
Internal audit's role in identification and investigation of frauds and other financial reporting irregularities

By John Cherpock, Managing Director, Protiviti Inc.

Say these names: Enron, Global Crossing, Tyco, WorldCom. What words come to mind?

Fraud? Theft? Corruption? Greed?

It's a safe bet these are some of the words that come to mind for millions of people in the United States and around the world.

Enron, Global Crossing, Tyco and WorldCom are by no means the only companies to have been looted by the people in charge of them. But they are recent and spectacular failures that created headlines months after their corporate governance meltdowns were revealed.

Other recent scandals involve Cendant, a travel and residential real estate services company that inflated income by \$500 million; Xerox, which restated earnings by \$1.2 billion after a whistleblower revealed accounting irregularities; Adelphia, one of the nation's largest cable companies, which filed for bankruptcy last summer after being looted by senior management; and Qwest Communications, which last year restated \$900 million in revenue. And the scandal allegations keep coming.

The week of Feb. 23 began with Dutch firm Ahold, the world's third-largest retailer with major grocery store and food service operations in the U.S., announcing that it had overstated earnings in its U.S. operations by at least \$500 million in 2000 and 2001. Ahold's news included the resignations of its president and chief executive officer and chief financial officer.

One day later the U.S. Justice Department announced a 12-count fraud indictment against four former Qwest executives. The indictment accuses the defendants of seeking to create more than \$33 million by wrongly reporting an order with the Arizona School Facilities Board. The action violated Securities and Exchange Commission rules, the indictment said.

The SEC filed related civil fraud charges against those four former executives and four other former Qwest employees, alleging that they inflated the company's revenues by \$144 million in 2000 and 2001 to meet Wall Street's expectations.

The next day two former Kmart Corp. vice presidents were indicted for allegedly inflating the company's earnings. The federal charges include securities fraud, making false statements to the SEC and conspiracy to commit those offenses. According to the indictment, the pair's false statements to Kmart's accounting and auditing divisions resulted in the company filing with the SEC a quarterly report that overstated operating results by \$42.3 million in the second quarter of 2001 and helped Kmart meet Wall Street's earnings expectations.

Later that day retailer Spiegel Inc. announced that its officers and directors have been the subject of a federal probe since January. Spiegel has been late filing financial reports. It filed its 2001 figures and reports for the first three quarters of 2002 the same week it announced the federal probe. Its 2002 fourth-quarter results and annual report have not been filed.

The probe centers on the late filings and whether Spiegel violated SEC rules by withholding information about the company's future. Not until early February did Spiegel reveal that its auditor had expressed "substantial doubt about the company's ability to continue as a going concern for a reasonable period of time."

The Sarbanes-Oxley Act, which Congress passed and President Bush signed last year, is one result of the public backlash against the rash of corporate scandals that have been coming to light. The act includes a variety of measures to improve corporate governance, including new reporting requirements to restore trust in the information corporations provide the public. How effective these measures will be remains to be seen, but this much is known: lawbreakers view laws as obstacles to get around.

The Qwest and Kmart indictments allege that the defendants knowingly filed false documents to hide their actions. They knew the law. They tried to get around it, according to prosecutors.

So internal audit has a big challenge and responsibility to identify and investigate fraud and other financial reporting irregularities.

The statistics

These numbers show how big the responsibility has become:

- About 6 percent of annual corporate revenue -- or \$600 billion -- was lost last year, up from about \$200 billion a year in 1996, according to the Association of Fraud Examiners.
- The average scheme takes about 18 months to detect. About 25 percent of companies hit by fraud fail to fix the problems that made them vulnerable to fraud in the first place. About the same percentage decline to notify prosecutors about frauds.
- About 30 percent of the time, fear of bad publicity is the stated reason for not notifying prosecutors. Certain evidentiary weaknesses and fear of counter-suits are other reasons.
- Of the 75 percent of companies that do go to law enforcement, about three-fourths of them see the wrongdoers convicted. Obtaining convictions, though, may provide small consolation when hundreds of millions or even billions of dollars have been lost and a company's reputation has been damaged or destroyed.
- About 80 percent of frauds involve asset misappropriation, with cash being the target 90 percent of the time. Corruption in various forms accounts for about 13 percent of frauds.
- The most costly and damaging frauds involve financial statements. The median loss is \$4.25 million per scheme. Legal risk and damage to the corporation's reputation add to the cost.

Employee tips and internal audits all uncover more frauds than internal controls or external auditors. According to the Association of Fraud Examiners 2002 Report to the Nation. Internal audit investigations discovered almost 19 percent of reported frauds in 2002. External auditors uncovered about 11.5 percent of them. Companies with an internal audit department suffer about half the losses as organizations without an internal audit department, according to the Association of Fraud Examiners.

Investigating frauds

Parties to investigations usually include internal audit, legal counsel, audit committee, regulators such as the SEC and law enforcement agencies and independent forensic investigators. Internal auditors may get on the trail of a fraud after noticing one or more fraud indicators. These include unusual or inexplicable

variances in books and records; irregular activity in cash procedures; high staff turnover; insufficient segregation of duties; lack of supporting documentation for journal entries or other adjustments; and excessive year-end or quarter-end adjustments.

These indicators often turn up in financial or operational audits. An especially good source of information is the disgruntled employee (who may be disgruntled because of the suspected fraud) or other employee who contacts a fraud hotline or provides a tip by some other means. More than one-quarter of all frauds are uncovered because of employee tips, more than any other source, according to the Association of Fraud Examiners. Company vendors also provide many valuable tips. External regulators or government agents and external auditors uncover frauds less often.

After detecting a possible fraud, internal auditors should notify counsel. Internal auditors typically do not have the training to conduct a fraud investigation on their own. Counsel also knows how to protect the company's reputation and guard against exposure to lawsuits from injured parties or even parties involved in the fraud. Also, the client-attorney privilege between a corporation and its counsel provides further protection. The privilege can be lost, though, if information is given to anyone outside the investigation team, including law enforcement agencies.

Corporate security also needs to be notified if fraud is suspected. Security can help take steps to protect evidence.

And, of course, the board and senior management need to be notified.

Whether to notify authorities depends on a variety of factors, including the scale of the fraud, evidence of possible outside involvement in the fraud, the company's responsibilities to protect funds and reporting requirements of governmental authorities or governmental fund providers.

If a company determines it should release information to the public, it should do so through appropriate channels, such as public relations or chief executive.

A major factor in the success or failure of an investigation lies in properly conducting interviews. Legal authority is usually not needed to interview people or delve into matters where fraud is suspected. Employees have the right to consult an attorney and may decline to answer questions to avoid self-incrimination. A private company would usually have the right to fire an employee in that instance. A public employer may not force an employee to choose between talking or being fired.

Employers may use deception to bluff a suspect into revealing information that may be helpful. To avoid lawsuits or tainting evidence, deception should never be used to threaten, force or coerce a person.

It is not necessary to provide an employee with a written notice of charges, but it could help avoid a lawsuit. Other ways to avoid legal repercussions are:

- never make unfounded accusations or statements;
- never ask about activities unrelated to work;
- never disclose private information about an employee to others not involved in the investigation; and
- never detain an employee for an interview in a way that could be construed as threatening or forceful.

Many investigations involve searches and surveillance, which can raise complex legal issues. For this reason, always consult counsel before searching files or desks or monitoring employee phone calls or taking similar actions.

Private employers generally have the right to conduct a corporate investigation. However, if law enforcement or regulatory authorities are involved in the investigation, an employer might need to meet

Fourth Amendment standards for privacy in the workplace. There is a risk that illegally seized evidence will be excluded from any criminal proceedings. To strengthen its legal position, a company should have written policies stating its right to search the premises and monitor telephone calls and emails for business purposes. Whenever possible, it is better to have an employee's consent to a search.

A good rule is to approach every incident as though it is an established fraud. Gather evidence as though it might be used in court to prosecute an offender. Include all relevant documents and exclude all irrelevant documents. For evidence to be accepted in court, it must be properly handled. Attempt to obtain original documents and handle them only as necessary. Identify each document and log it into a document tracking system, such as a database, so that no important documents are lost or misplaced.

A court will require a chain of custody before accepting a piece of evidence. To do so, track each item, noting when, how and from whom it was received. Also document where each item is kept. Also record whenever an item leaves the care, custody or control of the examiner. Use unique identifiers for evidence items. If it is not possible to write on the document, seal it and label the envelope. If fingerprint examinations are expected, use gloves to handle the documents and keep track of persons who may have handled the documents since they were obtained. Without these precautions, a judge could consider the evidence to be tainted and therefore inadmissible.

If the evidence is in a computer, perform a full backup of the server as soon as fraud is suspected. Do not use a computer on which suspected fraud occurred until it can be forensically examined. Do not open or examine suspect files yourself. Preserve a log of server traffic and an incident log where it cannot be deleted.

Investigators at WorldCom followed these procedures, helping to bring a stop to the fraud there. WorldCom's internal auditors suspected a problem and began to delve into the matter with appropriate care once the SEC began asking questions. They took careful steps with the evidence to preserve its integrity and reduce the risks outlined above. They also saved evidence by copying incriminating information onto a CD-ROM so that it could not be erased; and they leaked nothing to people outside the investigation.

Ultimately, they let the evidence lead them where it would. They did not jump to conclusions or make allegations. They asked questions, gathered information and then presented it to the board and audit committee.

Based on the WorldCom example and many other good ones through the years, I suggest that you put in place fraud and whistleblower policies that, among other things

- 1) forbid persons from making false allegations;
- 2) state the consequences if false allegations are made;
- 3) provide internal channels to report allegations;
- 4) outline sound investigation procedures;
- 5) outline external channels for the reporting of allegations and stress the importance of confidentiality;

SAS 99

The Institute of Internal Auditors endorses SAS 99 Consideration of Fraud in a Financial Statement Audit, but does not require it. SAS 99 emphasizes that auditors should exercise professional skepticism and identify risks that may result in a material misstatement due to fraud by brainstorming, asking management and performing analytical procedures. SAS 99 also stresses that auditors should assess the risk of fraud after taking into account an evaluation of the firm's programs and controls and should adapt the audit based on the findings of the evaluation.

We recommend that internal audit also use the SAS 99 approach in non-financial or operations risk assessments and audits. And we recommend that companies establish a fraud detection hotline as a deterrent. As noted earlier, employee tips break up more frauds than anything else. A fraud hotline makes it that much easier to obtain the information needed to detect and deter frauds.

As internal auditors, we have a role to play in making sure the companies we advise have controls in place to reduce the risk of irregularities going undetected for any extended period of time. As the past few years have shown, too many companies did not have an adequate system of internal controls to achieve this end.

With an angry public spurring Congress to improve corporate reporting and increase penalties for corporate wrongdoing, this is a time where internal auditors can make a positive contribution to the profession and corporate America. The spotlight is on what we do. If we do it right, we can bring more respect to the profession and help American business rebuild trust with the public it serves.

This is a summary of a presentation delivered by John Cherpock, Managing Director for Protiviti, at the Institute of Internal Auditors General Audit Management Conference in Orlando, Fla., on March 11, 2003.

For more information, see <http://www.knowledgeleader.com/>.

For questions please telephone: 1 866 923 8513. For requests from outside the U.S. or Canada, call +1 925 598 7771.

Material from the KnowledgeLeader® Internal Audit and Risk Management Community

<http://www.knowledgeleader.com>

© 2003 Protiviti. All right reserved.

Protiviti is the leading provider of truly independent internal audit and business and technology risk consulting services. We help clients identify, measure and manage operational and technology-related risks they face within their industries and throughout their systems and processes. And we offer a full spectrum of internal audit services, technologies and skills for business risk management and the continual transformation of internal audit functions.

1.888.556.7420

www.protiviti.com