



# Fraud and Embezzlement: The Insider Risk

Most Companies Don't Get Serious About Fraud Prevention Until They Become Victim To It. What About Yours?

A HILLARD HEINTZE EXECUTIVE BRIEFING PAPER





It's an uncomfortable truth. But in the vast majority of cases, acts of fraud and embezzlement occur because – somewhere in the spectrum of countermeasures, from keeping track of physical assets to championing a culture of security awareness – companies failed to establish even basic prevention-oriented practices widely proven and acknowledged to be very effective at mitigating the “insider risk”.

Like what? Well, take monitoring and internal controls, for example. Like ensuring segregation-of-duties and dual accountability. Like creating robust security controls that are specific to employee functions – and then testing them. Like avoiding dual reporting relationships – and removing the opportunity for an employee to tell different managers different stories.

Or take policies and principles. Like ensuring the company's code of ethics requires the disclosure of actual, potential and perceivable conflicts of interest. And requiring the identification of material interests insiders have in the business of any customer, vendor or supplier.

## Red Flags of Caution

Research has uncovered a great deal about fraud and embezzlement – clues that are crucial to defining the right countermeasures. In 2004, the National Threat Assessment Center of the U.S. Secret Service completed the Insider Threat Study in conjunction with the renowned Software Engineering Institute at Carnegie Mellon University. Here are a few interesting study highlights:

- Most insider events were triggered by a negative event in the workplace – and most perpetrators had prior disciplinary issues.
- Only 17% of the insider events studied involved individuals with administrator access.
- Three out of ten (30%) incidents took place at the home of the insider using remote access to the organization's network.
- Financial gain was the dominant motive, driving 81%. Other common motives were revenge (23%), dissatisfaction (15%) and desire for respect (15%).
- Most incidents required little technical sophistication. Only 23% of perpetrators held technical positions and 87% of the incidents used only simple, legitimate user commands.
- Perpetrators planned their actions. In addition, in 85% of cases, someone else knew of the plans.
- Perpetrators do not share a common profile. Just 58% were male, 54% were single, their jobs were scattered throughout the organizations and few of them were known troublemakers. However, 27% did have arrest records.

## A Smart First Step: Get Familiar With the Fraud Triangle

Most people who commit fraud against their employers are not career criminals. They are often trusted employees who have no criminal history and who do not consider themselves to be lawbreakers:

### So what factors cause these otherwise normal, law-abiding persons, to commit fraud?

The best and most widely accepted model for explaining why “good people” commit fraud is the Fraud Triangle. This is a model developed by Dr. Donald Cressey, a criminologist whose research focused on embezzlers, people he called “trust violators.” According to Cressey, three factors must be present - at the same time - for an ordinary person to commit fraud:

1. **Pressure or motive** - i.e., the need to pay bills, a drug or gambling habit, the need to meet productivity targets at work.
2. **Opportunity** - i.e., the occasion and positioning to commit a fraud without being discovered.
3. **Rationalization** - i.e., the logic and mindset that allows fraudsters to believe that their fraudulent act is justifiable.





## Practical Tips for Execution: Our Recommendations

### Tip #1 - Identify potential risks, threats and vulnerabilities - and understand the full costs of fraud before an event occurs

The risks of fraud can depend on many factors - some of them perhaps unique to your business. Get to know these well - and how to address them. Also, be aware of your potential losses as well as other costs, such as the legal settlement costs, financial restatement costs, increased insurance rates and operational costs for remediation. And don't forget to estimate both direct and indirect financial impacts to operations, customer retention and reputation.

### Tip #2: Know your people

Background screening is a critical best practice in fraud prevention at any time - but particularly during periods of economic turmoil. Don't just make screening a standard part of the employment process. Push further - and take special care in (1) defining the scope of the background investigation and (2) adopting an effective decision-making process that accounts for the investigative findings on a consistent and fair basis. One more thing: from time to time, conduct periodic updates and post-employment financial background checks, especially for key insiders.

### Tip #3: Make leadership, values and awareness top corporate priorities

Sticks work. But carrots are sometimes more effective. Champion positive attitudes about security. Support and empower your employees to report suspicious activity or incidents. Pay attention to your employees and how they feel about their jobs. Be attentive to changing behavior - one the key "leading indicators" of potential issues. And lead the charge - with passion and consistency - in creating a true "culture of security".

---

### For More Information

To find out more about preventing fraud and embezzlement in your business, contact:

- **Arnette Heintze**, Chief Executive Officer  
(312) 869-8500 or [arnette.heintze@hillardheintze.com](mailto:arnette.heintze@hillardheintze.com)
- **Ken Bouche**, Senior Vice President  
(312) 869-8500 or [kenneth.bouche@hillardheintze.com](mailto:kenneth.bouche@hillardheintze.com)



Hillard Heintze provides the strategic thought leadership, trusted counsel and end-to-end services that help leading public and private corporations as well as government agencies and major public service organizations advance best-in-class security strategies and investigations to protect and preserve the safety of their people, property, performance and reputation. For the last two years, Hillard Heintze has been recognized by *Inc.* Magazine as one of America's fastest-growing private companies - with a ranking of No. 242 on the 2009 Inc. 500 list and No. 583 on the 2010 Inc. 5000 list. The company has also been ranked by the Initiative for a Competitive Inner City (ICIC) #6 on its 2011 list of the 100 fastest-growing inner city firms in the United States.

Formed in 2004 by Terry Hillard and Arnette Heintze, the firm today is considered by many of its clients, its professional peers and its competitors to be one of the leading private strategic security advisory and management companies in the nation. For more information, visit [hillardheintze.com](http://hillardheintze.com).



The Hillard Heintze 360° INSIGHT publication is an ongoing and regular series of executive briefing papers on a wide range of critical and emerging issues at the forefront of best-in-class security and investigative practices today. To view other publications in the series, visit [hillardheintze.com/360insight](http://hillardheintze.com/360insight).

© 2011 HILLARD HEINTZE LLC