

Setting a Process To Proactively Detect Fraud Using Technology

By Richard B. Lanza, CPA, CFE, PMP

Fraud is an elusive enemy in that it is a human nature issue. Therefore, as quickly we can build a person-trap to catch a particular fraudster, just as quickly will the person find a new means to extract funds from a company. While this may be a defeatist attitude, I consider it more of a realistic situation assessment. Also, by admitting that technology *alone* will not stop fraud, it begins us down the road to better detecting it at organizations. Technology needs to be paired with the human mind to make a new form, a bionic one, that stands the best chance to detecting fraud in organizations. With these concepts in mind, this article will present three simple tasks for consideration when establishing a bionic approach to fighting fraud. Task #1 is to establish proactive reports that work to identify expected fraud routines; the common fraudster. Task #2 is to use data mining to find fraud in those unexpected places and Task #3 is to proactively measure the employee psyche for signs of past, present, and future fraud.

Task #1 – Set Up Proactive Fraud Monitors

While occupational fraud takes various forms, the result is always the same: The numbers generated by fraud cannot hold up to the unflinching logic of the accounting equation. If executives add false sales and accounts receivable to increase the company's revenue, profits and cash will be out of kilter. The advancement of technology has allowed for this "accounting equation" to be systemized into computer logic and applied to company data¹.

¹ Foreword by Joe Wells - *Proactive Fraud Detection of Occupational Fraud Using Computer Reports*

So it is that simple; systemize common frauds to computer logic and run reports to identify them in company databases. Or is it that simple? While everyone knows this is one key step to fight fraud, most professionals tend to freeze when asked to think of 20 reports they should be running to find fraud. They grope to identify five maximum with three of the five being (1) Benford's Law, (2) Duplicate Payments, and (3) Match the Employee to Vendor Listing. While such reports will add value, they are so common in approach that most fraudsters already know about them, and hence how to hide their tracks.

A better approach is to run the most common of common of reports (they are not worthless) AND run reports that are specific to the organization's fraud risk profile. To that end, the Institute of Internal Auditors Research Foundation recently issued the publication [*Proactively Detecting Occupational Fraud Using Computer Audit Reports*](#). This publication provides over 250 reports to fight fraud that are aligned to the Association of Certified Fraud Examiners fraud classification system. Therefore, the auditor can complete a risk analysis of the types of fraud that can occur in the company, look up the associated chapter in the publication, and identify a host of reports (average of about 20 per type of fraud) for execution on company data.

One popular method is to assign a risk value to each fraud type in the organization based on the following equation:

$$\text{Risk Value} = \text{Likelihood (\%)} * \text{Impact (Dollar Value)}$$

Although it may be difficult to assign a precise dollar impact value, one can be estimated based on the size of the account balance and a reasonable level of impact based on the total. For example, the risk of fictitious sales may be represented at total company sales \$100,000,000 multiplied by .5% which would be the amount which may go undetected assuming the particular fraud scheme (i.e., Revenue timing differences). Using this estimating approach, frauds with the

highest risk value would be selected for further analysis. As to the types of potential fraud, the

IIA Research publication summarizes them into the following categories:

1. Bribery / Illegal Gratuities / Economic Extortion
2. Conflicts of Interest
3. Fictitious Revenues / Timing Differences
4. Understated Liabilities and Expenses
5. Overstated Assets/Valuation
6. Improper Disclosures
7. Non-Financial Fraudulent Statements
8. Cash Larceny
9. Skimming
10. Inventory Misuse / Larceny
11. Billing Schemes
12. Payroll Schemes
13. Expenses Reimbursement Schemes
14. Check Tampering
15. Register Disbursements

With a fraud type selected based on a risk calculation and an average 20 report ideas in the IIA Research publication for that fraud type, the auditor can then use a “piggy-back” brainstorming method in which he/she identifies numerous other permutations of a selected report. For example, the report, “Extract vendor purchases that exceed the 12-month average purchases to that vendor by a specified percentage (i.e., 200 percent)” is used to identify phony expenses billed by employees. A piggy-back report may be the same report but only if the vendor was newly added within the year....an increased sign of the transactions fraudulent nature. Therefore, through brainstorming, the potential tests can be expanded while also refining the selected reports to be more specific to particular entities.

Task #2 - Use Data Mining To See What Can't Be Readily Seen

Most data analysis is query-based allowing the auditor to extract records meeting a certain criteria (i.e., invoices over \$1 million). The process is therefore inductive in nature and, while effective at times, it also misses the uncommon schemes that could sink an organization.

In essence, query reports focuses on the individual trees while leaving out any analysis of the forest. Let's face it, any good fraudster knows what is commonly searched for and will therefore develop schemes that are missed by such detection reports. Likewise with controls, every one can be circumvented or overridden.

In contrast, data mining techniques such as auto-rule generators (technology that automatically identifies rules within data files and then tries to find deviations to these rules) and data cube technology (software that allows a user to drill down, summarize, and graph data on the fly with no prior training) work to find emerging trends that have not become common enough for a standard report. For a more detailed discussion of this approach using two common audit software, please see the AuditNet article [*Learning What You "Don't Know" About Your Data Files*](#).

Task #3 – Proactively Measure Employee Attitudes

Internal controls have been seen as the panacea to fighting fraud although they only go so far since internal controls provide only “reasonable assurance”. In other words, controls can be comprimised by an overriding manager. However, what can't be easily erased is the effect on the employee who witnesses the override, especially if this the employee who is asked to be party to the comprimising. For example, a staff accountant asked to post a questionable entry without all of the associated approvals or a manager who asks for the check register to “reconcile” a few things over the weekened while knowingly creating a segregation of duties issue. Such acts do not go unnoticed to all employees within the organization yet the auditor could not cost-beneficially interview all of the employees in a comnpany to detect such fraud.

Or can they? Enter proactive survey techniques that use the power of the Web to survey employee populations cost-effectively and create “heat maps” of employee satisfaction,

dissatisfaction, and tell-tale signs of fraud. Better than hotlines that require an employee to proactively pick up the phone themselves, these surveys are pushed to employees for completion in an anonymous way over the Web. Once complete, pre-defined reports can be reviewed to identify “hot zones” within the company where fraud has already occurred or a high likelihood of being enacted.

These surveys capitalize on the fact that people, not computers, commit fraud and many witnesses within the company want to share what they know about organizational control issues. Therefore, the tools help tap into the valuable information on fraud detection that comes from workers, not databases, thereby extending data analysis beyond lifeless financial and transactional data and into the vibrant data stores in employees’ and business partners’ minds. Not only does this form of analysis broaden the organization’s risk and control awareness, but gathering information from a large number of people can also increase the predictability and confidence levels of the assessment.

As Toby Bishop, President of the ACFE notes, “Yet when it comes to “management override” and financial statement fraud, the 1987 COSO framework is short on details and does not reflect the results of fraud prevention and detection research conducted in the past sixteen years. For example, anecdotal evidence suggests that evaluations currently being conducted do not generally use extensive employee survey techniques that research has found can be effective in uncovering environments conducive to financial statement fraud. If we want to tell the difference between ethics programs that really work and those that are merely a corporate fig leaf, such modern and thorough techniques are vital.”²

² Business Crimes Bulletin, “Sarbanes-Oxley Litigation Trap”, Business Crimes Bulletin, January 2004

A list of survey software vendors is available on the AuditSoftware.net Web site (Vendor Directory) and a more detailed analysis of implementing such an approach can be found in the article [*Proactive Control Monitoring*](#) as listed on ITAudit.org.

Conclusion

While fraud needs more than a three-pronged technology approach to be eliminated, it can be slowed, better prevented, and can lead fraudsters to “think twice” before posting that next bad entry or emptying the cash drawer. Through stopping the simple frauds with proactive reports, finding trends that lead to new frauds, and analyzing employee behavior, companies can greatly increase their chances of stopping unnecessary drains on the bottom-line.

Richard B. Lanza, CFE, CPA, PMP, president of Cash Recovery Partners, L.L.C., in Lake Hopatcong, N.J., provides audit technology and project management assistance to companies. With automated report systems and personalized coaching, Lanza helps companies get quality results and find cost-saving ideas in minutes. Lanza is the founder of the non-profit Web site, www.auditsoftware.net where he offers a free planning workshop for professionals desiring to implement audit software. His e-mail address is: rich@auditsoftware.net, Web site is: www.infomagician.com, and his phone is 973-601-3701.