Crime Insurance—The Other Property Policy

April 2009

"Lack of money is the root of all evil."
-George Bernard Shaw, Irish dramatist and socialist

"Obviously crime pays, or there'd be no crime."
-G. Gordon Liddy, Republican mastermind of the 1972 break-in of the Democratic National Committee headquarters leading to President Richard Nixon's Watergate scandal.

"Organized crime in America takes in over $40 billion dollars a year and spends very little on office supplies."
-Woody Allen, U.S. movie actor, comedian, and director.

"We have seen the enemy and it is us"
-Pogo, main character of a long-running (1948–75) daily comic strip, created by Walt Kelly.

Even in the best of times people steal. The economic climate of 2009 will certainly create the atmosphere for many people to rationalize dishonest ways to make ends meet. Others will view their dishonest activities as business as usual and continue to look for an easy buck the old-fashioned way: take it from someone else.

by William K. Austin
Austin & Stanovich Risk Managers, LLC

White-collar crime should be of great concern to all risk management professionals. It can be occurring now, right in front of us. People we trust. How many times have we read in newspapers of the kind old bookkeeper, polished senior executive, parish priest, well-respected city manager, and other people we deal with day to day who are arrested for stealing from their employer or otherwise taking funds that did not belong to them?

Computers are an integral part of the financial accounting and transaction infrastructure of all organizations today. Organized crime in 2009 is not necessarily limited to that portrayed in the HBO series "The Sopranos." It is composed of organized individuals from around the world using state-of-the-art technology to steal funds by hacking and other means of penetration into an organization's accounting and finance technology systems.

When asked about internal procedures, many organizations state, "It cannot happen to us. Bill has been our controller for years. We would know if something was amiss." Yet, organizations seem to chance their profitability by not spending enough time ensuring that the peril of theft is minimized as much as possible. To paraphrase Pogo, "The white-collar thief looks just like you and me." Many risk management professionals seem to overlook or downplay the importance of crime risk management and appropriate use of crime insurance.

Theft

The peril of theft can pose loss to an organization as disruptive and costly as a wrongful termination, fire at a critical location, or a claim for products liability. "Theft," for purposes of this article, is defined as "the unlawful taking of property to the deprivation of the insured" and is the definition used in the Insurance Services Office, Inc. (ISO) Commercial Crime Policy (CR 00 23 05 06) (Loss Sustained) and Commercial Crime Policy (CR 00 22 05 06) (Discovery). Burglary (an act of breaking and entering a building with the intent to commit a crime) and robbery (the unlawful taking of property from care and custody of another threat of bodily harm), while significant exposures to many organizations, are not the focus of this article.

How Much Theft Coverage Is Provided by a Commercial Property Insurance Policy?

At what point does a crime policy insure the peril of theft that may not be insured by the commercial property policy? We begin with an examination of ISO property insurance forms: Building and Personal Property Coverage Form (CP 00 10 0607); Causes of Loss—Basic Form (CP 10 10 06 07); Causes of Loss—Broad Form (CP 10 20 06 07); and Causes of Loss—Special Form (CP 10 30 06 07). The reader is advised to review his or her own property polices as many insurers use a filing independent of ISO or use portions of an ISO form.

What Can Be Stolen from an Organization?

Assets can be stolen. Assets can be tangible (i.e., furniture or fixtures) or intangible (i.e. intellectual property). For the purposes of this discussion, we will deal with tangible assets defined by ISO as "personal property" which may range from office contents, furniture, and fixtures; inventory (raw, in process, finished); and cash and securities. The building and property coverage form declares specific tangible property is not covered: Accounts, bills, currency, food stamps, or other evidences of debt, money, notes or securities. Lottery tickets held for sale are not securities. If property is defined as "covered property" in commercial property insurance how is the peril of *theft* addressed in the three causes of loss policy forms?

The basic form and broad form provide coverage for loss from named perils. Neither form includes *theft, burglary, or robbery* as covered perils, but each do allow coverage for damage to a building caused by *burglars* breaking in or exiting the premises. The causes of loss—special form is thought of as an "all risk of loss" form except for perils specifically excluded. Theft is a covered peril within the special form but coverage is subject to exclusion for: Dishonest or criminal act by you, any of your partners, members, officers, managers, employees (including leased, employees), directors, trustees, authorized representatives or anyone to whom you entrust the property for any purpose: 1) acting alone or in collusion with others; or 2) whether or not occurring during the hours of employment. This exclusion does not apply to acts of destruction by your employees (including leased employees); but theft by employees (including leased employees) is not covered.

What Does This Mean?

No coverage for theft is provided in the basic or broad form whether it is theft of office equipment or cash and securities. While theft is a covered peril in the special form, loss is limited to theft of only a portion of tangible property; no coverage exists for tangible assets, such as money and securities. In this article, we will examine how ISO crime policies provide theft coverage to replace that excluded in commercial property policies.

ISO has several crime insurance policy forms available for an insured. Coverage is available on a *loss sustained* basis (CR 00 23 05 06) or *discovery* basis (CR 00 20 05 06). The difference in forms is similar in concept to occurrence and claims-made coverage triggers in liability policies: loss sustained is akin to an occurrence trigger, while discovery is similar to claims-made triggers. We use the ISO commercial crime policy loss sustained form as the basis of discussion within this article. The reader is advised to review his or her own crime insurance polices as many insurers use a filing independent of ISO or use limited portions of the ISO form.

From this point on we need to follow the risk management process for theft exposures and not rely on what we may have done for other covered property. The cash and securities loss exposure is different than the other tangible property exposures, and thus, risk financing treatments will need to be different as well. When we think of crime exposures and theft, we need to consider theft by an employee of an organization as well as theft by other than an employee.

Exposure Identification

It is, of course, crucial to identify crime exposures facing the organization. This includes identifying the entities and the dishonest acts to be covered.

Covered Entities

What entities within the organization have a crime exposure? Most entities have a crime exposure even if it has limited tangible assets (i.e., no building and limited office contents) as in a service business such as accounting firm or a "paper corporation" that has assets of only cash accumulated for tax purposes. The risk manager must understand the crime exposure of each entity to ensure coverage will be arranged correctly. While an omnibus clause may cover all entities of the organization, it does not replace the due diligence needed from the risk manager to ensure that exposure and coverage are addressed in the most appropriate manner.

Oftentimes, employee benefit plans are overlooked as "entities" that have a crime exposure and then are not properly identified in the crime policy. The Employee Retirement Income Security Act (ERISA) is a federal statute that applies to employee benefit plans such as 401(k), profit sharing/pension, medical, dental, life, and disability plans. ERISA has many requirements for a plan sponsor (i.e., employer) including specific requirements for insurance. The law requires that any person, not just an employee, who handles funds of an ERISA plan must be bonded. The ERISA bond requirement is a limit of 10 percent of the funds handled, subject to a minimum limit of $1,000 and a maximum limit of $500,000. A

limit of $1 million per plan is required by ERISA if the plan holds employer securities other than through a pooled investment vehicle. Employee benefits liability coverage (EBL) found in a general liability policy or ERISA fiduciary liability insurance, sometimes referred to as pension trust liability, do not satisfy the ERISA requirements for crime insurance.

Appropriate due diligence should be done by the risk management professional to ensure ERISA requirements are understood and addressed as needed for employee benefit plans sponsored by any organization. The employee theft coverage provided by an ISO commercial crime policy can be used to satisfy ERISA if each plan is included as a named insured. ERISA also has some other requirements that are included within the ISO commercial crime policy. If your organization is not insured by a recent ISO crime policy, you will need to review it to see if a separate ERISA compliance endorsement is needed.
ERISA compliance in a crime policy is often confused with both EBL and fiduciary liability insurance. ERISA requires only employee theft coverage; it does not require any other coverage—not EBL or fiduciary liability. Complying with ERISA in the crime policy does not provide any coverage to the organization for third-party exposures that may arise out of failures in plan administration or breach of fiduciary duty. EBL and fiduciary liability policies are available for the third-party liability exposures created by sponsorship of an employee benefit plan.

Dishonest Acts by Employees or Non-Employees

There are eight coverage sections to an ISO commercial crime policy. Only one section is for employee theft; the others provide coverage for loss caused by theft by other than employee. Coverage for employee theft is broad as it includes coverage for loss by forgery or alteration, computer fraud, and funds transfer fraud. Theft by a non-employee can be insured for forgery or alteration, computer fraud, and funds transfer fraud. The insured organization is given an option by ISO to insure its employee and non-employee exposures by different coverage limits.

Exposure identification for theft exposures is critical to arranging appropriate crime insurance, especially since coverage can be arranged quite differently for that caused by an employee or non-employee. An organization's risk manager must understand how it may use its employees for certain functions and how its financial operations and transactions may be penetrated by non-employees. Exposure identification can become complex since ISO defines "employee" in a broad sense, and organizations today may use the services of a non-employee in a manner similar to how it actually uses its employees. Therefore, it is critical for the risk manager to understand the differences.

How does a risk manager determine who an "employee" is for purposes of crime insurance? First, carefully review the definition of "employee" in the crime insurance policy used. Then develop a process that allows the risk manager to interact with all parts of the organization: operations—hire employees; human resources—manage employee services, such as job performance and employee benefits; procurement/purchasing for outsourced activities; and finance and technology to understand how an "employee" may be able to circumvent policy and procedure to steal from the organization. Only when the overall "employee" and "non-employee" exposures are understood can the risk manager begin to quantify the various exposures and determine the appropriate use of commercial crime insurance. This may be the most important step in the crime risk management process.

Conclusion

A risk manager needs to approach crime risk management and use of insurance differently than other processes used for commercial property insurance. Only when employee and non-employee exposures are understood can the risk management professional determine the appropriate arrangement of crime insurance for the insured organization. We will review crime coverage triggers, coverages available in the ISO crime policy, and how to establish dollar limits by coverage section in Part 2 of this article.

Contact information:
William K. Austin, Principal
wkaustin@austinstanovich.com
Telephone 888-540-7604 Fax: 888-650-7803
www.austinstanovich.com