When Technology is Used to Facilitate Fraud©

Al Marcella, Ph.D., CISA, CISM

> "Our goal is not to capture market share or be global. Our goal is to be the No. 1 stock on Wall Street
>
> Bernard Ebbers, in 1997 [now former CEO WorldCom and federal prisoner]

Today's crime scene is mobile, virtual, and nearly invisible. Evidence of wrongdoing is volatile, fleeting, and consisting of mere electronic bits surging across global networks through countless servers to unnamed routers onto faceless desktops. Welcome to the era of high tech electronic fraud (e-Fraud).

According to a Sage Software survey conducted by M/A/R/C Research, 21 percent of small businesses did not have a system in place to prevent employee fraud and another 13 percent didn't know if they did or not. Roughly a quarter of companies that have suffered fraud losses in the past have not established preventive measures. Twenty eight percent of small businesses that responded to the survey said they had been victimized at some time by employee fraud.[1]

Fraud can be defined as unlawfully depriving a person of his or her property or legal rights through intentional misrepresentation of fact or deceit other than forgery or counterfeiting, "An intentional perversion of truth" or a "false misrepresentation of a matter of fact" which induces another person to "part with some valuable thing belonging to him or to surrender a legal right".

A more viable working definition of fraud is a deliberate deceit which is planned and executed to deprive an individual of property, money or any other valuable security. Fraud must be committed with intent and includes actions of misrepresentations and/or acts of omission.

This definition hasn't changed much due to the impact of technology; technology has only made the commission of a fraudulent act easier, easier for both individuals and corporations. Weakening and difficult economic times will make good, honest people consider engaging in dishonest and illegal things (and actually carrying through to do those bad things!). The opportunity that technology provides to engage in potentially dishonest activities presents the organization with a considerable and heightened security risk and exposure.

What are the reasons for an increase in fraud? There are many, however, topping the list are:

1. No Standards of Business Conduct

2. Inadequate controls
3. Lack of emphasis on prevention
4. Weakening of society's values
5. More sophisticated technology/tools
6. Staff downsizing
7. Economic pressures

Current global economic pressures for companies and the employees who own, run, manage, and operate them, to perform, succeed, return profits, and survive, create financial pressures (and incentives) that are difficult to resist, and many give into this pressure. Technology makes this potential fraudulent activity easier, timelier, and less likely to result in the risk of disclosure or prosecution of the perpetrator.

Management must consider implementation of solid internal controls to mitigate potential fraudulent activities. The risk of fraud will not be eliminated…controlled yes, eliminated no!

In July 2008, The Institute of Internal Auditors (IIA) along with the Association of Certified Fraud Examiners (ACFE), and The American Institute of Certified Public Accountants (AICPA), released a jointly prepared document entitled "Managing the Business Risk of Fraud: A Practical Guide."

This new guidance outlined five key principles of a fraud risk management process and recommends ways in which boards, senior management, and internal auditors can fight corporate fraud. Key principles, according to the jointly prepared Guide, for proactively establishing an environment to effectively manage an organization's fraud risk include:

1. A fraud risk management program should be in place, including a written policy.
2. The organization should assess periodically, its fraud risk exposure.
3. Where feasible, prevention techniques to avoid potential key fraud risk events should be established.
4. Established detection techniques to uncover fraud events.
5. A reporting process should be in place to solicit input on potential fraud, and establish a timely methodology to investigate and take corrective action regarding potential fraud.[2]

Only through diligent and ongoing effort can an organization protect itself against significant acts of fraud.

High-tech fraud or e-Fraud exists in many forms:

- ID Fraud
- Counterfeiting
- Cyberlaundering
- Internet Fraud
- Skimming
- Terminal Cloning
- Phishing
- Spoofing
- Steganography
- Factoring

Leading the pack or at least the most widely publicized is ID Fraud, or more commonly referred to as identity theft.

According to Javelin Strategy and Research (2009) there were 10 million victims of identity theft in 2008, in the United States, and 1.6 million households experienced fraud not related to credit cards (i.e. their bank accounts or debit cards were compromised) (U.S. Department of Justice, 2005).

The Identity Theft Resource Center (ITRC) Breach Report presents individual information about data exposure events. Breaches identified by the ITRC as of July 2, 2009 totaled 268, this represented 12,322,887 exposed records, each with a potential of falling victim to fraudulent activity.

In the world of high-tech, e-fraud, with access to just a few key pieces of information, a criminal is very capable of impersonating an individual and engaging in fraudulent activities using the victim's identity. These fraudulent activities can and do defraud the victim, businesses, financial institutions and potentially countless unseen others, out of literally thousands, hundreds of thousands of dollars annually.

Controls to help mitigate high-tech fraud fall into three categories:

1. Detective - actions taken to detect and correct undesirable events which have occurred.
2. Corrective - controls are designed to correct errors or irregularities that have been detected
3. Preventative - actions taken to deter undesirable events from occurring.

To help ensure that these controls work as anticipated and continue to perform as expected by stakeholders, management must be proactive and provide a continuous monitoring of these controls. Monitoring is achieved via routine audits conducted by trained information technology and financial auditors, as well as through the use of specialized, automated software and in some cases, hardware.

Mitigating IT fraud takes a combination of both technical and non-technical skills, along with an updated IT tool set.

These tools include but are not limited to:

1. Networking Monitoring
    - Network Analyzers
    - Retrospective Network Analysis
    - Vulnerability Management
    - Network Intrusion Prevention
    - Network Intrusion Detection
2. Regular Fraud Risk Assessment
3. Physical Security of High Risk Assets
4. Fraud Awareness Training
5. Identity Management

> "Preventing fraud is infinitely better than detecting it afterward and then struggling to recover from financial losses and negative publicity."
>
> Neil Cowan, MIIA, ACIS, former Director General of the European Confederation of Institutes of Internal Auditing

Typical questions which require solid answers when assessing the viability of an organization's anti-fraud program include:

1. What types of fraud are most likely to occur with the organization?
2. Given the nature of the business, what are the inherent risks of fraud (e.g. types of fraudulent activity that are associated with the or inherent to, the nature of the business)?
3. What is or has been the "history of fraud" across all operating units with the organization?
4. How adequate is the existing fraud detection program/process in monitoring, detecting and controlling/mitigating fraud, within the organization?
5. What are the most significant gaps in the organization's existing anti-fraud program?
6. Given the nature of the business, how likely, i.e., what is the probability of a fraud actually occurring? Would the organization realize that a fraud has occurred?
7. What is or would be the significance (financial, legal) or business impact (loss of customer confidence) to the organization, were a fraud to occur?

E-Fraud is not going away; in fact it is most likely headed for an increase. Only through proactive, aggressive due diligence will organizations be able to keep the growth of e-Fraud in check.

Continuous assessments, implementation of appropriate anti-fraud tools, training and awareness programs, support and strong backing from senior management are the essential ingredients to a successful enterprise-wide anti-fraud program.

Citations and References

1. "High-Tech Fraud Prevention," Journal of Accountancy, October 2008, www.journalofaccountancy.com/Issues/2008/Oct/High_Tech_Fraud_Prevention.htm, retrieved July 2009.

2. "Managing the Business Risk of Fraud: A Practical Guide," July 2008, www.theiia.org/media/files/fraud-white-paper/fraud%20paper.pdf, retrieved July 2009.