

TOTAL ASSET MANAGEMENT
Sarbanes-Oxley and the Autodiscovery
“Watchdog” Process

A Management White Paper by:

William B. Hesselbaugh

Frank Kassel



COPYRIGHT NOTICE

Copyright © 2008 by William Brett Hussenbaugh, Frank Kassel, and Veriam Technologies Inc. All rights reserved.

This document is protected by the copyright laws of the United States of America. It may not be reproduced, nor may any of its contents used in whole or in part, without the express written consent of the author.

ABSTRACT

This paper shows a real example of where a common IT Asset Management autodiscovery concept – the concept of using autodiscovery to validate the presence of network-connected PCs in the enterprise – can cause concern for internal and external auditors when considering Sarbanes-Oxley. It shows the auditor’s perspective and the trap that an IT Asset Manager can fall into if not careful. Finally, this paper gives a recommendation on how to proceed.

THE WATCHDOG PROCESS

Call it “watchdog” or what you like, the concept is pretty simple – use your autodiscovery tool to periodically verify that your PCs are still somewhere within the bounds of your enterprise. Some even use subnet information to get a “fix” on where the asset is when its presence is validated by the autodiscovery tool. This is not a new concept, however Sarbanes-Oxley now offers a new twist that is important to note.

Anyone who has tried to track IT hardware knows just how difficult it is to have a high percentage of accuracy concerning the whereabouts of PCs – especially laptops. Using the network to validate the presence of PCs and laptops is a good idea, and the practical IT Asset Manager looks at this practice as just another piece of a complex set of tools and processes – it represents augmentation but not the entire solution. The fact is, anyone can disconnect their PC and leave it sitting in an empty cubicle with its cables wrapped around it, or under a desk, or in a closet – and it happens all the time. Because most of us know and accept this as the nature of our business, we expect some percentage of our assets to fail to “report” at their appointed time for scan. We expect that the presence of some of those PCs will be validated by other catch points – such as the laptop user who calls the service desk for support (assuming we’ve integrated our asset tracking with the service desk), but after it’s all said and done we realistically expect to have some percentage of assets in a “we can’t say definitively where it is” state at any time. If that number is 10%, we may consider ourselves average, and if it’s 3%, we may consider ourselves best in class. Your internal and external auditors, however, most likely won’t see it the same way.

A REAL LIFE EXAMPLE

Consider a large company whose asset manager recently underwent an internal audit. The auditor was shown a report that documented a percentage of PCs whose whereabouts could not be definitively stated and that had not “checked in” via network login in over 90 days. The internal

auditor wrote a comment in his report citing the lack of definitive knowledge of the whereabouts of the PCs as an issue, which then spawned an intensive set of internal initiatives aimed at reducing that percentage to something more reasonable.

“WHAT WE HAVE HERE IS...’FAILURE TO COMMUNICATE.” Strother Martin, from the movie *Cool Hand Luke*

“More reasonable”, as it turns out, is a relative term. To an asset manager, who knows the difficulty in attaining, and sustaining, definitive location knowledge of a high percentage of all PC assets, 3% may seem entirely reasonable – even a stretch. To an auditor, concerned about the misappropriation of sensitive information that may be on the local PC hard drives, or password or URL history information that could be used to hack into corporate systems, 0% is the only reasonable response. Herein lies the trap – beware and do not fall into this trap as the large company in the example did. As a seasoned asset manager knows, it is practically impossible to hope for sustaining positive location knowledge of 100% of all PC assets, so there is little hope of satisfying the auditor. There is a way to avoid this trap, so read on.

THE AUDITOR’S PERSPECTIVE

Sarbanes-Oxley (7/02) Sec. 404 requires management to internally document, assess, test and report on the adequacy of internal control (design and operating effectiveness) over financial reporting, asset acquisitions and dispositions, and asset safeguarding (prevent/detect unauthorized acquisition, use, disposition - ref. Sec. 103 and SEC Rule 33-8238). Once management has done that, the external auditors will test management’s documentation, assessments and assertions, and will issue their own audit opinion report as to whether internal control is adequate. Internal control deficiencies that do not provide reasonable assurance (low risk) that material misstatements in the financial statements, via errors or fraud, will be prevented or detected on a timely basis during the ordinary course of business are known as “Material Weaknesses”. Material Weaknesses must be disclosed in management’s internal control report. If a deficiency exists that is less serious but still allows more than an inconsequential misstatement, this is known as a “Significant Deficiency”. Significant Deficiencies that are related must be aggregated to determine whether the aggregation is, in and of itself, a “Material Weakness”. When a “Material Weakness” exists, the external auditor must conclude that the company’s internal control is “not effective” in its report to the SEC and investment/creditor community. Frequently, when a Material Weakness is reported, CFOs get fired, CIOs get fired, the company’s stock price takes a hit, and the Directors & Officers insurance cost goes sky high.

On the surface, not being able to account for 10% of all PCs might not seem like such a big deal quantitatively. Sure, the fixed asset “existence” and “valuation” assertions will require an adjustment to the fixed asset subsidiary ledger and related general ledger accounts for the carrying amount of the missing PCs. In many companies, this adjustment will not be deemed “material”, because from a money standpoint, the carrying amount of the lost PCs relative to all other corporate assets is relatively small. If the adjustment is not made, the potential adjustment will be tracked and could, along with other potential adjustments, tip the aggregate adjustment threshold and require a larger financial statement adjustment be made. The lack of PC fixed asset accountability could, therefore, still get the blame, but the blame would be greater for tipping a much larger adjustment. However, a lack of sufficient accountability over asset acquisitions and

dispositions may be a direct violation of Sec. 404 and related SEC rules in cases where, even though the quantitative amount of the assets involved is small, the qualitative value of data directly associated with the asset is large. In these cases, it is reasonable to suggest that the “materiality factor” for establishing accountability (acquisition, disposition, unauthorized use or access) over these assets is “smaller rather than larger”, such that a lack of sufficient accountability over such assets might, at a minimum, constitute a “Significant Deficiency” and could very well be a “Material Weakness” under Sec. 404.

From a Sec. 404 standpoint, however, the larger problem is likely the lack of internal control (general controls and application controls) over the information on the PCs.

PCs typically have URL histories, saved passwords, and local data (data files and e-mail) stored on them. Consider what could happen if a “lost PC” fell into the wrong hands:

- Saved passwords could allow access to ERP/servers where fraudulent transactions could be entered undetected and sensitive data compromised (customer data exposed to competitors, payroll data scanned for social security numbers and sensitive salary data, financial data leaked before public release)
- URL history could allow a hacker undetected access to ERP/server log-ins, where password-cracking software could be used to gain ERP/server access
- Local data could include customer data, payroll data, and financial data. In the wrong hands:
 - that data could be manipulated such that fraudulent transactions could be entered
 - confidential customer, payroll or patient data could be compromised such that laws could be violated (HIPAA, Gramm-Leach-Bliley, California SB 1386)
 - data that represents documentation (books, records, memoranda) that must be retained via Sec. 802 could be lost

To illustrate the seriousness of the situation, consider for example if a company could not track 1% of its PCs. On the surface, 1% of a company’s PCs might not sound like a big deal from a money standpoint, but consider if that 1% were in the Payroll department, the Finance department, the Sales department, the Credit Department or the Procurement department. Unauthorized ERP/server and local data access could be a real problem, such that controls over the unaccounted for or “lost” PCs do not provide reasonable assurance (low risk) that material misstatements in the financial statements, via errors or fraud, will be prevented or detected on a timely basis. And that, my friends, is the definition of a “Material Weakness” in internal controls (due to weak PC physical access control over data, weak PC logical access control to ERP/applications and data).

HOW TO PROCEED

To avoid falling into the trap described earlier in this article, consider following these points of advice:

- Join forces with IT security. The ideal answer is to be able to demonstrate, to the satisfaction of an internal or external auditor, that sufficient access security or compensating controls exist to negate any risk to the corporation should a PC fall into

<http://www.veriam.com>

the hands of an individual with mal intent. For example, as compensating controls, all PCs could have their URL-histories automatically erased during boot-up, password-saving could be disabled, server/application passwords could be rotated frequently, restrictions via job-description could be placed on what data could be stored on local PCs, ERP/network hack detection software could be installed, and ERP access/violation detection software installed (attempts to gain unauthorized access to incompatible functions monitored and reported).

- Consider setting up different “risk” classes for PCs, which might mean a different disk image based on “risk” class. Conceptually, a high “risk” class PC would be highly controlled to the extent that it is physically impossible for it to contain sensitive data locally, have passwords stored locally, or past URLs stored locally. This class of PC would be issued to employees who do not possess a need to have potentially compromising information stored locally – they do all their work on the network. It may be time to reconsider “thin clients”. That would arguably leave a smaller percentage of PCs in the higher “trust” classes, creating a smaller and more manageable population to track.
- Be proactive. Work with internal auditing to construct a go forward plan that is practical, yet satisfies the concerns of all involved. Don’t wait to get audited and hope for the best. Don’t automatically assume that sufficient compensating controls exist to mitigate PC access control weaknesses. What you don’t know can hurt you.
- Wait until all phases of the plan have been completed, by all parties involved, to publish any reports from your watchdog process.

Sarbanes-Oxley is simultaneously raising the importance of ITAM as well as challenging it. Some IT asset managers, especially hardware IT asset managers, may now have a new catch point to consider as a result – internal audit. Embracing this new catch point appears to be the best course of action.

About the Author

Brett Husselbaugh has over 20 years of experience primarily in the IT industry. He has consulted with over 25 of the leading Fortune 500 companies on strategies for optimizing the IT investment. With experience as both a CIO and a CEO, Brett brings a unique and practical perspective to IT management, promoting the concept of operating as a "business within a business" to deliver measurable value. Brett is a proven business leader, an innovative thinker, a highly effective writer, and an enthusiastic and motivational public speaker.

Brett has experience as founder and CEO of TOBEK Technical Services, an IT Asset Management firm which he started with no outside investment and grew to 80 people in three years. He then positioned the firm and sold it to Inacom, a Fortune 500 company. Brett also has experience as a CIO, Managing Partner for Managed Services, VP of Strategic Development, VP of Services R&D, Principal Consultant, Industry Analyst, and Program Manager.

Brett has published several magazine articles as well as over 50 industry white and position papers. He has spoken on numerous occasions to audiences of senior and executive management teams on optimizing IT investment, developing strategy, and effective IT management.

Brett holds a Masters of Science in Electrical Engineering from the University of Texas at Arlington and a Bachelors of Science in Electrical Engineering from the University of Maryland at College Park. He is currently a member of American Mensa.

Frank Kassel is a senior manager (Oracle and Coopers & Lybrand) with over 25 years of Audit, Forensic Accounting, Information Technology and Governance/Compliance experience. He has extensive experience in internal control and IT auditing, and Enterprise Risk Management (ERM/COSO). He advises clients and client attorneys, lenders and E&O insurers on Sarbanes-Oxley Sec. 404 internal control and fraud (COSO and CobIT), Sec. 401 Disclosure and Sec. 409 Event-reporting requirements and on Sec. 1102 Officer Due-Diligence. Mr. Kassel is a frequent lecturer and counsel to senior management on Governance, Sarbanes-Oxley and risk/fraud/internal control issues. He is a CPA (licensed, Illinois), a CMA, CISA, holds a Masters Degree in Accounting, and is a Goldratt Jonah (Theory of Constraints).

OTHER PAPERS BY THE AUTHORS IN THIS SERIES

All papers can be downloaded from <http://www.husselbaugh.com>.

2001, "Total Asset Management. Value Model and Comparative Value Propositions"

2000, "Total Asset Management. Implementation Best Practices"

1998, "Total Asset Management. Phase III Metrics – Definition and Usage"

1997, "Total Asset Management. Phase II (Perpetual Inventory) Implementation Guide"

1996, "Total Asset Management. Benefit Analysis and Implementation Guide"

William Brett Husselbaugh
<http://www.husselbaugh.com>

<http://www.veriam.com>