

INTRODUCTION – Current existence of “due diligence requirements”

Insurance is, by its very nature, a risky business. Limiting your exposure to claims and litigation is paramount. To that end, especially in this economic climate, insuring clients who have no interest in performing due diligence measures, or being proactive in limiting their exposure to loss, seems to be a losing proposition.

In almost every kind of liability insurance, home, property, car, etc., there is some level of due diligence expected on the part of the insured. Fire clearance areas, rise and run measurements for stairs, building codes, etc., all are in existence, to some degree, because of the advisability of due diligence to limit the exposure of the insurance companies.

Insurance companies give premium discounts to vehicle owners who have installed anti-theft devices and alarms in their vehicles. Home intruder alarms also fall into that category. Come to think of it, who would want to insure someone who is unwilling to take the responsibility for any kind of due diligence to prevent the kind of incidents being insured against?

“Due Diligence” requirements do not exist in the world of the fidelity policy

In the world of the fidelity policy, insurance companies are on the hook for losses suffered, including embezzlement, fraud, theft of property or intellectual property, etc. Costly litigation is a real possibility for nearly all claims, potentially costing both the insurer and insured millions of dollars over the life of the policy. Surprisingly, insurers do not expect or require the insured to conduct comprehensive due diligence to assist in the mitigation of these losses.

Companies spend large sums of money to protect their computer network, their physical workspace and to limit violence and sexual harassment in the workplace. All of this is a great start. This posture covers two out of the three necessary components of a comprehensive risk management program. Typical Risk Management postures overlook training and utilizing the people in your organization as the last line of defense in the battle against occupational fraud, in its many forms.

In the recent 2008 ACFE Report to the Nation, it was noted that an average of 46% of all incidents were discovered because of a tip from an employee or vendor. Given this overwhelming percentage, it seems logical that bolstering the employee's ability to recognize and report embezzlement, fraud or theft of corporate assets should be a mandatory step that all insurers should require.

How the Insureds see this issue

When discussing proactive measures with your insureds, the response invariably received by Insight Tactics is “We have insurance; we do not need to take those steps.” Roughly translated, this means that your insureds are not willing to shoulder any of the cost of adequate and comprehensive due diligence.

What that means for the insurers is your insureds expect you to carry the full load of responsibility for losses incurred, but they are not willing to help shoulder the burden of proactive self-help.

Current Trends

In the field of law recently, insurance companies who cover firms for conflict of interest issues have mandated that firms follow a provided “conflicts check-list” to help ensure that all potential conflicts are rooted out prior to engaging the client.

Supporting Research and Data

According to the 2005 Private Sector Risk Survey done by Chubb Insurance, of the 148 companies who reported an incident of employee fraud or theft, the average incident cost the company \$348,306. Nearly 33% of the executives interviewed expected to be hit by some type of employee fraud or theft in the coming year...and they are STILL unwilling to shoulder any of the responsibility for conducting comprehensive due diligence.

The number of examples that exist where the average loss from corporate espionage is in the \$400,000 range is endless. If even one of your corporate fidelity clients is in the fields of research and development, the auto industry, the cosmetic industry, the toy industry, the video-gaming industry, the entertainment/movie/music industry or any of the myriad industries that support the above list, chances are your client has already been targeted.

In September 2008, the Association of Certified Fraud Examiners (ACFE) published their bi-annual Report To The Nation on occupational fraud. This report compiled statistical data from Certified Fraud Examiner who investigated each of the 949 incidents reflected. The statistical data for the report are compiled from incidents where the incident was discovered, reported, investigated, and the perpetrator was reasonably identified.

There were some interesting conclusions drawn, such as:

- 1) The average incident in this group was \$175,000
- 2) Sixty percent (60%) of all the incidents were over \$100,000
- 3) The average incident involving managerial employees was \$1,000,000
- 4) Forty-six percent (46%) of all private sector fraud was caught because of a tip from an employee or vendor

At Insight Tactics, we firmly believe that educating your insureds' employees how to recognize the common indicators of embezzlement, fraud and other forms of economic or corporate espionage is the most important factor in deterring occupational fraud, in its many forms. Providing an anonymous reporting structure and a corporate culture that encourages employees to participate in the company, not just put in their time, is also invaluable to the mitigation of these losses.

The Math

The ACFE estimates that occupational fraud costs the average company 7% of their bottom line, annually. If this estimate is applied to the 2008 U.S. GDP, occupational fraud will cost our economy \$949 billion dollars this year. The truly frightening aspect of this number is that the ACFE and U.S. Chamber of Commerce estimate that only 30% of all incidents of fraud that are discovered are reported.

If this number (\$949 billion) represents 30% of the actual total of incidents, this may mean the actual number (accounting for the 70% of un-reported incidents) is nearly \$3,163,333,333,000 dollars (that's \$3.163 trillion). This staggering sum represents losses directly attributable to occupational fraud, corporate and economic espionage and competitive intelligence activities. In the current economic state, our economy cannot stand idly by and suffer losses of this size.

The U.S. Chamber of Commerce and the ACFE report that approximately 20% of all new-business failures each year are due to corporate espionage or employee malfeasance. Indifference to the existence of this situation is inexcusable. In the final analysis, it is the insurers who are on the hook for this staggering sum, or for what portion of that reported sum they cannot find a way out of paying.

What do you do about it?

The FBI's Corporate Espionage Outreach web-site presents a list called "The Top Six Things You Can Do To Stop Corporate Espionage." "Provide your employees on-going security training" is item six on that list. The type of training being recommended is called Employee Security Awareness Training.

Insight Tactics offers a comprehensive Business Counterintelligence Program that is directed at mitigating losses from occupational fraud, embezzlement, theft of corporate assets or any other variety of corporate/economic espionage or competitive intelligence gathering activities.

Insight Tactic's Corporate Employee Pattern Recognition (CEPR) Training is a more comprehensive and robust version of the awareness training required for all contractors and sub-contractors dealing with the DOD. Over its 47 year track-record, this program boasts a 26% interdiction rate of intended acts of fraud or espionage. Given the current confluence of economic climate, 2,000,000 jobs lost in the U.S. economy, and millions of home-owners losing their homes, there has not been a situation so ripe for employee malfeasance since the Great Depression.

Our Business Counterintelligence Program does not cost the insurer a dime. The sole "cost" to the insurer is the cost of adding a clause to the fidelity policy recommending or requiring this type of annual certification for companies applying for or renewing a corporate fidelity or employee theft policy.

The cost of the training is borne by the insured and, as a result, your insured will experience less incidents of occupational fraud, theft of corporate assets or losses from economic or corporate espionage and competitive intelligence gathering activities. Fewer actual incidents (both the reported and the unreported kind) means less claims filed, fewer denied claims and significantly lower arbitration and litigation costs.

This comprehensive Risk Management posture produces a company that is more profitable, less risky to insure, and, from the insurer's perspective, one that is shouldering a fair share of the responsibility for mitigating losses from occupational fraud and other types of economic or corporate espionage.