

Fraud Mitigation and Biometrics following Sarbanes-Oxley

"Your company might be compliant, but you are still exposed to fraud!"

Paul Sheldon Foote and Reena Hora

California State University, Fullerton

pfoote@fullerton.edu

EXECUTIVE SUMMMARY

Abstract

The old days of external auditors claiming that they are not responsible for detecting fraud and of managements depending upon management letters from external auditors for learning about weaknesses in their internal control systems have changed with the enactment of the Sarbanes-Oxley Act (SOX). Following SOX, external auditors, corporate attorneys, directors, and managements of large companies have legal obligations to mitigate fraud. The full research paper (see link below) will prove that even your company might be compliant, it is still exposed to fraud and major damages. Until legislators will make the necessary adjustments, management has to take matters in their own hands and do more than the minimum requirements to protect their assets and investors!

Accounting Frauds and Scandals

The major accounting and corporate scandals of early 2000 led the US Congress to pass the Sarbanes Oxley Act (SOX) in 2002. SOX requires corporations to have tighter internal controls and transparency in their financial reporting. Following SOX, external auditors, corporate attorneys, directors, and managements of large companies have added responsibility and legal obligations to mitigate fraud.

Lawsuits and Criminal Cases

Many investors and third parties who have relied on managements' reports and their certified financial statements have gone to court to recover losses. The outcomes of these cases over time demonstrate changing legal expectations.

Lawsuits against External Auditors

There have been many court decisions which will discourage certified public accountants from accepting financial audit engagements if corporate managements have not taken active steps to mitigate the possibilities of frauds.

No Insurance Coverage

It is unrealistic to expect companies to not improve internal controls and buy extended insurance to cover them from losses. At least one major insurance company has rejected to insure accounting firms for legal liabilities.

Sarbanes-Oxley Act (SOX)

Sections 302, 404, and 906 have increased the responsibility of corporate management and external auditors towards fraud mitigation. Management is required to create internal control procedures and test these periodically. They also require certifying that the periodic reports filed with SEC are transparent and truly represent the operational results and financial condition of the company. Violations can lead to large fines or imprisonment, or both. Managements must now assess their internal controls. External auditors must express an opinion on managements' assessments of internal controls.

Public Company Accounting Oversight Board (PCAOB)

PCAOB was created following Sarbanes Oxley Act to set auditing standards for public companies. All registered audit firms are now required to use PCAOB's Accounting Standard No 5 for their audits of internal controls and financial statements.

Statements on Auditing Standards (SAS)

SAS 99 guides auditors to detect material misstatements due to fraud.

DuPont Case Study

DuPont is an example of a company with officers certifying that its internal controls are SOX-compliant. However, the absence of accounting fraud does not mean the absence of risks or of losses. A DuPont employee accessed and downloaded \$ 400 million worth of intellectual property to give to his new employer, the rival firm Victrex.

Biometrics: An Identity Management and Fraud Mitigation Solution

Frauds cannot be completely eliminated, but controls can be put in place to minimize frauds. The risk of theft of intellectual property at DuPont could have been mitigated if biometric controls were used to grant access to the parts of the system hosting their intellectual property and other sensitive data. Biometrics uniquely identifies a person by comparing distinctive biometrics features of a person with a previously created digital template of those features and clearly rejects unauthorized users.

Fraud Mitigation in an SAP Environment using bioLock

Security risks for companies using only passwords:

- The system access and authorization is based on username and passwords.
- SAP segregates duties based on roles. Users with these roles have system access through username and passwords. It is possible for a user to use another user's username and password to perform transactions and go undetected.
- SAP's customers grant system access to business partners, vendors and external consultants increasing their exposure to risk.
- It is impossible to track, which person actually accesses or changes critical information.

It is easy to get someone's username and password. This increases the risk for fraud. Biometrics is a much more secure way to control system access as each user will be uniquely identified and no one can use another's identity to log on. This will also provide "true" segregation of duties.

bioLock provides 3 levels of security in an SAP environment:

- Requires fingerprint authentication to log onto system
- Fingerprint authentication can be set at the transaction level and can also be set to require dual authorization for sensitive transactions such as wire transfers above a certain amount.
- Fingerprint authentication requirement can be set at certain sensitive fields or info types.

bioLock provides logs of who tried to access the system and of who viewed which documents or transactions. This can provide evidence in court cases. bioLock authorization can be limited to sensitive transactions and few key users automatically eliminating all others.

In the DuPont case, a bioLock package of 1,000 seats could have protected their top 1,000 users and sensitive data. This would have prevented access to the sensitive data and would have cost them a few hundred thousand dollars, a small price to pay to protect their intellectual property, image and stock price.

Download the complete research paper at: <http://business.fullerton.edu/resources/biometrics/>