated and stored using a networked computer system. The security of this information is a critical issue, as loss of data could result in severe financial, ethical or legal repercussions. Ensuring the security of information without sacrificing the usability of a system is a challenging dilemma faced by most organizations.

The protection of data and information systems is known as Information Security, which is based on the core principals of confidentiality, integrity and availability (collectively known as the CIA triad).

- Confidentiality
  Maintaining individual and corporate privacy requires preventing unauthorized disclosure.
- Integrity
  Modifying or updating information needs to be consistent and ensure reliability.
- Availability
  Information, including necessary system applications and any related security controls, should always be available to any authorized user.



Model of CIA Triad

Other principals to consider are:

- Possession and Control
  The ability to access data should be restricted to those who are authorized. Users should also be responsible for the security of the data they can access.
- Authenticity
  Incorrect representation or attribution of information decreases the value of the data.
- Utility
  Information should always be provided in a suitable format. This includes the storage format as well as the appearance.

These principals can be violated either unintentionally or intentionally by internal members of an organization or by external others. One of the main outcomes of information security is the prevention of data loss.

Data Loss

When information security is considered as part of risk management, one issue commonly identified is data loss. Many organizations focus on the possible threat of data theft or the vulnerability in unsecure information access. However, data theft and unauthorized access are only two examples from the four subcategories of data loss. To properly assess and reduce data loss risks for a specific organization, all four categories need to be considered.

Types of Data Loss

There are four major subcategories or types of data loss which need to be considered when developing a method for preventing data loss:

- User Access and Actions
  E.g. accidental, or deliberate, deletion of a file or program, misplaced data storage devices, and other events arising from lack of knowledge or experience. Modification of data, misuse of programs or storage formats, sharing passwords or any other form of security decreasing activity.

- Failure
  E.g. software crashes, power failures, database connection loss, data corruption or any form of error that affects volatile storage.

- Crime / Loss of Confidentiality
  E.g. unauthorized data sharing, data theft, hacking, sabotage or malicious software such as viruses, worms and Trojans.

- Disaster
  E.g. fire, flood, earthquakes or any physical event that may destroy the data storage device.

Although there is no foolproof method for perfect system security, proper precautions can greatly reduce the impact and frequency of data loss events.

Prevention of Data Loss

Data breeches are of significant concern due to the increase in frequency and severity of data loss and the corresponding cost. Many organizations are now legally required to provide a level of security as well as a means of accountability. Although protecting valuable information is core to any business, finding a solution to information security that is customized to an organization needs can be a challenging problem.

Due to the large variety of data loss causes, a huge variety of ways exist to help prevent data loss. Unfortunately, each method has its own limitations and sometimes undesirable side-effects. The best solution often involves a mixture of preventative techniques.

Anti-virus Software and Firewalls

The use of anti-virus software and firewalls can help protect a system from hacking and malware. Limiting methods of external infiltration will reduce the chance of data being stolen or corrupted. Some products also produce log files that can be used to trace information about possible attacks.

Data Backup

Regular backups or archives of information ensure that data can be restored if lost. It is also advisable to keep a copy of important information off-site in the case of a disaster. While this method can protect against some forms of data loss it is still important to consider security issues when keeping copies of information; backups may be an easier target for data theft if not stored appropriately.

Encryption and physical security are two methods which can be applied to backup data to improve security.

Encryption

Encryption has long been recognized as an effective method to help protect the confidentiality of information. Enciphering data is a method that protects the actual data, without relying on access security measures. Encryption can help reduce the effect of data theft, as enciphered data, without access to a method of deciphering, is effectively useless.

Log Files

Many devices are capable of producing information about system activity. This information can be recorded in the form of a log file. Log files can provide very detailed information which can be used to detect and help prevent data loss. Many systems can be configured to produce more information in log files than what is available with default settings. The Windows operating system is capable of monitoring user authentication attempts, tracking file access and modification and many other events which can all be recorded in log files. Although this information is a powerful tool in preventing and tracking data loss, it can be difficult to analyze or interpret. Log file analysis software should be used to ensure that information is being interpreted and used correctly.

Note: For information about using Microsoft Windows Event Logs with WebSpy Vantage, please read our Managing Event Logs white paper.

Monitoring Software

Monitoring software allows organizations to supervise users and detect possible threats to system security. This has a variety of benefits over using a purely predictive approach or reducing system usability. Monitoring does not prevent the users of a network from accessing certain content or block system features. Users that are aware of monitoring software are less likely to intentionally destroy or tamper with data. Any data loss that does occur can be detected, allowing immediate ramification measures to be deployed, minimizing damage. The ability to capture and analyze electronic resource usage, at any point in time, enables organizations to quickly respond to new threats. This flexibility and adaptability is essential in an environment of evolving threats.

Physical Security

Providing a secure environment for a computer system is essential to prevent theft of the entire system, inclusive of data. Warning signs, barrier walls, locks, alarms, surveillance cameras and guards are all methods of deterring theft in general. Methods specific to computers include many types of locks, such as cable locks, case locks and USB port locks, and storing external devices, such as removable HDD and laptops, in hidden places or safes. Another method of physical security, growing in popularity, is biometric authorization. Some laptops require fingerprint scans, and many locks can be used with inbuilt biometric security features.

Restricting Access

There are many methods of restricting user access of information. The predominant method is the use of individual or group permissions that can be configured to limit access or other properties. Appropriate levels of access help prevent data loss as well as provide security and confidentiality of information.

Providing required access to information while limiting the risk of internal data theft, is a more challenging problem. Most solutions involve removing system functionality, such as changing BIOS settings to disable write access to external media, removing screen capture abilities, and blocking internet, email or FTP sites. Implementing selective constraints on system abilities requires very intelligent algorithms as well as exhaustive testing; software has not reached a level that is able to completely satisfy security requirements by selectively preventing access.

A viable alternative to attempting to block each individual threat is using monitoring software in conjunction with detailed log files and appropriate log file analysis software.

WebSpy Software

Developing a complete solution for information security that includes data loss prevention and fits perfectly with your organization, without restricting system use is a very large project that may take a significant amount of time and resources. Detailed examination of hundreds of solutions, considering both advantages and disadvantages, implementing a variety of options, solving interoperability issues and finally using and managing the complex array of products can quickly become a logistical and financial nightmare for any manager or system administration team.

WebSpy software has been developed to remove the challenges from tracking your system, users and information. It is suitable for monitoring and reporting on a large range of system security details and fully customizable to any organization. The software is highly configurable, powerful and yet easy to use. WebSpy products can therefore satisfy the needs of system and network administrators as well as non-technical managers.

WebSpy's 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 Ultimate incorporates a Web Module, secure internal website, 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.

Vantage and Data Loss Prevention

Vantage provides organizations with a large number of business benefits. The comprehensive information provided by Vantage can assist in identifying Internet and email misuse, identifying and resolving network problems, identifying download issues, preserving bandwidth and minimizing litigation risks. Vantage allows organizations to prevent and detect three of the four types of data loss previously identified:

User Access and Actions

System auditing helps protect system resources and information by recording access attempts and other related information. Real-time indications of network incidents and an audit trail of user activity can be assessed using Event Logs (a record of the information generated from systems auditing). However extracting useful information from Event Logs can be challenging as it is very difficult to manage and filter the vast amount of data generated. Effective analysis of user access requires reliable and powerful collecting, reporting and analyzing of Event Logs. Without strong Event Log management, systems are vulnerable to user access data loss.

WebSpy Vantage provides support for all three essential activities:

- Collecting
  Log Files are stored in an optimized database called a storage, allowing fast data access with complete reliability.

- Reporting
  Reports collate information from a storage and display useful information that is easy to understand. There are many templates available and reports can be saved in a variety of file formats or emailed.

- Analyzing
  Running an analysis creates a summary based on the data in a storage. A summary can be interactively browsed and filtered to any level.

Vantage also provides filtering and aliasing (to enhance readability of data) of log data, guaranteeing the extraction of meaningful information.

Note: For more information please read our Managing Event Logs white paper.

Failure

System failures, such as software crashes or database connection loss, can be traced and examined by analyzing the information contained in System Logs. Regularly auditing System log data allows potential incidents to be reported as they occur and can also assist in preventing future occurrences.

System Logs are an important tool in network monitoring; however managing System log data can be very challenging. System Logs generate a large amount of data, which makes manual extraction or filtering of data very difficult. Additionally, ensuring data integrity requires the collected information to be entire and reliable, which can only be achieved with an appropriate method of storage and sensible representation of extracted information.

Importing System Logs into Vantage creates a reliable storage to contain your log data, allowing effective reporting and analyzing of information pertaining to system failures.

Crime / Loss of Confidentiality
With support for more than 200 log formats, Vantage can be used to monitor anti-virus software, Internet usage, email and instant messaging activity and network devices, including firewalls, VPNs, gateways and proxy servers.

Access to this information empowers organizations to identify and investigate security breaches, minimizing data crime and protecting company privacy. With an intuitive, easy-to-use interface for extracting meaningful information, Vantage provides organizations with the ability to prevent data loss and ensure information confidentiality.

Additional Benefits

Vantage also provides a wide range of other monitoring benefits, including:

Security Device Monitoring

- **Strengthen Security Controls**
  Verify the configuration of a network's firewall and its control of network traffic. Identify and investigate security breaches, determine the source of email viruses and manage their organizational impact.

- **Maximize Effectiveness of Existing Blocking and Filtering Solution**
  Review websites that employees have been denied and granted access to in order to validate the effectiveness of existing Internet filtering service.

Network Device Monitoring

- **Improve Network Management**
  Enhance management of network resources and diagnose network problems, assess bandwidth usage, examine logon activity and unauthorized file access.

Email and Messaging Monitoring

- **Protect Confidential Information**
  Monitor email and instant messaging activity to protect the transmission of confidential organizational information.

- **Maximize Email Virus Protection**
  Analyze log files from email virus scanning software, or devices, to identify source of viruses. Identify who sent the virus, who received it, attachment name and how virus scanner dealt with it.

Additional Information

Information Security - Wikipedia
Security News - TechTarget
Computer Security – JM University
Information Technology Security - Tippit
Parkerian Hexad - TechEncylopedia
CIA Triad – University of Miami
The High Cost of Data Loss - InformationWeek
Security Guide - F-Secure
Firewalls – Joseph Barbish
How Firewalls Work – Jeff Tyson
Backup - Wikipedia
The Best Ways to Backup – Les Shu
What is Cryptology? - TechFAQ
Log Files - Webopedia
10 Critical Physical Security Measures - ZDnet
USB Lockdown – Alexandru Pancescu
Security Guide for Windows – PC Tools
Security Guide for Macintosh – Secure Mac
Linux Security – Guardian Digital

WebSpy

For more information about WebSpy please visit http://www.webspy.com

If you would like information about using Vantage with Microsoft Windows Event Logs, please read our Managing Event Logs white paper.

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
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
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, 9 Colin Street West Perth, Western Australia 6005
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