Commentary

Firms should be proactive in preventing fraud, espionage

Billions in losses could be avoided with background checks, protection of trade secrets

By Paul Jaeb

In today's relentlessly competitive global marketplace, most executives take extraordinary efforts to help their business succeed.

They invest millions of dollars in research and development, as well as marketing, distribution and advertising. They spend vast sums on insurance to protect against loss of the buildings in which their businesses operate and the equipment they use to produce their products, and to cover liability for the performance of their products in the marketplace.

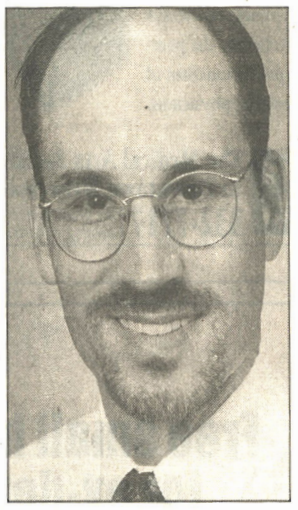
Yet, for all of the extraordinary efforts businesses make to try to ensure their success, many completely overlook insurance against loss from a source much easier to identify and much closer to home.

Their employees.

According to TRW, the credit reporting agency, American businesses lose over $500 billion each year to internal and external fraud — a staggering amount that cuts directly into the bottom line of businesses and adversely affects almost every sector of the American economy.

What does that mean for individual businesses? In a survey by the Association of Certified Fraud Examiners, the average loss per business was estimated at $120,000.

Most companies are reluctant or embarrassed to admit that they may have a problem with their employees. Many companies fear the Orwellian overtones of checking up on their workers. Yet the numbers are too large to ignore. Employee deceit is one of the most preventable losses that businesses can manage.



About the author

➤ **Paul Jaeb** is president and owner of Heartland Information Services, a Minneapolis business intelligence firm. He is a member of the Association of Certified Fraud Examiners and the Society of Competitive Intelligence Professionals. He is past president of the Minnesota Association of Private Investigators.

Recent headlines

You need only to look at some recent headlines in the Twin Cities to see the scope of the problem. And you may be surprised to discover that some of the worst examples of employee fraud come not from rank and file, but from the executive suite.

One of the most spectacular business failings in 1997 was Equisure, a Minneapolis-based reinsurance company. In August 1997, Equisure's stock traded at $15 a share and the company had a market value of $167 million. The company soon collapsed amid accusations of fraud and insider trading that were leveled against officials of Equisure, including its former CEO and CFO.

At one point in the crisis, Equisure issued a press release in which its newest CEO referred to a group that included his predecessor as "conspirators who hatched a plan to defraud Equisure shareholders of millions of dollars. . . . They are thieves. They are liars. They are cheats."

Fortunes were lost and careers were ruined because of the collapse of Equisure, and *much of it was preventable.*

Citing court records in a Texas case, Corporate Report magazine in November reported that David Sachman, Equisure's former CFO, was really Paul Yorke Wade, an alleged international insurance criminal. In August, Wade was in a French prison awaiting extradition to Belgium.

A trained investigator could have uncovered Wade's background and provided an early warning, if anyone had bothered to ask. But most companies, after investing millions in their products, never think to perform a simple background profile on their key employees who are responsible for investing the company's assets.

Unfortunately, most companies wait until after a fraud has occurred to ask for help. This is penny wise and pound foolish. Any company competing in today's global marketplace cannot afford to be without a plan for instilling internal controls to avoid losses *before they occur.* And no employee, no matter how senior, should be hired without a thorough background profile.

Corporate espionage

Another problem that businesses face is industrial espionage. There are many examples of corporate spies stealing secrets from other businesses to gain a competitive edge in the marketplace. The problem has become so prevalent that Congress passed the Economic Espionage Act of 1996 making it a federal crime to steal trade secrets, giving law enforcement a new tool in fighting corporate theft.

Yet despite the new law, many businesses remain unaware of their vulnerability. Physical security is not enough. With all of the locks and digital access codes that we have installed in the workplace, our offices resemble Fort Knox. Yet many businesses throw important financial data in the garbage, where it that can be retrieved and then used by their competitors. Internal safeguards must be put in place so that corporate spies never have the opportunity to commit corporate espionage. Additionally, employees must be trained not to share proprietary information with anyone unless they know this person or unless a background profile or company profile has been performed.

Examples of alleged employee theft of trade secrets make the headlines regularly. Right now investigators are probing Reuters news agency officials over charges that a U.S. subsidiary used information stolen from rival Bloomberg. Last year, Kodak blamed a former employee for allegedly selling trade secrets to the filmmakers' rivals, including 3M Co.

The bottom line is that companies need to add business intelligence to their list of concerns. From employee background profiles to due diligence on all important transactions, companies need to invest a small amount of money up front to avoid losing a large amount at the back end. Business intelligence is a proactive, preventive measure that should be part of every business plan.