Risky Business
Manage crime, fraud, and theft

By Timothy Koenig, CPCU, CIC

“Is that your signature Ralph?” The bank manager’s spread a fan of cancelled checks on his desk, sliding one at random toward you. He’d called an hour or so before, asking if you’d stop by to give him a “bit of advice.”

“Odd,” you’d thought, especially since neither you nor your company had any dealings with the man’s bank, but his voice had a this-is-serious tone that now had you bending forward to look at the image of one of score of your company checks—totaling many thousands of dollars—each with signatures that looked nothing like yours …

Your building burns. You wreck a company truck. Your product causes an injury or damage to another party’s property. Your employee suffers a workplace injury. These are easily recognized and identifiable business risk losses which can adversely impact your company’s operations and finances. And, through appropriate risk management techniques,
including insurance, these losses can usually be effectively controlled and managed.

Somewhat less recognizable, but with the potential to cause significant adverse impact to your business, are losses which may result from fraud, theft and crime. Losses can be internally-caused or come from outside the organization. Examples of internal losses include employee theft of money, property or theft/misappropriation of trade secrets or operational processes and may also include the manipulation of production, sales or financial information, to the benefit of the offending employee(s). Employees may also have the ability to access the records or assets of customers or to develop schemes to influence customer behavior and obtain confidential information.

Examples of externally-generated fraud which can impact your business include theft of money, equipment or products (retail theft); check and document forgery; credit card misuse/theft; wire transfer fraud; contract fraud and intentional representation; and the relatively new, but greatly expanding exposure of cyber-related theft of valuable company data, including confidential customer and employee records and information, which also can result in significant third-party liability claims.

While the total cost of fraud-related loss is difficult, if not impossible to measure, the cost to U.S. companies and the overall economy are staggering and estimated by the Association of Certified Fraud Examiners, to climb well into the high, multi-billion dollar range. And in addition to the direct dollar costs of fraud/crime losses, there are significant indirect costs, including the costs to prevent, investigate and manage these crimes, as well as the emotional, morale and loss of reputation costs to businesses and their employees.

Risk management is the process by which an organization can prepare for and then deal with various business, operational, financial and hazard risks which can impact the company’s health and ability to survive and prosper. The risk management process which can be applied to potential exposure of crime and fraud-related losses is the same as for any other type of potential hazard which could impact a business. The process includes …

1. Identify the loss exposure
2. Analyze the exposure for its potential impact on the business
3. Select an appropriate risk management technique(s)
4. Implement the selected risk management technique
5. Monitor the results of the risk management program

Loss exposure identification

There are many techniques an organization can use to identify fraud, crime and other similar loss exposures. The primary technique involves the use of specialized fraud/crime risk assessment questionnaires which can be obtained online or from various fraud prevention organizations or from insurance companies which sell products and services to specifically address these exposures.

In completing a risk assessment questionnaire, a company should involve and solicit input from key employees representing all major operating aspects of the business, including Finance, Operations, IT, Transportation, Purchasing, Human Resources and General Administration. Obviously, the size of the organization will dictate the number of different
people involved in the assessment, but again, all major operating functions should be included.

In many cases, it may make sense to involve outside specialists and/or trusted business advisors, including your company’s accountant, banker, attorney, outside IT consultants and insurance/risk management representatives. Such specialists may be able to offer particular expertise on the topic or provide examples of loss exposures based on past experience with other clients or colleagues.

Analyzing the exposure’s impact on the business

Once a loss exposure has been identified, the next step in the risk management process is to analyze the exposure’s potential impact on your company. The key measures in this analysis are Loss Frequency and Loss Severity. As with the exposure identification process, questionnaires and assessment tools can be completed, with the input of key operating units of the company and assistance from outsiders.

Loss frequency is the number of times a loss is expected to take place in a given period of time and can be expressed as:

1. Almost never—extremely unlikely to ever take place
2. Slight—could happen, but not likely
3. Moderate—happens occasionally
4. Definite—happens regularly

Loss severity is the maximum dollar potential amount of the loss and can be expressed as:

1. Slight—Relatively low amount, which the company can typically afford to sustain with little negative impact
2. Significant—Loss will cause negative impact and some part will have to be financed, either before or after the loss takes place
3. Severe—The loss is potentially catastrophic and could cripple the company unless most or all of the cost is financed.

Tying together the loss frequency and loss severity will give your company a way to assess the financial impact of a loss exposure. Normally, loss frequency and loss severity tend to be inversely related and more severe losses typically have the potential to take place less frequently. For example, retail theft and credit card fraud losses may be frequent for some types of businesses, but normally, the dollar amount of each loss is relatively low. On the other hand, fraudulent wire transfers and employee theft of valuable trade secrets are rarer, but have the potential to have a greater negative financial impact on the company. The creation of a matrix, with loss frequency measures on the bottom and loss severity measures on the side can be used to assess the total impact of a loss exposure and help determine the best technique(s) to manage the exposure.
Selecting risk management techniques

A primary risk management technique is Risk Control, which is a conscious act or decision to take steps to reduce a loss exposure’s frequency and/or severity. Methods of risk control include avoidance, loss prevention and loss reduction.

1. Avoidance is a risk control technique which involves taking action to make sure the loss exposure can’t occur. While avoidance is a very effective in reducing losses, it may not be practical or possible, since many loss exposures tend be a natural part of conducting a business. And, in the case of fraud and crime losses, these are perpetrated by third parties and consequently, difficult to avoid.

2. Loss prevention is a risk control technique which reduces the potential frequency of a loss. For example, a company could decide to conduct detailed background checks on all new employees, suppliers or vendors. Or, all sensitive electronic files could be protected with strong passwords, which are frequently changed. In the case of fraud-related loss exposures, steps may be able to be taken to have your attorney carefully review all contracts or agreements, especially with new customers or vendors and to conduct online research on these companies. There are many good crime and fraud prevention checklists which are available online or from CPA firms, banks, law firms or insurance brokers.

3. Loss reduction is a risk control technique which reduces the potential severity of a loss exposure. For example, a company can limit the amount of cash carried by outside sales or delivery employees to reduce potential theft losses. Or, a company can establish bank procedures to reduce the limit for wire transfers.

Risk Financing is a risk management technique which involves making a conscious decision as to how the loss exposure’s cost will be handled, either before or after the loss takes place. With this technique, losses can be either Retained or Transferred.

1. A company may make the decision to retain the potential cost of a loss by generating funds from within the organization. Retention can be planned or unplanned; complete or partial; funded or unfunded.

Planned retention takes place when a company has identified and analyzed a loss exposure and makes the decision to internally absorb the potential costs, either because that’s the most cost effective method or because there are few, if any, alternatives. Planned retention works best for low severity losses or for companies with significant financial resources. In the case of small theft losses, many companies will make the conscious decision to internally fund these losses, since they normally will not cripple the organization and there may be no other cost effective alternative.

Unplanned retention takes place when a loss exposure has not been properly identified/analyzed and funding has not been considered. Unplanned retention can be catastrophic and cripple a business if the cost exceeds the company’s ability to immediately fund or transfer the loss cost.

Complete retention takes place when the cost of the loss is totally assumed by the company’s internal finances, either planned or unplanned. Partial retention takes place when a portion of the cost of a loss is handled internally and the remainder is somehow transferred outside the company. Provided the retention decision is planned, the extent of the
retention will be based on the expected frequency and severity of the loss and the company’s financial strength.

If the company decides to retain all or a portion of the loss, the cost can be handled by pre-loss funding, with funds that have been saved and set aside; with current loss funds which are generated at the time of loss; or, with post-loss funds which are arranged after the loss—typically borrowing.

2. Risk Transfer is a key risk financing technique which involves either insurance or non-insurance transfer of the potential economic loss associated with exposures such as fraud and crime losses.

Through the purchase of insurance, a company can transfer a substantial portion of the financial risk of a loss to an insurance company, in exchange for the payment of a premium. In other words, a relatively small, certain cost is exchanged for a possibly large, uncertain cost. Insurance is a very common risk financing technique for many crime-related losses, including both employee and non-employee theft of money and physical assets; the fraudulent signing of checks or negotiable instruments; wire transfer fraud and unauthorized computer access to funds; and more recently, losses involving the theft or manipulation of sensitive or confidential data and records, including employee, customer and vendor information, as well as the resulting legal liability a company may have from the failure to properly safeguard this information.

Keep in mind, insurance companies are in business to analyze exposures and make a profit by assuming a predictable portion of the risk of loss. Consequently, the more exotic, unpredictable or potentially severe the exposure, the more costly the premium. And, in some cases, insurance may not be available, at any cost. Also, insurance policies for these types of losses tend to be non-standard and can vary greatly in terms, conditions, coverages and exclusions. It is very important to carefully review and tailor policies to a company’s specific needs, in order to successfully transfer risk using insurance.

Non-insurance transfer of financial risk may often be the preferred, least costly, or sometimes the only way for a company to transfer many types of crime and fraud-related loss exposures. The most common form of non-insurance transfer of potential financial loss is accomplished via contracts, additional insured and indemnification requirements. Through the use of contracts, a company may be able to transfer a substantial portion of risk back to the other party. Contracts may require the other party to purchase the necessary insurance coverage and/or to indemnify the party suffering loss, if caused by the other party’s negligence or actions. Typically, the company with the most clout will be in the position of dictating terms and being able to push exposure to the other party.

Implementing the selected risk management techniques

The crime and fraud loss exposures have been identified and analyzed for their potential impact on the company; the risk management technique(s) have been selected; and the company must now begin the implementation of these techniques.

Depending on the size of your company, implementation may be as simple as having the company owner or president make the determination to start the process, or it may involve communication and coordination between operating departments and the determination of various levels of responsibility and authority. For example, who within the organization is going to decide how and where to obtain background checks on employees, suppliers and vendors? Or, who is going to work
with the company attorney to review contracts, agreements and legal documents? And who is going to work with the company’s insurance broker to obtain, review and select coverage proposals?

**Monitoring results of the risk management plan**

Determining the success of your risk management techniques may be difficult, depending upon the expected frequency and severity of losses. Reductions in high frequency/low severity losses are going to relatively easy to measure; however, the success of techniques established to reduce low frequency/high severity losses are determined by not having any of these losses or minimizing their impact on the company’s finances.

As with all successful business plans, a risk management plan can’t be established and then forgotten. In addition to monitoring plans for success, it’s important to regularly review the plan for any possible changes or modifications, including …

Have new exposures developed, based on new operations or activities? For example, the establishment of a new operating division, with new supplier agreements.

Have there been changes to the potential frequency or severity of any existing exposures? For example, the company has started obtaining and storing the credit card information of customers.

Have different or new risk management techniques become available or more cost-effective? For example, a new type of insurance product becomes available and/or there is a reduction in premium.

**The indirect cost of crime and fraud losses**

Unfortunately, in the case of many crime or fraud-related losses, there may be significant indirect costs to a company which cannot be insured or transferred. This includes the costs of investigation, research and the time spent by owners, supervisors and other employees to manage these losses. Also, in the case of losses which may be caused by long-time, trusted employees, there can be a very negative impact on the morale of the remaining, effected employees. And losses which result in the theft of valuable trade information or intellectual property can cause significant damage to your company’s reputation, as can theft or fraud losses perpetrated by your employees on other parties.

In the true case of that company owner confronted by the bank manager with forged checks: the embezzlement was preventable. That expensive lesson’s focused management’s attention upon managing risk. Particularly from the unexpected actions of even long-time, highly trusted employees.

They’ve learned that crime and fraud losses cause immeasurable negative impact on businesses and individuals, even as in this case, threatening the future of the company. While many losses may be unforeseen and nearly impossible to avoid, a business can be proactive in trying to identify and analyze possible exposures and take steps to control, reduce or transfer potentially catastrophic costs through the use of properly selected and implemented risk management techniques. With risk as with every key decision—remember, managers manage.
Tim Koenig (tekoenig@ehd-ins.com) is an assistant vice president and account executive for Engle-Hambright & Davies Inc., one of the Mid-Atlantic region’s largest insurance and employee benefits brokers, headquartered in Lancaster, PA. He has more than 30 years experience in the development, sales, and management of commercial insurance programs for medium-large businesses and organizations.