

## IT WOULD BE "CRIMINAL" TO DROP YOUR CRIME COVER

Efficient and effective risk managers keep an eagle eye on their insurance portfolio. In previous *Alerts* we have visited the topic of what a typical Crime or Fidelity policy covers; now it may be prudent to consider the other side of the risk equation: your potential exposure. In recent conversations with risk managers we have explored the range of potential perils in the 21<sup>st</sup> century, post-Sarbanes-Oxley world. This *Alert* distills those discussions as we outline the range of exposures a Crime policy can cover in the internet age.



## IDENTIFYING YOUR POTENTIAL RISKS

Theft of money, securities or other property by employees or outside individuals is a serious exposure for any company. The introduction of computer technology and the internet, however, have opened an entirely new avenue for employees or outside computer hackers to steal corporate assets. In addition, computer fraud holds significant potential for dishonest employees and others to cause catastrophic losses.

Management often oversimplifies their company's exposure to theft, limiting their thoughts to inventory or petty cash exposures, things that are physical in nature. While these are exposures that cannot be ignored, the overwhelming majority of crimes committed against

large organizations are much more sophisticated and result in losses in the millions of dollars.

**Ninety percent of all significant theft losses involve employees. These are often long-term employees who have found a gap in the internal control mechanisms designed to prevent such activity.** The variety of schemes utilized by dishonest employees is almost endless and although the use of prudent internal controls, internal audits and a diligent outside CPA firm can greatly offset the risk, even the most diligent firms have sustained large theft losses.

Exposures to theft by non-employees, other than losses involving collusion with a company's employees, are much more limited. Most theft by non-employees involves burglary or robbery, vendor fraud, forgery, counterfeiting, computer or wire fraud or extortion. Of these, vendor fraud has greatly outpaced the other perils in frequency and severity. Computer and wire fraud, however, hold the greatest potential for catastrophic loss.

The risk grows with each separate office or location where a firm does business. Operating located in many countries and locations requires organizations to rely heavily on local management to enforce internal controls that prevent and detect fraud. In most organizations, the controls become increasingly watered down the further the responsible parties are from the firm's leadership. The extra resources that would be required to strengthen enforcement, unfortunately, often take a back seat to meeting budget.

## CORPORATE EXPOSURES

- **Fraudulent fund transfers.** E-commerce has dramatically increased the possibility of catastrophic crime loss. With billions in various accounts, breach of computer security allowing fraudulent access to bank systems, unlikely as that is, could result in staggering losses. The largest paid loss of this type we know of to date exceeded \$40 million. The largest near miss was over \$200 million. (Underwriters tell us the hacker/employee overdraw the account by \$10 million, thereby stopping a fraudulent transfer that otherwise would likely have been completed.)
- **Purchase of nonexistent inventory or services.** Such losses involve a dishonest officer or manager submitting bogus invoices for goods and services that are never provided or whose value is grossly overinflated. One of the more publicized losses of this type involved a major metropolitan public transit authority that sustained a loss in excess of \$20 million when senior management knowingly purchased \$7 fittings for \$250 per piece and split the profits with a crooked contractor.
- **Mergers and acquisition.** The upheaval of a merger or acquisition may or may not be an occasion when corporate oversight and company loyalty waver and crime risks increase. More common in our experience is that post-acquisition review of accounts and operations will reveal crime that may have been committed by employees of the acquired company – in some cases for years. Your current Crime policy affords coverage for unknown prior acts involving newly acquired companies.



## TREASURY EXPOSURES

- **Management of a firm's investment portfolio.** This is a significant risk for most large, publicly traded companies. In some cases, this exposure can amount to billions in marketable securities. The Association of Certified Fraud Examiners (ACFE), in its 2006 *Report to the Nation on Occupational Fraud and Abuse*, reported that 2% of all firms surveyed not only sustained a loss involving the fraudulent transfer of securities by an employee/officer of the company, but the losses were severe – seven figures or higher.
- **Theft, destruction or misplacement of securities held on premises.**
- **Creation of fraudulent loans and lines of credit by a company officer.**

# FIELD OFFICES

- **Fraudulent lines of credit by local management.** In most global organizations, local offices and plants are likely to have a certain amount of autonomy in the management of finances, including establishing bank relationships in foreign locations. This creates the opportunity for fraud. While there have been many multimillion losses of this nature, one of the more publicized recent events involved an Asian brewer. A local finance officer took out \$78 million in loans from numerous local banks and used the funds to pay off gambling debts.
- **Padded payrolls.**
- **Vendor fraud.** Employees can collude with vendors to help the vendors charge for services, i.e., software, building maintenance, manufacturing, etc. that were never performed or were performed at exorbitant prices.
- **Bookkeeping and accounting schemes.** Accounts can be manipulated to hide improper payments or purchases.
- **Burglary or theft of inventory.** Highly marketable items that are easily moved in the black market are the most frequent targets of theft.
- **Acceptance of bogus warehouse receipts.**

# REPUTATIONAL RISK

**A multimillion theft loss to any organization is at best an extreme embarrassment to the company and at worst, for publicly traded companies, a lasting blow to investor confidence in the company's management.** Reputational damage can have a material impact on the company's market capital and bottom line. When such losses occur, it is common for management to announce publicly that the company maintains Crime insurance to address such losses. Not only does the coverage soften the impact to the company's bottom line, but it helps assure investors that the company was prudent enough to make allowances for such events, unlikely as they may appear.

# ERISA REQUIREMENTS

Many Crime programs automatically include coverage for the pension and welfare benefit plans that are required to be bonded in accordance with the Employee Retirement Income Security Act (ERISA). In as much as the coverage is mandated by law, should the Crime policy be dropped, many organizations would still need to purchase Crime coverage for each of these plans.

While the examples we have provided do not take into account all of the possible loss scenarios we have seen clients face, they do identify the most frequent types of losses experienced by large organizations. We believe they constitute a compelling argument for maintaining and even improving your Crime program.

# REGIONAL CONTACTS

## **Atlanta, GA**

CharlesMaxell  
P- 404 224 5123  
F- 404 224 5001  
charles.maxell@willis.com

## **Boston,MA**

David Goldstein  
P- 617 351 7498  
F- 617 351 7430  
david.goldstein@willis.com

## **Chicago, IL**

Brian Gauen  
P- 312 621 4855  
F- 312 621 6870  
brian.gauen@willis.com

## **Denver, CO**

Jim Iacino  
P- 303 218 4039  
F- 303 218 4058  
jim.iacino@willis.com

## **Los Angeles, CA**

Chris Crawford  
P- 213 607 6294  
F- 213 607 6301  
chris.crawford@willis.com

## **New York, NY**

Steve Leggett  
P- 212 915 7901  
F- 212 519 5460  
stephen.leggett@willis.com

Steve Pincus  
P- 212 915 7940  
F- 212 519 5460  
steve.pincus@willis.com

## **Radnor, PA**

Matt Schott  
P- 610 254 5642  
F- 610 254 5600  
matt.schott@willis.com

## **San Francisco, CA**

MichaelMahoney  
P- 415 291 1535  
F- 415 982 7978  
mike.mahoney@willis.com

*Executive Risks Alerts and Newsletters provide a general overview and discussion on a wide range of topics. They are not intended, and should not be used, as a substitute for legal advice in any specific situation.*