

Fraud, an overlooked risk

1 a: DECEIT, TRICKERY; *specifically* : intentional perversion of truth in order to induce another to part with something of value or to surrender a legal right **b:** an act of deceiving or misrepresenting : TRICK

<http://www.merriam-webster.com/dictionary/Fraud>

John Glenn, MBCI SRP

When we cobble together a risk list for an Enterprise Risk Management (ERM) program, we "round up the usual suspects."

The major headings are Weather, Technology, and Human. All standard concerns for any Business Continuity (COOP in FedSpeak) plan.

Since we are developing a true ERM program, we also look at things often either considered "out of scope" for Business Continuity plans or things simply overlooked. A few quick examples:

- Client resources
- Government whims
- Insurance, including business interruption
- Lender strength.
- National and international economies.
- Reputation.

What we often overlook is fraud.

Granted, fraud can be buried under the title of "Human" since it is a risk caused by human greed or a desire for revenge.

But in the collection of general risks, fraud often flies under the radar.

Yet fraud has been a headline item for a number of recent years.

Some of the fraud cases, e.g., Enron, led to new regulations: the Sarbanes Oxley Act (SOx).

Many made headlines, including major names such as Goldman Sachs, Lehman Brothers, J.P. Morgan Chase, Morgan Stanley, Merrill Lynch, Salomon Smith Barney, Bear Stearns, UBS Warburg, and Piper Jaffray.

Some fraud cases lead to poisoning, viz. recent revelations about Chinese false teeth and the US dentists who pass them along to their patients.

There is the ever-in-the-headlines credit card fraud.

A Web search turns up a plethora of sites focusing on fraud. The tip of the iceberg includes

- SEC Actions (<http://www.secactions.com/>)
- POGO (<http://pogoblog.typepad.com/pogo/2008/07/over-900-whistl.html>)
- National Consumers League fraud center (<http://www.fraud.org/>)
- Inbox Robot's fraud page (<http://www.inboxrobot.com/news/corporate-fraud>)
- IRS (<http://www.irs.gov/compliance/enforcement/article/0,,id=174633,00.html>)

The mother lode for planners may be the Association of Certified Fraud Examiners (ACFE) Web site at <http://www.acfe.com/>.

An ACFE news item by Peter Goldmann that prompts this effort is titled "*No Fraud Here*" – *Can Management Afford to Continue Ignoring the Threat?* It may be read at <http://www.acfe.com/newsletters/fraud-examiner.asp?copy=august08-Goldmann-column>. I'd like

to claim that I found this on my own, but in truth, it was pointed out by Imran Majeed on the UK-BCP list (uk-bcp@yahoogroups.com) .

A brief aside. This scrivener participates - not just lurks - on a number of ERM/BC and related forums and lists, including DRJ's Forum and several Yahoo groups. It would be impossible to keep up with everything ERM by myself, but by sharing with others my "reach" is multiplied hundreds of times, with the benefit that articles such as the one Imran cited cross my virtual desk.

Goldmann is Editor and Publisher of White-Collar Crime Fighter (<http://www.wccfighter.com>), a subscription e-newsletter.

We know there's a risk, but . . .

Despite knowing we are surrounded by fraudulent activities, the ACFE article (ibid.) begins by telling readers "Less than one-half of organizations proactively identify fraud risk and have anti-fraud programs, policies and controls in place that are monitored and enforced by the board and senior management. "

The statement is based on a Protiviti (<http://www.protiviti.com/>) study titled Preventing Fraud: Assessing the Fraud Risk Management Capabilities of Today's Largest Organizations (<http://www.protiviti.com/portal/site/pro-us/menuitem.ca45dac229328c0fca19f110f5ffbfa0/>).

The Protiviti-commissioned study gauged the fraud risk management (FRM) capabilities of FORTUNE 1000 companies and large not-for-profit organizations. The primary findings of the study were three:

1. Organizations are at different maturity points in their capabilities to evaluate, mitigate and monitor fraud risk.
2. Organizations are struggling to understand what FRM means in the context of their daily operations.
3. Education and awareness are critical issues that need greater attention in order to successfully manage fraud risk.

A Deloitte Forensic Center survey, Ten Things about Fraud. How Executives View the "Fraud Control Gap", (<http://www.deloitte.com/dtt/article/0,1002,sid%253D140674%2526cid%253D177505,00.html>) notes that companies overall have in recent years enhanced their efforts to implement effective anti-fraud measures, a substantial "fraud control gap" is still glaringly evident from the data collected.

Goldmann's conclusion: Six-plus years into the "Sarbanes-Oxley era", most companies are still highly vulnerable to fraud of all kinds and management appears to show little intention of "tightening up" anti-fraud defenses.

Goldmann adds that "This, unfortunately, is not surprising. Fraud remains an issue most managers still find easy to ignore. Why? Because fraud is unpleasant... investing in fighting it has no immediately quantifiable ROI ... and it is desirable — indeed reassuring — to assume that the organization is so well managed that it is at minimal risk of being victimized by fraud. Moreover, many executives of large public companies have convinced themselves that the multi-millions spent on compliance with Sarbanes-Oxley is more than enough to protect them against major fraud."

An ACFE report cited in Goldmann's article, Report to the Nation on Occupational Fraud & Abuse, estimates that US organizations lose seven percent of their annual revenues to fraud.

Goldmann notes that seven percent "represents an upward spike of two full percentage points since the last survey was published two years ago—or nearly fifty percent. This is another in a

long series of indicators that no matter how daunting the fraud threat, management still finds ways to convince itself that fraud is a 'second-class' priority—that there are far more pressing demands than taking an active role in the organization's defenses against financial crime."

Having cited the general problem, Goldman begins to sound like any ERM practitioner when he rhetorically asks "Why is it not obvious to senior management that fraud losses far exceed the financial outlay that would be required to substantially reduce those losses?"

How much of a reduction in loss?

"Organizations that implement fraud awareness training, hotlines and other key elements of a Fraud Risk Management (FRM) program are rewarded with a more than 50% reduction in fraud losses," he writes.

Get expert opinions

I contend that ERM (a/k/a BC and COOP) practitioners need to be Subject Matter Experts (SMEs) in one thing: Emergency Risk Management.

As ERM SMEs, three of the things we must know - and convey to our clients, regardless if we are "captive" practitioners or consultants - are that for the best program,

- The practitioner is an SME only in creating ERM programs and plans
- Internal SME input is basic to all programs and plans
- Outside experts' input is required

I never understood why a "business continuity planner" is expected to have an InfoTech security background, particularly when there are such people already on staff.

Much of the outside experts' expertise normally is more-or-less freely available. The weasel wording "more or less" will become clear in a few paragraphs.

Physical security? The local constabulary is available. The officers know both the risks that are generic and those that are unique to the organization - perhaps due to location, perhaps due to product or service, perhaps due to the employee population (e.g., retired military).

Fire safety? Who better than the local Fire Marshall who can ferret out fire hazards and provide training to avoid or mitigate hazards and the appropriate means to extinguish a fire if one occurs (let's keep water off an electrical fire).

Emergency medical personnel, sometimes associated with the local fire brigade, sometimes with a hospital, and sometimes with a First Aid organization, can provide basic first aid training. Having basic, recommended, equipment on hand and the knowledge to use it appropriately and safely can save lives.

General risks? Invite the insurance carrier to send in one of its experts. Insurance carriers generally jump at the chance to reduce their fiduciary risk - insurance companies, we must recall, are in business to make money, not pay it out. Just ask anyone who has stock in an insurance company.

The earlier weasel wording, that the assistance is "more-or-less freely available" is due to the fact that all of these experts are paid by the organization, albeit indirectly, either through taxes or insurance payments. The bottom line: the organization pays for, and can legitimately expect to receive a service from, these function's experts.

Is it worth bringing in paid experts such as members of the ACFE?

As with most things ERM, that is a decision to be made by management.

The practitioner, however, needs to do all necessary homework to guide management. Is the cost of an external SME worth it? What is the potential Return On Investment (ROI)?

Is a seven percent "hit" to the bottom line acceptable to management?

At the same time, practitioners need to expand their personal knowledge by participating in organizations, and on lists, that relate - directly as the DRJ Forum - or indirectly - as does the International Association of Emergency Managers (IAEM) list - to the business in which we are SMEs. The organizations which employ ERM/BC/COOP practitioners should encourage this and should support expanding a practitioner's knowledge through membership in professional organizations.