Results Oriented Change Management

Validating Change Policy through Auditing

Abstract

Change management can be one of the largest and most difficult tasks for a business to implement, monitor and control efficiently and completely. It is also one of the most important practices a business must control to be adaptable, protected from various security threats, and compliant with government regulations. This whitepaper describes the philosophy of change, the basics of change management and its implementation, as well as the problems facing organizations without clear change control policies. We will address automated auditing solutions to confirm, and thus control, verification of authorized changes and identification of unauthorized changes while focusing on regulatory compliance issues.

Introduction

"How can a stable organization whose goal is to maintain itself and endure be able to change and evolve?" – J. deRosnay

Change is a necessary part of maintaining a homeostatic business. Homeostasis should not be construed as lack of growth, for it can only be maintained by reaction to change (e.g. change in the marketplace), and those reactions should be productive. Maintaining homeostasis, or a "baseline" for a company, requires that company to react to every change with a series of modifications equal and opposite to those that instigated the change. If change is performed well through proper channels and processes, ideally, a level of dynamic stability can be reached and a natural state of pacing will occur with periods of large and small change occurring at reasonable intervals. This allows the organization to have periods of "rest" in which to become accustomed to the more significant periods of change while still making small but necessary alterations. Monitoring and managing changes that occur in a business's IT infrastructure is necessary to maintain environmental integrity and secure important informational assets, as well as comply with government regulations.

Managing Change

What is change management?

Change management is broadly defined as a set of processes put in place to ensure the orderly, systematic, and controlled implementation of significant changes. A problem or opportunity is evaluated, and possible solutions are discussed as well as the means required to execute them. Through a chain of command, these changes are made should those involved agree that the end result justifies the means required to perform the necessary actions. A "change" can be anything from adding or deleting a user from a network to restructuring group policy, and much more. The vast difference of organization type and company goals will define what changes are significant enough to be passed through this process. Changes to user rights, changes to data access, and changes to assets constitute significant changes. For most corporations, IT compliance issues come into play when making changes affecting sensitive data and user rights, and auditing the change management process becomes a requirement, not just a good idea.

Why is change management important?

There are three schools of reason regarding the importance of change management. The first, regulatory compliance, involves government mandated requirements that often make change management processes necessary auditing subjects. The second, standards compliance, deals with industry standards such as COBIT and ISO framework. The third, security, is geared toward personal company concerns, goals, and issues.

Regulatory Compliance

Requirements put forth by the Sarbanes-Oxley act (SOX), PCI/DSS and HIPAA, among others, generally include sections obligating corporations to maintain close watch over activities such as administrative changes and policy changes that are a part of the change management process, especially those relating to financial data and personnel files. If performed manually, data available from the event logs is limited and will incur a significant cost to the organization in time and resources. It is economically beneficial in most cases to employ an automated auditing system that will effectively reduce the number of hours required to gather, organize and review the information necessary for regulatory audits.

Standards Compliance

Industry standards such as COBIT, ISO, and ITIL are frameworks intended to provide an organization with a set of guidelines which facilitate IT security and compliance with most applicable government regulations. An organization chooses the particular framework that they feel best suits their regulatory and security needs, and makes the appropriate alterations or additions to the original framework as needed. These frameworks provide a good basis for IT governance and change control, and generally include requirements for the auditing of configuration and other changes.

Security

Permissions given to each employee on a network should be assigned based on a separation of duties (*SoD*) model. From a security perspective, separation of duties are enacted to prevent a conflict of interest, whether real or perceived, while restricting the access rights held by any individual.

Upon an employee's change of status (termination, promotion, or lateral movement within a corporation), permissions must be changed or eliminated based on that individual's new position (or lack thereof). This is done to maintain the safety and integrity of sensitive or valuable information as well as prevent unauthorized persons from making changes without following proper procedure. If a change is performed either maliciously or otherwise, without following procedures set forth, the results can be disastrous.

A report on insider threat states that 29% of malicious damage to a system or company in the report was performed by insiders who had either been granted inappropriate access permissions, or who had created a backdoor into the network through which to anonymously perform damaging acts. This makes insider threat the second greatest cyber security threat next to outside attacks (CERT). However, the mean damage resulting from insider attacks is 10 times greater than that from outside attacks, states a study on over 5oo incidents of data breaches. Maintaining the proper channels of authorization and implementation for change allows the change process to occur smoothly, efficiently, save time and money, as well as reduce the substantial risk of insider threat damages.

Footnotes:

CERT. 2005. Insider Threat Study: Computer System Sabotage in Critical Infrastructure Sectors. Rev. ed. Pittsburgh, PA. Software Engineering Institute: Carnegie Mellon University.

Verizon Business Risk Team. 2008. 2008 Data Breach Investigation Report. Verizon, Inc.

Change Management Evolution

Change management as it is generally practiced today has evolved from two very different schools of thought; mechanical or engineering focused change, and psychologically focused change. The engineering side placed emphasis on the processes, systems, and structures of a business as if they were physical parts of a machine. The psychological side focused on people and how they personally react to changes in their environment, e.g. how productivity, morale, or job satisfaction is affected. Beginning in the late 19th century, students of business improvement had been practicing and learning how to make changes to the operations of a business as a mechanical system, focusing on observable, measurable business elements that can be changed or improved.

The mechanical focus on change and the human focus on change have converged over time to become the hybridized model of change management most often seen today. The benefits of both schools of thought are integrated to provide a logical and performance based approach to change while keeping those individuals involved in the process in mind.

Auditing the Change Management Process

Overview

Auditing the change management process can be a strenuous and time consuming task. Successfully documenting changes requires gathering log information from multiple sources, reading the data and translating it into some sort of readable report. Raw logs and even some processed logs provide some data, but often in a format which is too cryptic to be of any value. Other critical change events, such as some settings within Windows group policy provide little or no valuable data relating to the change. Many of these events provide data about the nature of the changes while omitting information about who performed the change. The manual collection and/or translation of such data

requires a substantial commitment of resources and time to effectively perform the task.

Automating the process of auditing and reporting from this data, put quite simply, will save organizations time and money. Resources may be reassigned to other high value projects, leaving the task of review and customization to a smaller, more efficient team.

To simplify the collection of data, audit software should contain the ability to filter and report only on the specific data needed, as defined by organizational requirements.

Verification of Authorized Changes

The primary value in change auditing lies in its ability to verify that an authorized change has taken place, and has been performed correctly. The ability to see the details of a change, such as specific rights assigned to a user, or the before and after settings of a group policy object, are critical to the audit process. Some specific instances are outlined below.

Termination

There are many instances of security breaches resulting from a terminated employee's efforts to take revenge on the organization. Upon termination, steps must immediately be taken to ensure that the terminated employee no longer has access to the company's network in any way.

By auditing changes in administrative privileges and user rights, as well as user logon and logoff actions, one can prevent any mistakes when closing an employee's account with the company and ensure that they are no longer accessing anything on the network.

Should the ex-employee be allowed post-termination access to the network for reasons deemed appropriate by the company, their access to all files and folders as well as other changes made by the user can be audited to ensure that no inappropriate actions are taken.

Promotion/Lateral Movement

When an employee is promoted, rights must be changed as is appropriate to the employee in question's new position, as well as the person taking his or her place, and so on down the line.

Good auditing software should allow you to audit the changing of rights and privileges to ensure that the appropriate actions are taken when making such changes. This is also true when employees are moved laterally though a company and require different sets of rights and privileges.

Identifying Unauthorized Changes

Unauthorized changes can be monitored and audited as easily as authorized changes with the right auditing software. By creating auditing filters set to alert the user to any configured events desired, unauthorized changes can be made apparent immediately. These alerts can be set in real time, and can notify users of unauthorized elevation of privileges, as is described below.

Real Time Alerts

When configuring audit filters, real time alerting is an integral tool that allows messages to be sent upon the occurrence of any desired operation to one or more individuals to whom the operation may concern. Real time alerts allow immediate action to be taken to rectify unauthorized changes or malicious or accidental manipulation of critical data or privileges.

Elevation of Privileges

When privileges are elevated for an individual or a group, in most cases not all prior privileges should be parented in to the new privilege set. Auditing user rights can ensure that all users maintain the proper sets of privileges without error. If users are left with unauthorized privileges, any actions, inappropriate or otherwise, made using those privileges can be audited and traced back to the perpetrator.

Automating the Audit Process with LT Auditor+

By automating the audit process, LT Auditor+ provides its users with an easy solution to audit changes to directory and policy configurations, as well as user and group rights assignments.

Get Immediate Results

LT Auditor+ installs with a baseline set of filters to begin collecting audit activity immediately. Easily customize the default configuration to collect only the data needed to achieve your specific objectives.

Bulletproof Auditing

LT Auditor+ does not simply report raw log data. Raw events are instantly translated into real, recognizable activity; no event id memorization required.

Scheduled, Customizable Reporting

Choose from over 100 ready-to-run reports, or use them as templates and customize for specific uses. Reports may be scheduled for automatic delivery at desired intervals to any number of people.

Easily Manage Audit Data

LT Auditor+ consolidates audit data from the entire organization into a single secure repository. Audit data is easily archived to meet regulatory or policy requirements.

Summary

The set of processes put in place to control significant change is vital to any organization. The auditing of these changes is necessary to maintain regulatory compliance, standards compliance, and general security.

Change management practices have evolved into a combination of mechanical processes and human involvement that canvases most concerns regarding change. These include proper SoD models, their maintenance during employee changes to prevent insider threat risks, and regulatory compliance.

Attempting to audit the change management process manually using raw or even processed logs requires a significant amount of time and resources. Automated auditing solutions can greatly ease the substantial burden of change management auditing by achieving immediate results, translating raw data to easily readable formats, and scheduling reports to be generated when needed.

LT Auditor+ is the leading solution for real-time surveillance, auditing, and forensic analysis across Windows and Novell networks. It protects against unauthorized access, ensures privacy of data, guards against theft of intellectual property and monitors the use or abuse of user privileges. Features include 24x7 unobtrusive user and activity monitoring, powerful data filtering, real-time alerts, customizable reports, audit trail data protection, and cross-platform consolidation. In addition to enabling users to immediately pinpoint the root of security breaches, it reduces downtime and investigative costs, as well as providing compliance with audit and privacy regulations.

LT Auditor+ is an excellent tool to aid your company in establishing and maintaining quality change management procedures. For more information, visit www.bluelance.com or call 1 800 856-2583.