Internal Cyber Threat Prevention

Mitigating the Risk of Data Loss and Corruption

Abstract

Insiders pose the greatest threat of data loss or corruption to the institutions for which they work or worked. Statistics show that the cost of lost data per record is rising, as well as the incidence of data theft. Disgruntled employees and ex-employees are, for many reasons, stealing proprietary or sensitive data at an alarming rate.

In this white paper, we will address the risk factors associated with insider threat, especially in difficult economic times, statistics that quantify this rise of threat, as well as preventative measures and solutions that can be taken to mitigate certain risk factors.

Introduction

> *"The search for static security - in the law and elsewhere - is misguided. The fact is security can only be achieved through constant change, adapting old ideas that have outlived their usefulness to current facts." - William Osler*

Protecting information assets requires a dynamic security practice. As technologies advance, protocol must change in order to maintain information integrity. That said, a series of policies and procedures should be in place and strictly followed upon the termination of any employee, voluntary or otherwise. Should technology changes or data theft trends require change in these procedures, appropriate change should be made.

When companies cut back bonuses and raises, defer promotions, and outsource more to save money, negatively affected employees are more likely to perform malicious activity primarily as an act of revenge. It is important not only to maintain vigilant technical security, but to assess risky or uncommon personal employee behavior as well. The best approach to prevention of insider threat requires both HR and IT attention.

Insider Threat Risk Factors

"Risk is the combination of threat, vulnerability, and mission impact." - CERT Common Sense Guide to Prevention and Detection of Insider Threats, 3rd Edition – Version 3.1

Layoffs

Layoffs occur all the time, but are particularly prevalent in these rough economic conditions. Employees who are laid off or fired are potential risks to a company as they may become disgruntled or concerned about their financial and personal futures. This can lead to attempts to sabotage a company's information assets, steal data for financial gain, or steal data to leverage a position at another company.

Employee Dissatisfaction

Employees who feel that they have been treated unfairly by their employers are much more likely to perform malicious acts against their company than those who are satisfied with their jobs. A negative reaction to a disciplinary measure, new job duty, demotion, denied raise, or lowered bonus may cause employees to become disgruntled. In a recent study by the Ponemon Institute, it was found that 61% of employees who found their employers to be untrustworthy and lacking integrity and fairness stole data. Only 25% of employees who trusted and respected their employers stole data.

Separation of Duties (SoD)

Proper separation of duties (SoD) can prevent employees with too much access from either accidentally or maliciously manipulating proprietary, financial, or otherwise sensitive information. By giving employees access rights to only what they need to work, insider threat risk is greatly reduced.

Security Education

Educating all employees, temporary, high level, low level, or otherwise, is an integral part of creating and maintaining a secure environment. This will protect against insider threat risks of a malicious or accidental nature. Once employees are aware of safe and unsafe practices, they can be helpful in identifying others who may be posing a threat to the company.

Trusted Outsiders

Contractors, temporary employees, consultants, and other trusted outsiders can pose a great threat to a network. They are often given privileges that allow high levels of access, depending on their job criteria. As employees of other companies or self employed individuals, these outsiders may not have strong feelings of loyalty or respect toward the company for which they're presently working.

Account/Password Management

Creating passwords that are reasonably complex and changing them as frequently as needed is always a good security practice. As a part of security education, employees should be told not to share passwords for any reason.

Preventative Measures and Solutions

"Prevention is better than cure." - Desiderius Erasmus

Pre-Employment Screening/Employee Monitoring

Performing a background check can be helpful in weeding out potential candidates for insider theft during the hiring process. Thirty percent of employees who committed insider theft, according to a recent CERT study, had a previous arrest history. 18% were arrested for violent offenses, 11% for drug or alcohol related offenses, and 11% for non-financial/fraud related theft offenses. Had these employees been screened before hire, the insider attacks would not have occurred.

Changes in employee behavior or financial status should be recognized and evaluated. Disgruntled employees will inevitably show their dissatisfaction, and proactive measures should be taken to address their issues. Employees who have recently encountered financial problems should be monitored as they are more likely to commit insider theft for financial gain.

Create and Enforce Clear Security Policies and Procedures

Assessing risk factors specific to an organization and implementing the proper security policies and procedures lessens insider threat risk. These policies and procedures will vary by organization, but some essential security basics are appropriate throughout. Monitoring of file use, user privileges, logons, and downloads to removable storage devices should be in place for any employee with access to anything not in the public domain.

Policies should be documented regarding appropriate use of company systems and the data therein, procedures to air grievances, performance evaluations, and ownership of employee-created company information. Documentation and distribution of these type policies can prevent misunderstandings that may lead to employee disgruntlement, and thus, insider threat risk.

Educate Employees on IT Security

IT security policies mean nothing if the employees in an organization are unaware of them. Upon hiring, employees should read and sign documentation addressing company security policies. Periodic re-training should take place to ensure that all employees are up to date on the current policies and procedures. Security awareness is not like riding a bike; it can be forgotten or pushed to the edges of one's memory. Security training updates help employees keep company security at the forefront of their thoughts while conducting business.

Enforce Separation of Duties (SoD)

Giving users the least privileges necessary to perform their job duties is necessary to maintaining a secure environment. It is equally important to maintain least privileges when employees are promoted, demoted, or make a lateral move in the company. Auditing user rights is helpful in maintaining SoD by allowing administrators to see when privileges are changed, that they are done so with respect to change management, and specifically that change control request.

Remove User Access following Termination

Once an employee has been terminated, it is of the utmost importance to retract all access privileges immediately and repossess all company devices (e.g. Blackberry devices and laptops). In certain instances where termination occurs amicably, further access may be allowed for a specified period of time for the ex-employee. Though this practice is not recommended, should a business feel that it is appropriate, it would be wise to monitor this user's access heavily to ensure safety of proprietary information and critical system or data files.

Auditing as a Prevention and Detection Tool

Auditing is possibly the most valuable prevention and detection method regarding insider threat. Any signs of misappropriation of information can be seen through the proper auditing tool, if used well.

Any good auditing tool should be able to monitor file/folder/directory access and manipulation, changes to user privileges or group policy changes, USB storage device downloads, logons and logoffs, including failed logon attempts, and native event logs.

Reporting capabilities are important to an auditing tool. Windows logs can provide most information necessary to discover illegitimate activity; however, the logs are cryptic and take a lot of time and resources to cull pertinent data into a sensible report manually. Auditing tools should provide reporting that is clear, concise, and easily readable.

Real time alerts are quite useful when configured to alert the appropriate party to certain actions that would require immediate attention. They should be able to be sent to any number of parties, and different parties depending on the incident being reported.

LT Auditor+ Solutions

LT Auditor+ provides out of the box default auditing filters and reports which can be easily configured to meet any business's specific needs. Ease of deployment, comprehensive auditing, real time alerting, and easy to read, plain English reports are some of its most beneficial features.

LT Auditor+ can determine who performed what operation where and when for any auditable event. Reports featuring drill down capabilities and multiple output formats can be scheduled and automatically sent to the appropriate parties.

With LT Auditor+, you can be sure that your network is secure, protect yourself from internal and external threat, and maintain a keen watch over your business's day to day activities.

Summary

There are many factors that contribute to the rising risk of insider threat, including layoffs, employee dissatisfaction, and lack of security education, among others we've discussed in this paper. Being proactive about reducing your risk of insider threat can prevent information theft from occurring if the right procedures are practiced.

Screening employees prior to hiring, enforcing clear security policies, and educating employees on security policy are some of several ways a business can attempt to prevent insider threat.

Auditing employee activity is one of the most important measures one can take to ensure network security. Real time alerting is necessary when attempting to prevent theft. It allows immediate action to be taken to rectify inappropriate manipulation of or access to data.

LT Auditor+ automates the process of auditing and reporting critical operations and system changes, delivering actionable intelligence in the form of easy to read, plain English reports. For more information, visit www.bluelance.com or call 1 (800) 856-2583.