Fall 2014

1.866.931.1300

PALOMAR INVESTIGATIVE® GROUP, INC

"Reliable Information For Business Decisions"™

While most IT and Accounting personnel are honest, they are indeed the individuals who hold the "Keys to the Kingdom." Realistically, though, not everyone in these positions is honorable.

This group has accessibility of *"internal controls"* consisting of assets and management resources. When abused, there is a greater potential for workplace fraud and exposed safeguards, highlighting a serious business risk.

Mitigating these threats is incredibly important. Business executives, human resource managers, and in-house counsel must take back their master "Keys to the Kingdom." This can be a challenge since the real "key-holders" are behind the scenes.

Oftentimes these essential roles are overlooked when work is performed in a timely fashion, and when specific tasks are completed without a hitch. Smooth sailing IT and Accounting departments doesn't trigger questions or audits.

Yet, with more than 20 years of corporate investigations under our belt, we have seen the results when things go wrong.

ACCOUNTING/FINANCE & INFORMATION TECHNOLOGY

The spotlight on these two areas is by no means disproportionate in where one dominates the other. Rather, when losses do occur, the backlash of damages is the most severe.

Accounting/Finance employees have unique opportunities for malfeasance. A compromised roster includes embezzlement, diversion of funds for unauthorized purposes, and fraudulent financial statements. Undoubtedly, this group controls the direction and flow of money for your business. According to recent statistics, accounting-related occupations are the direct cause of 30% of all internal fraud cases; including, a median, high-impact loss of approximately $500,000.

IT and IS employees are a click away from internal communications, client interactions, R&D data, and so much more. Our investigations have uncovered disgruntled IT employees who actually pried into confidential e-mails. Other activity has included transferring of proprietary data to unauthorized, outside entities, including:

- Leaking secret, internal business plans
- Stealing identity information from HR databases
- Granting "back door" access into company systems

It's estimated that IT personnel remain responsible for about 3% of internal frauds. While this percentage is low, you should proceed with caution. The compromised data is not always quantifiable into dollars.

Continued on other side

Who really has THE KEYS TO THE KINGDOM?

...Continued from other side

PROVEN PREVENTATIVE MEASURES

There is an array of standard business practices to help alleviate the risks of deceit and fraud. As we all know, a lack of internal controls leads to business instability.

We recommend a variety of measures to incorporate into sound business processes:

Hotlines: Operating 24/7, these call-in systems enable employees, contractors and others to report malfeasance (of all types) taking place within your company. Studies have validated a high percentage of "business misconduct" issues are revealed through toll-free hotlines. Losses can therefore be minimized. There are a range of providers, including *EthicsLine at 888-782-4769.*

Regular/Unannounced Audits (IT & Accounting): Random audits, layered with in-depth reviews, are highly advantageous for numerous reasons. However, avoid CPA firms and IT specialists who once worked with your employees. Audits and reviews should be conducted using a clean slate.

Confidentiality/Non-Disclosure Agreements: As California laws frequently change; you are wise to involve an employment lawyer to periodically review these agreements. Provide employees with a copy of the signed document upon hire; and, another copy at time of departure. A verbal reminder (at separation) of their continuing obligation(s) is also suggested.

All temporary and contract workers should sign uniquely worded NDAs. We recognize that these documents are only one tool for preventing losses. Nevertheless, you will definitely need them in any matter potentially involving the court system.

Background Checks: Background screening is a standard practice, but more in-depth measures should be implemented for potential IT, Accounting, or other finance-type of employment.

Scrutinize any **"red flags,"** including:

- Wage attachments
- Bankruptcies
- Tax Liens
- Civil Judgments
- Credit Bureaus, if warranted

Financial woes are frequently tantamount to future fraud schemes and embezzlements. Unfortunately, employers are almost always the first target.

A "Global Fraud Study," available at www.ACFE.com, published by the *Association of Certified Fraud Examiners,* offers a great springboard to help safeguard and educate businesses management.

For questions or assistance with business-related investigations, please contact Gordon J. Schmidt, CPI, at 1.866.931.1300.

PALOMAR INVESTIGATIVE® GROUP, INC

1.866.931.1300
www.piginc.com
CA Lic. PI 16437

"Reliable Information For Business Decisions"™