Group Project. In-Depth Risk Analysis

Crime/Employee Theft

RMI 2901. Introduction to Risk Management - Dr. Marc Ragin

Group 1: Tessa Kaye, Ngoc (Nathan Pham), Arlo Antle, Morris Scott
4-18-2016

Content

Introduction

Employee theft is a major risk of crime that deteriorates the operations of many businesses. While many people may think that most theft losses come from non-employees, 90% of all significant theft losses come from employees (Willis North America). Each year, a company loses on average 5% of its profits due to fraud and theft (Karpp). Without the proper implementation of risk management practices, organizations can suffer huge financial losses. The *Report to the Nations* by The Association of Certified Fraud Examiners (ACFE) projects a potential global theft loss of $3.7 trillion annually for organizations. Moreover, employee theft is harmful to the working environment and culture of a firm. This report examines the risk of employee theft through defining its exposures, perils, hazards and classification. In addition, the recommendation of risk management options will be proposed in detail. More specifically, suggestions will be put forth concerning loss control and loss financing methods for companies of different industries with distinct risk exposures.

(1) Description of risk

Employee theft is a risk of crime that many organizations are facing. It can be defined as any activity of an employee who steals, uses, or misuses company assets without permission. It is important to refer to the stolen property as company assets in order to emphasize that these items are not limited to cash. Table 1.1 is an overview of employee theft's exposures, perils, hazards and classification.

Table 1.1. Overview of employee theft

Exposures	- Tangible property (money, equipment) - Intangible property (trade secrets, time, computer data, intellectual property)
Perils	- Larceny, embezzlement, skimming, fraudulent disbursements, stealing of business opportunities
Hazards	- Employee hiring processes that lack proper screenings - Lack of an internal control system - Low morale within the workplace - Lack of an enforced policy
TRM risks	- Property risk - Net income risk
ERM quadrants	- Hazard risk - Operational risk
Other risks/quadrants that may influence this risk	- Employee turnover (operational risk) - Internal audit risk (operational risk)
Classification	- Pure - Static - Particular

Exposures, perils, and hazards

Assets that are at stake when considering this type of risk include both the company's tangible and intangible property. Examples of tangible items include the company's money, equipment, inventory, supplies, or merchandise (if it is a seller of goods). However, the intangible property that is misused by an employee can be more valuable than tangible items in some cases. This property includes a firm's time, intellectual property, and trade secrets. An employee theft scheme that has been on the rise in recent years is computer fraud. This occurs when employees copy data containing trade secrets or other important information from employers and for their own benefit, distributes this to other individuals or organizations in exchange for money.

If a company experiences employee crime loss, there are many perils that are possible immediate causes to the loss. Perils that result in employee theft are acts like larceny or embezzlement, skimming, fraudulent disbursement, and stealing business opportunities. These fraudulent actions by employees will create a direct loss for their employer. Larceny results from employees' stealing from the company without any authorization, and hence differs from embezzlement. An embezzler takes away the property that they are trusted and legally authorized to access. Both larceny and embezzlement occur after the business has received and recorded the property. In contrast, skimming is stealing that occurs before the company has recorded the asset, and can be referred to as an "off the books" crime. If an employee engages in fraudulent disbursement, it generally looks as though he or she is participating in legitimate business activity. However, that employee is using company systems illegally for their self-benefit, including engaging in fraudulent fund transfers, check tampering, billing schemes, purchase of nonexistent inventory or services, payroll schemes, and expense reimbursement schemes. An employee stealing company's business opportunities is a peril that differs from those previously mentioned, because it causes a loss of intangible property to the firm that employs them. Losses from this type of peril are comprised of stolen, high-value information.

Hazards related to employee theft risk increase the frequency and severity of a risk but are not the direct causes to employee theft. Employee hiring practices that do not properly screen the criminal backgrounds of prospective hires are a hazard related to this risk. This initial screening is essential to any business; there are too many applicants who attempt at making false claims on their resumes in addition to trying to cover up past criminal records. In fact, 80% of job seekers lie on their resumes (Cream.hr). However, a survey of 2,500 hiring managers constructed by CareerBuilder shows that only 56% of these managers have caught candidates

lying on their resumes (White). As a result, 24% of people who lie on their resumes still get hired. With 119.3 million current full time employees in the United States, the 28.63 million people who have lied on their resumes can expose their companies to employee theft risk because their lying is a display of low morale (The Employment Situation – March 2016).

Another hazard increasing the likelihood of employee theft crimes in companies is when they have an absence of proper internal controls. Internal controls act as a system to assure that company goals are being achieved through the work of its employees. One person is not able to make a transaction without involving another employee, which causes employee theft to be more difficult to commit. According to the ACFE's reports, organizations who were victims to employee theft who had implemented some sort of internal control had losses that were significantly less than those who had not (AFCE). Internal controls that are effective will result in employee compliance.

There is a correlation between low employee morale and theft in the workplace. Regardless of the reason, low morale can cause many problems for an organization. With implementations like internal controls and other deterrents employee theft is harder to commit. However, employee morale that is persuaded from the top down is equally important because employees are not motivated to do their jobs and follow company policy in an environment where the outcomes for the firm do not matter to them. According to the Gallup Organization, there are 22 million actively disengaged employees in the United States, costing the economy as much as $350 billion dollars per year in lost productivity (Ali). It is vital for companies to foster business environments with high morale because their employees are much less likely to commit theft if they feel that they are proud about taking part in meaningful work.

The level of importance of effective workplace policies is on par with how valuable enforcing those policies is. If a firm does not establish policies that act as a model to employees for their expected behaviors and other work standards, it puts itself at risk for employee theft. When firms have implemented policies regarding employee theft specifically, employees are deterred from committing theft in the workplace because they are aware of their punishments. Furthermore, these policies can protect a company from legal claims that may occur. Making employees aware that they will be terminated at their first offense of detected employee theft will protect a firm from wrongful discharge claims (BizFilings). In order to give employees an improved quality of work life, companies should make it their priority to establish the most appropriate policies and have an employee culture that is aware of them.

Classification of risk

Employee theft can be classified as a pure, speculative and static risk that falls under both categories of traditional risk management (TRM) and enterprise risk management (ERM).

Employee theft risk is considered to be pure because there are only two states of the world in an incidence of employee theft, either a loss or no loss. If all employees responsibly manage company property and information, companies will not suffer employee theft losses. On the other hand, when there are dishonest employees who want to take advantage of their authorizations and steal from the company, the company will have a loss to manage. As a company experiencing theft committed by its employees will never result in a gain for a firm, an insurance market exists to help firms cover and finance these losses. Employee theft can be further classified as a particular risk, as there is no correlation of losses occurring at the same time among firms in the same country, industry or geographic location. A theft incident that happens to one firm does not affect the frequency or severity of theft for other firms. Finally, this

criminal risk is static as employee theft has not changed dramatically in the past twenty years. While the platforms that people have used over time to steal have changed, the basic characteristics of the risk have remained the same. The motive for these crimes, which is greed, has remained constant. Moreover, new legal regulations can change depending on the new schemes or technology but they are passed with all the same underlying rationale of restricting employees' uncontrollable selfishness. Therefore, the overall frequency and severity of employee theft have remained static.

Moreover, employee theft risk can be classified as a traditional risk management risk, more specifically as property and net income risks. The company has a legal interest in the property at stake when considering employee theft. The firm's ownership interest lies in all of the assets that can potentially be stolen, tangible and intangible. All property, either equipment or trade secrets, serve as capital for a company to produce and develop. Therefore, the ownership of the property has numerous meanings to a company. Consequently, the ownership interest that the firm has in their property is also highly related to net income risk. The ultimate goal of many businesses is to make a profit, which is the subtraction of expenses from revenue. The loss of property will directly affect the company because it can increase company expenses and decrease revenues. Repair and replacement costs are also considered in the company's primary loss. The secondary loss is the cost of terminating the employee offender and hiring a new employee. The process of replacing lost property or training new employees takes time and may cause business interruption, which further increases losses in revenue.

In addition to its classification as property and net income risks under TRM, employee theft is also an ERM risk under both the hazard and operational quadrants. Employee theft risk is usually considered to be a hazard risk, arising from property loss exposures. However, this is

also an operational risk, resulting from the day-to-day operations of a company. When viewing employee theft as an operational risk, a company is able manage their risk through risk control and risk financing methods available for ERM risks. As an operational risk, employee theft is closely associated with the people, systems, processes and controls within a company. The working culture among employees has a direct impact on the "people" category of the risk. Within an engaging environment, employees will feel more responsible for the company's property and are less likely to steal from the company. By understanding the psychology of employees and the importance of working environment, a company can better develop and implement loss control practices. In addition, the finance, accounting or supply chain systems of a company can either increase or decrease their risk of employee theft. If a process, such as funds transfer, is not properly designed for managing and supervising, it will open up the opportunity for employees to steal from their company. Even with well-designed processes, proper control procedures would make a positive change in managing the risk of employee theft.

As employee theft can be classified under both the hazard and operational quadrants of ERM risk, other ERM risks such as employee turnover can influence this risk. Within the operational quadrant, employee turnover has a substantial impact on employee theft. When a company has a high turnover rate, its employees generally remain working for shorter periods of time. As a result, they are less engaged and act less responsibly when handling company property. In that environment, low responsibility and engagement level can lead employees to feel less guilty for stealing from the company. Consequently, the frequency and potentially the severity of the employee theft risk can increase. In contrast, if a company has a turnover rate that is too low, employees who have worked for the firm for an extended period of time could potentially become less engaged and less invested in their work, posing their company a threat of

employee crime. Another risk related to employee theft is internal audit risk, which is also an operational risk. Internal auditing is a process that checks all company systems and controls. If a company cannot properly manage its internal audit risk, the severity and frequency of employee theft are more likely to increase. For instance, a company with a high employee turnover can still manage its employee risk through internal auditing. With a good internal audit system, the company is better able to supervise and notice suspicious activities from employees. Considering other ERM risks that influence employee theft gives a company a more holistic view of their risk portfolio.

All of the aforementioned information makes up the classification of employee theft risk. Considering employee theft under TRM as property and net income risk and under ERM as hazard and operational risk, a company can better evaluate the risk and develop appropriate risk management method.

Risk Identification Methods

In order for the risk management function of a company to accurately evaluate and manage its risk of employee theft, it must identify its risk. Most cases of employee theft are detected by accident or come to the attention of the employer via the notification of another employee. According to the American Society of Employers, the average time that it takes for an employer to detect a scheme of employee theft is 18 months (Murphy). In order to minimize this time, companies have several methods that ascertain their risk of employee theft. The first step that a firm takes is screening its applicants systematically before they are hired. A thorough background check consists of scrutinizing the applicant's criminal history, civil history, driver license violations, past employment, and references (Schaefer). In addition to screening its

applicants, the company should screen its vendors. By reviewing its contracts for its vendors, the company is further able to detect fraud occurring within the company.

Firms can further identify their employee theft risk by running audits to examine the financial records of employees with access to the company finances. These audits can be irregularly scheduled to surprise employees or be handled by a third party. Audits are part of the company's internal controls. Internal controls encourage effectiveness, decrease risk of asset loss, and help to safeguard the reliability of financial statements and obedience of laws and regulations. To ensure that the system of internal controls that the company has is efficient and covers all functions of the company, it can use flow charts to display its auditing process. A firm can further detect its risk of employee theft by requiring its employees to submit employee reviews for their coworkers. Because some companies can be very large in size, these surveys can be very helpful in giving the employers a better idea of the behaviors of its employees.

Frequency, severity and risk map of employee theft

The risk of employee theft is considered to have a low severity and high frequency. According to the ACFE's reports, 75% of employees have stolen at least once from their employer. 51% of these offenders repeat their criminal behaviors. These numbers clearly demonstrate the high frequency of employee theft. Concerning severity, a report shows that the annual amount stolen from U.S. businesses by employees is $50 billion (Employee Theft

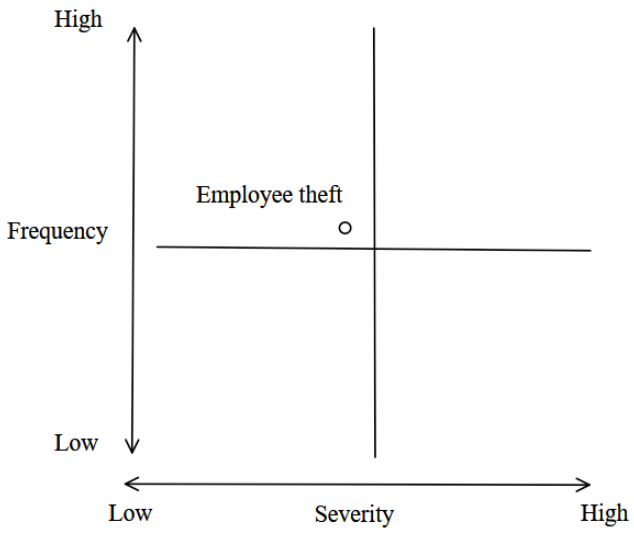


Figure 1.1. Risk map of employee theft

Statistics). Furthermore, employee theft was the reason for 33% of business' bankruptcies in the United States. However, on average, the losses from employee theft only account for 7% of the annual revenues that are lost to theft of fraud. Therefore, employee theft is a risk of low severity. The frequency and severity of employee theft are shown in Figure 1.1.

Frequency and severity of different employee theft exposures

Figure 1.2 communicates the variance of the frequency and severity of the acts of larceny, embezzlement, skimming, fraudulent disbursement, and stealing business opportunities. According to the ACFE's reports, acts of larceny result in a median loss of $75,000 per year and had a reported amount of 99 cases out of a sample of 1,148 businesses (Karpp). Although there is no specific data on the frequency and severity of embezzlement, it can be considered to be more severe than larceny, due to embezzlement being an act of stealing from an employee who is trusted and legally authorized to access the property. Skimming is a crime with a severity of $80,000 in median losses and a frequency of 159 cases out of the 1,148 businesses surveyed, both greater than the frequencies and severities of larceny or embezzlement. It is more difficult for a firm to detect assets that have never been recorded. Fraudulent disbursements had the next highest frequency and severity of the employee fraud exposures, with a frequency of 168 cases and a severity of a median loss of $163,000. This can be due to fraudulent disbursements appearing to look like regular business conducted by the company. Finally, the

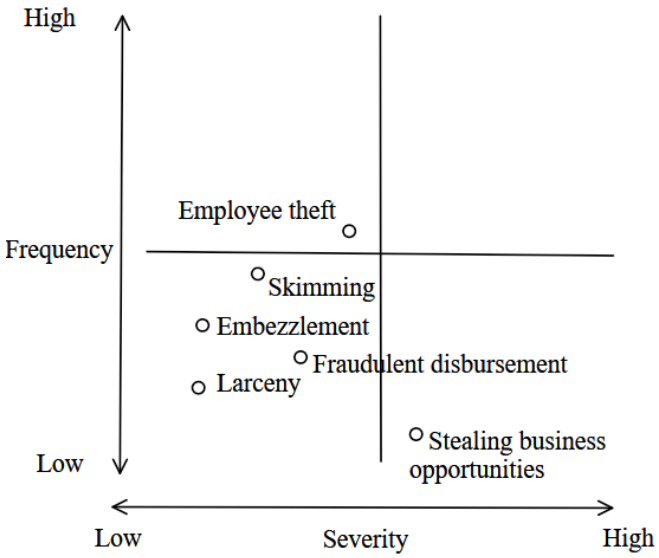


Figure 1.2. Risk map of multiple exposures

exposure of stealing business opportunities has the highest severity of its losses. This is because it incurs an opportunity cost for the victim firm. The lack of data regarding the severity of the losses from this exposure can be attributed to the difficulty of estimating losses of intangible assets. However, its frequency is lower than that of the other exposures because it is a harder crime to commit.

Discussion of Small Businesses

Small businesses - organizations with no more than about 500 employees – are the most susceptible to employee theft. In fact, in 2015, four out of every five victim organizations had fewer than 100 employees (Karpp). An issue regarding this is that small businesses lack the resources that large companies have to identify, control, and manage employee theft. In many cases, many small business owners assume that having a low number of employees means that the employees will always be honest and loyal. This wrongful assumption can cause the business to take a passive approach to preventing employee fraud.

The internal controls of a company play a large roll in its ability to detect, limit, and manage employee theft. This gives small businesses a disadvantage because they lack appropriate safeguards and do not have the employee numbers to possess a thorough system of internal control. For example, a company with one employee in charge of its finances is more exposed to employee fraud than a business that has an entire team of accountants. These internal controls that smaller businesses lack both discourage theft and consistently review the actions of other employees- a critical function for encouraging high morale within the company.

A study conducted by Jay Kennedy, a University of Cincinnati criminal justice doctoral student, shows that while 64% of small businesses have experienced employee theft, only 16%

of those who experienced this issue reported the incident to the police (Brooks). According to this study, the four main instances when employers hesitate to involve the authorities after an incident of employee theft are when the business owner does not see the ill-treatment serious enough to give his or her time to go beyond terminating the employee, when the business owner seeks counsel from a third party (usually an attorney) and that individual advises against it, when the employer has emotional ties to the employee criminal, or when the employer sees the criminal justice system as ineffective or unhelpful.

An overview of employee theft risk among different business sectors

Figures 1.3 and 1.4 portray the median losses occurring from employee theft and the percent of employee theft cases across several business sectors. In 2015, employee theft caused the retail sector to suffer the largest median loss when compared to other sectors, $606,012. However, it only made up for about 6% of the cases of employee theft reported in 2015. On the other hand, the financial sector amounted to have 24% of all reported employee theft cases but its median loss only fell within the median range of losses at $271,000. The high severity of employee theft in the retail sector and the high frequency of employee theft in the financial service sector show that the retail sector and financial sector are at the greatest risk. Sectors whose percent of employee

Figure 1.3. Percentage of employee theft cases

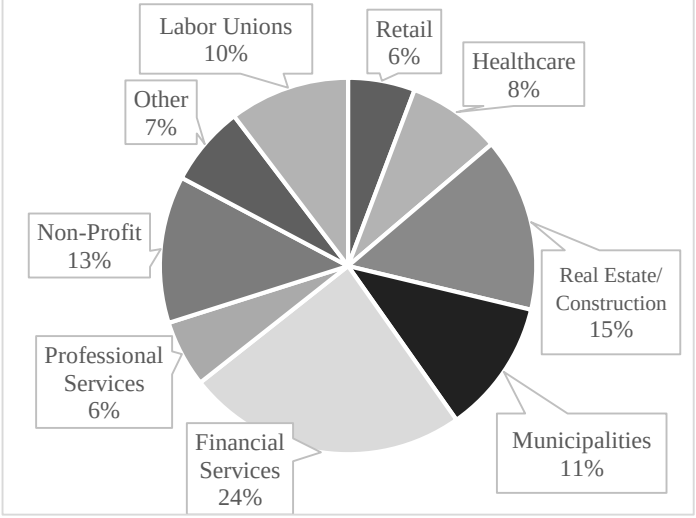
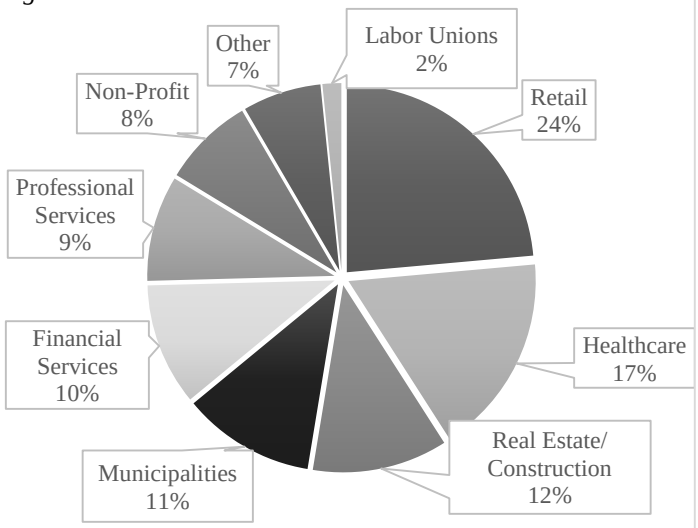


Figure 1.4. median losses



theft cases on par with their share of the total median losses among sectors are the real estate and construction and municipalities sectors. However, the real estate and construction sector has a severity and frequency that are higher than those of the municipalities sector.

Employee theft risk can be compared among many other categories. Table 1.2 is a display of these demographics:

Table 1.2. Other demographics from 2015

Perpetrator Characteristic	Significance
Employees in senior positions	**53 %** of the reported schemes
50 years old	The **median age** of the perpetrators
Employees with long tenures	The **majority** of all reported schemes
Women	**60 %** of the reported schemes
Non-management employees	**43 %** of the reported schemes
Professionals in the finance and accounting sectors	**40 %** of the reported schemes

Legal discussion

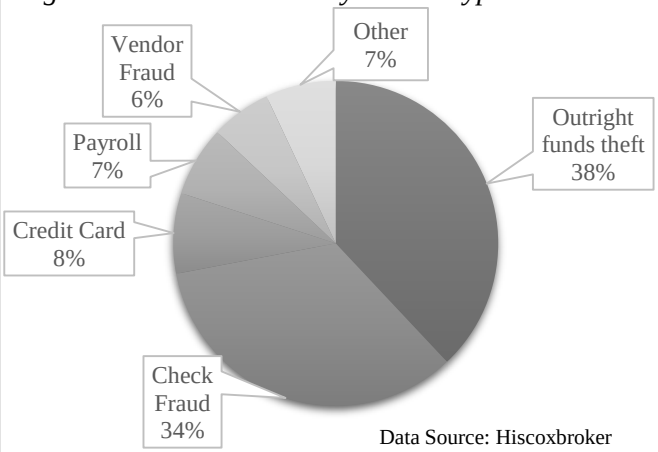
Most laws relative to employee theft are criminal laws. There are other legislatures regarding employment practices that are closely related to this risk. Most of the legal acts that affect the risk of theft from employees have been passed more than 20 years ago. However, there are certain changes in laws and new statutory acts that affect modern types of employee theft like more complicated financial schemes or data theft.

Most of these laws have the purpose of protecting employers from lost property. Employers are protected by criminal laws that establish punishments for internal thieves. A popular type of employee theft is embezzlement. It differs from regular theft from outsiders because it occurs when an employee from a company takes property entrusted to him or her with the intent to deprive the owner of the property. By legal definition, an embezzler is lawfully entrusted with the property, while a thief improperly obtains possession of the asset. Embezzlers can be punished financially for their criminal behavior through fines or imprisonment. In addition to embezzlement, other schemes of employee theft such as larceny, skimming, fraudulent disbursement, and stealing business opportunities are prohibited by criminal law. Employers are legally permitted to terminate employees who steal from their companies. Furthermore, there are laws protecting whistleblowers, which encourages other employees to report fraudulent activities that are committed by other employees or even executive officers. For instance, the Federal Whistleblower Law provides administrative remedies through the Department of Labor for Federal Employees who report fraud or theft. More recent laws come from more complicated fraudulent financial crimes or cybercrimes. From the Enron and WorldCom financials scandal, the Sarbanes-Oxley Act was passed in 2002 to prevent future fraud from a company's finance or accounting departments. In addition, the Intellectual Property and Cyber law prevents employees from stealing intellectual property and computer data from their employers. All of the above-mentioned legislatures help in reducing the severity and frequency of the employee theft risk of organizations.

In addition to the aforementioned legislatures, there are legislatures that protect employees from privacy invasion and discrimination. By implementing certain risk control methods, employers may be confronted with laws regarding privacy invasion. For example, many employers want to install surveillance cameras to help either avoid the theft before it happens by deterring

possible offenders or investigate an occurred loss. However, in certain situations, employees may argue against that policy and consider that as privacy invasion. Moreover, if employers want to investigate a suspected employee, they may try to keep the employee in the office. It seems reasonable, as the employer may be afraid that the employee will flee with the stolen property. However, the employer may negligently commit false imprisonment. Claims made against employers regarding employee theft are usually for false imprisonment during the investigation process of employee crimes. The fine can be from $1,000 to $10,000, which is not a severe financial loss for the majority of existing firms (Theoharis).

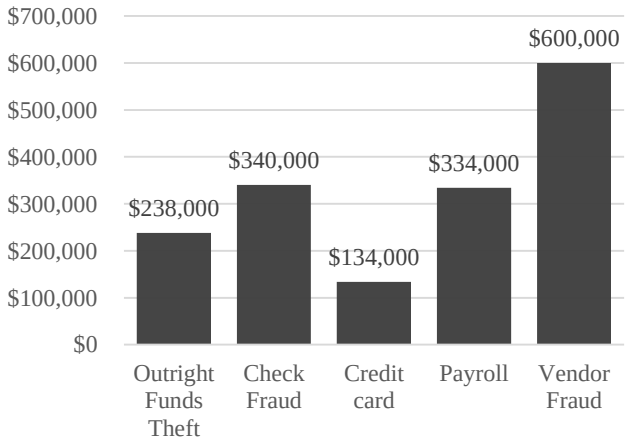
Figure 1.5. Federal cases by scheme type



Typical claims regarding employee theft are lawsuits against employee theft of tangible property. The severity of these losses has a large range, from hundreds of thousands to billions of dollars. Figure 1.5 describes many federal cases about employee theft. Outright funds theft cases happen the most frequently with 38% of all reported cases. Check fraud claims account for 34% of the cases, followed by credit card fraud (8%), payroll fraud (7%), and vendor fraud (6%).

Among the five schemes of employee theft lawsuits displayed in Graph1.6, the median settlement cost for vendor fraud is the highest ($600,000).

Graph 1.6. Median loss by scheme type



Check fraud and payroll fraud cases are less costly with median losses of $340,000 and $334,000, respectively. Outright funds theft and credit card theft are the least expensive claims by employers against their employees with median losses of $238,000 and $134,000, respectively.

A catastrophic employee theft case is the Enron scandal with embezzlement claims totaling in $40 billion. In the Enron case, the thieves were the company's executive officers. Jeffrey Skilling, the COO of Enron at that time, set up an accounting scheme allowing the other executive officers to hide billions of dollars from failed projects and negotiations. The Enron scandal resulted in the bankruptcy of the company and the creation of the Sarbanes-Oxley Act in 2002, preventing accounting loopholes that could cause other employee theft incidents.

Conclusion of risk description

This section examines the characteristics of employee theft through its definition, classification, exposures, and perils. These characteristics play a role in a company's ability to identify their risk of employee theft. The risk's description is an important background for companies to be aware of when considering and selecting the appropriate risk management practices for this criminal risk.

(2) Loss control methods

The first major approach to managing the risk of employee theft is loss control. The objectives of loss control are to reduce the frequency and severity of losses that the company faces. This can be carried out through the company's loss prevention and loss reduction methods for employee fraud. Controls refer to the processes, techniques, and strategies that discourage theft by employees (Employee Theft – Part Two). Although there is no loss control method that

completely eliminates employee theft, companies should minimize their risk of employee theft by controlling their losses. Firms are able to reduce frequency by loss prevention and decrease severity by loss reduction. Table 2.1 outlines conventional strategies that a company can use to control the risk of employee theft.

Table 2.1. Conventional loss control methods

Loss Control Methods	Purpose
Communication of Expectations	- Ensure that employees understand the attitude the company has towards employee theft - Encourage compliance and alignment with company goals
Communication of Consequences	- Deter employees from stealing any type of company property - Send messages to employees that severe action will be taken
Strict Hiring Process	- Screen out high risk prospective employees and reduce the occurrences of employee infidelity
Define Ownership & Responsibilities	- Create responsibility among employees - Have employees take responsibility for their tasks - Ensure no confusion in case of loss in distinct business functions (receiving, procurement, etc.)
Separation of Duties	- Create an environment where multiple parties would need to be involved in order for a theft to occur - Individuals much more likely to steal compared to groups of employees
Collaboration Between Departments	- Communicate and transfer data correctly and efficiently - Processes that involve multiple departments are less likely to experience internal theft
Managerial Intervention/Scrutiny	- Spot check various processes within an organization - Conduct random investigations to ensure problems are discovered - Check compliance among lower-level employees
System Implementation/Maintenance	- Inventory systems are known to spot inconsistencies in product and to trace embezzlement or other types of fraud - Maintain a record of inventories that are to be matched up against comparable records to identify anomalies

Loss prevention

Companies use loss prevention methods to reduce the frequency of losses. These practices are implemented to interrupt the chain of events leading to a loss and may or may not impact the severity of losses. Pragmatic loss prevention strategies include communicating internally, screening potential employees, establishing a complying employee culture, and

distributing duties that discourage employee infidelity. It is vital to any organization to pursue all possible endeavors that reduce employee theft risk, as it has been known to cost companies a significant amount of revenue every year. To efficiently defend against employee theft, several of these methods must be put into action simultaneously. Therefore, it is necessary to understand all of these methods and how they work together in preventing an organization's losses.

Employee Responsibility

An effective method of prevention is ensuring that all employees are aware of their responsibilities. Upper-level managers should define and clarify ownership roles and responsibilities for all company employees. This warrants that each employee is accountable for issues occurring within their own domain. It is a misconception for companies to think that their audit departments are fully responsible for discrepancies. There is no solely responsible department when employee crimes occur. An auditor's job is assessing whether the controls are properly designed and working in an effective manner. In certain businesses, professionally trained auditors are made use of in terms of locating losses. These auditors are considered a desirable source of corporate information, and have a role of possessing knowledge concerning corporate practices, policies, procedures, incoming technology, etc. (Draz). Interactive departments are also necessities that create awareness of employee theft, strengthen communication, and reduce the opportunity for loss to take place. Altogether, there are numerous procedural precautions to take.

Isolation of Duties

Another necessary policy to reduce loss frequency is isolating employee duties. This particular notion applies to firms of all sizes. For example, the person who processes cash

receipts should not be the same person who processes the funds that are disbursed (Balmer). To ensure the wellbeing of the company, no single employee should have control over all parts of a given financial transaction (Preventing Employee Theft). There are vulnerabilities within any business, so bank deposits, petty cash disbursements, invoices, and many other transactions in a company should be monitored tightly and should have sufficient controls in place for protection (Preventing Employee Theft). An example of a company control is encouraging employees to turn in those who they believe are misappropriating company resources. Many employees are deterred from doing so because they have a sense of fellow employee loyalty or a fear of backlash from other employees, which is why many firms implement anonymous tipping situations where employees can submit their suspicions of other employees (Klein). Red flags include minor employee actions, such as keeping a calculator or other suspicious items with them on a constant basis (Tanker). Although this may seem overzealous, it is a small measure in comparison to the damage that employee theft can cause.

Internal communication

The first loss prevention strategy is strengthening the internal communication within the company. Through an effective internal communication system, employers increase employees' awareness of their responsibility to protect the company's property. When workers know that an upper-level manager or supervisor is keeping watch over anything that may be stolen or embezzled, the likelihood of theft occurring decreases. Ensuring a zero-tolerance policy is key and employees must know that management is prepared to take any legal action necessary (Walsh). When a company is informant to its employees about its methods of loss detection and gives its employees training on theft prevention, it is strengthening its zero-tolerance environment. The company should also stress employee awareness of guidelines and policies. To

ensure efficiency and maximum effectiveness, this should include the procedure of firing any employee on the spot who is caught stealing and prosecuting them (Walsh). After the disbursement of these guidelines and policies to every employee, written copies of the policies should be disbursed to every company member and signed to ensure that everyone is aware of the rules and regulations in place to prevent theft (Preventing Employee Theft). This method of risk control prevents the possibility of employee crime by creating employee awareness.

Hiring process

Another way that companies prevent employee crime is in their hiring process. There are multiple attributes that must be observed in order to ensure the safest work environment with respect to employee crime. Employees must be selected carefully based upon certain criteria that may cause them to be a higher risk for the company such as having a criminal background. It is recommended that no employees with criminal backgrounds are to be hired in order to maintain the safest possible environment. In many cases insurance companies will not provide compensation to firms who experience losses from an employee who has a “documented history of dishonest behavior" (Employee Theft – Part 2). Furthermore, a study has found that 12% of those involved in company fraud have been previously fired by an employer for fraudulent conduct. Criminal activity in a prospective employee's past is serious and threatening to the wellbeing of the company. When an employee is hired, it is also recommended that they have completed an application form. This is an obvious yet often overlooked method of screening employees, especially concerning the applicant’s references. Employers should communicate with the listed references in order to verify the validity of the applicant and said references. Certain positions may require a credit check or criminal background check of the prospective

hire (Preventing Employee Theft). When hiring employees, many methods of control are put into action.

Managerial actions

There are practices that can be put into motion by supervisors and managers at many levels, as long as there are subordinates involved to be controlled or watched over. Managers must ensure cooperation by employees themselves. To truly encourage a culture that enforces compliance in a trusting manner, managers must act as examples for their employees. The tone that the upper level employees set concerning risk control of employee theft creates that actions that are taken by employees (Draz). Lower level employees will have no motivation to abide by control plans if the people with positions above them are not setting an example. Upper management controls this themselves by establishing plans that fit their firm's culture. These plans must detect all fraud and tolerate none of it, while at the same time fostering a culture of compliance (Klein). The overall environment behind the firm concerning the loss control must be cohesive and comprehensive to function progressively.

There are many distinct procedures that managers can take part in. For example, some particular methods that reduce retail employee theft include planning unannounced manager visits to retail stores spot-check inventories and cash drawers, maintaining and checking company check deposits, and keeping track of "No Sale" transactions within a particular location (Tanker). Continuing on, implementing badge ID check systems in employee entrances seems to have positive effects for the management of employee crimes (Preventing Employee Theft). The aforementioned practices are very effective in protecting company assets because they deter possible offenders and detect employees who are violating company policies. The ongoing processes of a business must be constantly scrutinized by a higher up in order to ensure as little

loss as possible (Balmer). Human Resource programs such as profit sharing, fair compensation, and other practices go a long way with building employee loyalty, which can help to decrease employee infidelity (Preventing Employee Theft). There are plenty of options within this micro-setting of risk control for employee theft, some being checking incoming merchandise against invoices, checking outgoing shipments against shipping documents, and even having an area where garbage is collected before disposal (Preventing Employee Theft). All of these methods may seem minor and are oftentimes overlooked, yet can cause significant losses to firms if they are taken advantage of.

Loss Reduction

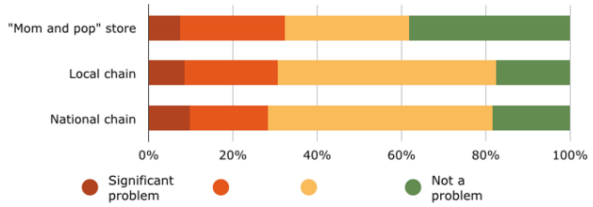
Loss reduction also plays an integral role in the process of controlling a company's risk of employee theft. Through loss reduction procedures, companies can reduce the severity of losses when they occur. These practices may not affect the frequency of the loss, but they minimize the financial value of employee theft loss. A company can approach loss reduction by using pre-loss and post-loss methods. Pre-loss loss reduction methods are preferred by most companies, as reducing losses after they occur can be an enormous obstacle.

Pre-loss loss reduction

Companies reduce employee theft losses by using technology to monitor and identify suspicious actions that can be potential theft activities. Inventory systems have proven to be a functional tool in identifying where theft originates from by performing random inventory checks. Various reports show that lower losses from internal theft are linked to higher inventory software usage. This is further perpetuated by the fact that those companies with software in their systems rather than pen-and-paper methods of inventory perceived more risk of internal

malevolence. Figure 2.1 (courtesy of Burnson's article) shows disconnect between sizes of chains and their perceptions of the amount of employee theft occurring. It is clearly a problem with Mom & Pop stores seeing as they have a much less perceived risk than that of reality. Due to these reasons, Mom & Pop stores are considered to be most at risk for petty employee theft (Burnson). Many articles concerning employee theft risk have stressed the importance of inventory systems as relevant risk reduction facilitators.

Figure 2.1. Employee perceptions of theft, by store type



Other technological measures can be implemented in order to secure this exposure from any loopholes in the system that create the opportunity for theft. Firms utilize certain technology security measures such as installing antivirus software, protecting themselves with firewalls, and utilizing complex passwords (Davis). Although physical larceny and embezzlement are reduced through the use of deterrents like cameras and other security measures, the security environment of the virtual world is vastly different. Internet risks are increasing every day, and small implementations like those aforementioned make huge differences for companies. In addition to those implementations, it is recommended to regularly back up data to another source, secure Wi-Fi to the fullest extent possible, and limit access to critical data (Davis). Other risk controls along these minor parameters include fingerprint scanning for activities such as clocking in and out, or even to validate an employee's access to certain data. Such operations are significant to a firm's management of employee theft.

Post-loss loss reduction

The most common post-loss reduction methods are investigation processes and litigation management. When theft occurs, a company needs to immediately cooperate with police officers in investigating the incident. Any decision that is hesitant in involving the authorities will result in further financial losses for the victimized company. Through investigations, the company can understand the scheme of theft and take corrective action for the prevention of future internal thieves. Moreover, internal communication should be reinforced. Once the thief is caught, he or she must immediately be terminated. The termination of that dishonest employee should be announced to other employees so that anyone can be warned. If the financial loss is substantial, a legal case should be filed to retain at least a partial value of the loss.

Shortcomings

Companies should be aware of the shortcomings of loss control methods concerning the risk of employee theft, as there are some aspects of an exposure that are residual and therefore unable to be diminished to zero. A concern of employee theft is that most of the measures taken to control its losses are pre-loss rather than post-loss methods. With an exposure like employee theft, it is more effective in scenarios where theft is fought against before it occurs. There are options available that are implemented after losses, such as punishing offending employees to the fullest possible extent of the law. The main post-loss actions for employee theft involve making an example of events when losses occur and how they are managed. Although both are involved in this risk control process, pre-loss controls are more significant in comparison to their counterparts.

The predictability of losses along with the difficulties of increasing said predictability are other shortcomings. This type of loss does not have a possibility of increasing predictability aside from increased previous records. Looking at loss history would most likely be a viable risk control option in terms of predictability, but this does not assist in creating a substantial loss control program. Avoidance is also impossible when it comes to employee theft and infidelity. No matter the type of business or the controls taken, as long as one has employees working for them, this risk will be existent and prevalent. Whether it is proactive or reactive, avoidance is not an option in this case. Due to these reasons, the use of loss control in order to reduce frequency primarily is a more viable option than attempting to combat the risk via the aforementioned methods.

Conclusion of loss control methods

Firms are constantly fighting this threat in order to maintain business efficiency and cut losses using various loss control strategies. Although every firm should have measures and plans in place, one must perform a cost-benefit analysis in order to determine the most effective plans. Once these plans are implemented, they must be enforced and monitored extensively to ensure maximum control (Klein). Both prevention and reduction are utilized in this particular risk control, with each having their own respective role within the organization. Most actions to be taken are performed at a management level rather than an employee level, therefore most of the duties lie within managers' and their actions. Risk control is a key aspect of any company's risk management strategy, and therefore must be taken into account with any particular exposure.

(3) Loss financing methods

Firms also manage their risk of employee theft by utilizing different loss financing methods. The options of external funds, through risk transfer, and internal funds, through risk retention, are both available sources of finances for losses. When considering the risk of employee theft, methods of alternative risk financing, such as derivatives or hedging, are not widely used.

External funds (risk transfer)

In regards to risk transfer, both insurance and non-insurance techniques are taken into consideration. The popular risk transfer method comes from external funds through insurance companies. Non-insurance techniques are not popular in financing the risk of employee theft.

Major insurers, policy provisions

Crime insurance is a common type of insurance for employee theft because it covers most of the crime losses that can financially hurt many companies. Many insurance companies offer commercial crime insurance including Chubb & Son, Travelers, AIG, and others. A typical crime insurance policy provides coverage for a variety of employee theft crimes including dishonesty, fraudulent tax refunds, senior management fraud, funds transfer fraud, forgery, and computer fraud. It also compensates lost property, such as money and securities. The coverage for large losses, such as that from AIG, typically ranges from $3 million to $34 million for different types of theft schemes including foreign employee fraud, payroll manager fraud, false invoicing, or inventory fraud. The maximum claimed loss in regards to employee theft was reported to be up to $77.5 million for senior management fraud (Fidelity Claims Scenarios). The

most popular type of claim for AIG was vendor fraud with covered losses ranging from $11 million to $40 million. For example, a group of manufacturing employees conducted a scheme to undervalue scrap from a scrap dealer. In exchange, these employees received cash and other benefits valued at $40 million. Though the loss were significantly high to businesses, it was fortuitous enough to be covered by insurance companies.

Another common source of external funds is a financial institution bond. This form of insurance protects financial institutions and banks from employee theft, money and securities fraud, as well as counterfeiting. They protect directly against property losses resulting from employees' actions; for many banks, financial institution bonds are a requirement. Based on Section 18(e) of the Federal Deposit Insurance Act, the Federal Deposit Insurance Corporation can require it for banks with a penalty if not instilled as part of their system. Since internal theft is a greater risk, many banks are required to use federal institution bonds and other means to protect against internal risk (Magrann-Wells).

Other important provisions and application process

While crime insurance vastly covers many types of losses, certain losses are uncovered and the application process is complex for the insureds. First, if the actions were committed by the employers or business partners, the insurers will not indemnify the loss. This first condition is to avoid moral hazards by employers. Second, many insurers only cover the financial losses of the crimes, not the liabilities beyond the losses. If the employee crime resulted in a lawsuit by consumers against the company, the indirect losses from the lawsuit would not be covered by the insurance policy. Third, if the losses were triggered by loopholes in accounting or management systems of the insureds, the losses would more likely be denied coverage. This third condition is

to ensure that the insureds act more responsibly in controlling their risk of employee theft. The insureds cannot be negligent after buying coverage for the risk.

Additionally, each business in the application process for insurance also must fill out detailed information regarding its risk management, risk controlling and internal auditing processes. For example, the application form from AIG requires a company which wants to buy crime insurance to submit claims history, its number of employees, as well as their titles, responsibilities, and geographic locations. Audit and internal control procedures, vendor information, funds transfer and computer systems must also be provided.

Premium rates and loss ratios

From the insureds' applications, insurance companies determine the rates based on the number of employees in the company and the amount of current coverage it has. The sector of the company is also key. If a company is in the financial sector or the retail sector, the rates would be higher because they are more likely to deal with the most employee theft. Employee theft varies widely based on the size of the company and the amount of controls and resources. Therefore, costs will vary based on the expected loss (p^*) of the risk at each specific company. In 2015, the top four business insurers included Chubb, Travelers, AIG, and Great American Insurance Group. These four took up over 50% of market share in the industry. Their listed direct premiums were $236.9 million, $195.8 million, $115.1 million, and $84.2 million, respectively (MacLeod).

Fidelity insurance premiums were fairly steady from 2014 to early 2016 with small increases and decreases. However, in both 2013 and 2014, underwriters in commercial crime had been seeking increases in premiums by about 3-5%. In 2015, the underwriters were satisfied with

their profits and premiums. Though the premiums remained the same from 2014 to 2015, premiums from financial institution bonds had increased modestly. In 2016, total premiums are expected to decrease by a small amount for large and medium sized companies. For small companies, premiums are expected to increase by 0-3%.

In comparison, the insurance companies generally face moderate losses. The aggregate loss ratio increased from 46% to 52% in 2013. AIG was one notable outlier with a loss ratio of 81.7%, inflating its loss ratio by a significant amount since it has relatively large premiums. In 2014, the aggregate loss ratio decreased from 52% to 40%. That year, 5 out of the 10 companies with the highest premiums had a loss ratio of less than 40%. CNA had a listed loss ratio of –5.1% (MacLeod). Sometimes, the value of outstanding claims can change due to events, such as a judge's decisions. This, in turn, leads to a negative loss ratio (Levine).

Table 3.1. Companies with the Ten Highest Premiums

	2012		**2013**			**2014**		
Underwriter	**Direct Premium ($M) (%)**	**Loss Ratio (%)**	**Underwriter**	**Direct Premium ($M)**	**Loss Ratio (%)**	**Underwriter**	**Direct Premium ($M)**	**Loss Ratio (%)**
Chubb	240.7	62.6%	Chubb	234.6	70.1%	Chubb	236.9	75.4%
Travelers	190.1	56.0%	Travelers	194.4	42.1%	Travelers	195.8	48.3%
AIG	132.5	81.7%	AIG	123.7	33.1%	AIG	115.1	96.6%
CUNA	84.2	59.7%	Great American	85.6	30.4%	Great American	84.2	39.2%
Great American	82.7	24.2%	CUNA	80.3	60.3%	CUNA	78.7	21.9%
Zurich	72.8	51.3%	CNA	71.3	17.1%	CNA	71.8	-5.1%
CNA	68.6	48.4%	Zurich	64.6	59.9%	Zurich	66.7	98.3%
Hartford	49.1	45.1%	Hartford	48.6	26.5%	Hartford	48.2	36.7%
Liberty	24.5	35.8%	WR Berkley	28.2	30.8%	WR Berkley	27.0	22.6%
ACE	23.6	66.0%	ACE	24.1	29.7%	ACE	25.3	66.6%

The insured's approach, moral hazard and adverse selection

As insurance for employee theft is expensive, companies that need crime insurance have to carefully consider, select, and buy appropriate types of insurance that fit their needs. In fact, many companies are prudent when buying coverage for employee theft. Although this risk can cause large financial losses for businesses, insurance policies are still not attractive to many organizations, especially mid-size companies. Insurance for employee theft is difficult to find since it is difficult to prove. Proof of theft involves legal action and prosecution. Generally, the limits start at $5,000 and companies commonly increase it anywhere from $10,000 to $100,000. ACFE's reports included that the median loss for employee theft every year is $140,000. Furthermore, more than one-fifth of the companies sustained a loss of more than $1 million. Despite that fact, most mid-size organizations either do not buy insurance or buy insufficient insurance. The ACFE reports that only 16% of companies buy full insurance for losses of employee theft.

For many insurable risks, moral hazard and adverse selection are two major negative influencers. Moral hazard is when the presence of insurance triggers behavioral changes of the insureds. Potential moral hazard with employee theft tends to happen in businesses that have looser management and internal auditing systems. With the presence of insurance, companies may choose not pay to install better supervising technology or other loss control methods. Other changes of behaviors due to moral hazard include fake claims of theft that do not exist to take advantage of insurance. However, the probability of companies engaging in moral hazard is low. As employee theft is a net income risk, if affects both revenues and expenses. Even with insurance, loose auditing systems cause losses for companies. Employee theft insurance only

covers the replacement cost of lost property which reduced expenses. However, the loss of revenue from employee crimes that result in business interruption is unavoidable. If property is stolen, the time that it takes for the company to identify the loss, file a claim, and wait for reimbursement from insurers negatively affects the operations of the company. The business is interrupted, therefore a loss of revenue still occurs. Therefore, employee moral hazard where companies have insurance and decrease loss control practices in order to save money is unlikely. The probability that fake claims will be identified by insurers is high. Insurers are professional and efficient in the investigation process and recognize fake claims. Furthermore, if a fake claim is identified, the insurance contract will be voided and the insured will lose all of their paid premiums. Thus, moral hazard from fake claims is not a significant concern for the risk of employee theft.

In addition to moral hazard, adverse selection is another issue of the insurance model. The problem with adverse selection occurs with the presence of choice when "good" risks can drop out and "bad" risks can enter the insurance pool of risk sharing. Good risks are those that can be determined to have a relatively low p* and therefore are the least risky prospects. Conversely, bad risks are those with high p* and are higher risk due to their unpredictability. Asymmetric information also increases adverse selection. The idea of insurance is for many people of independent and homogeneous risks to pay a small amount of money as premiums and receive claims in the event of a loss. Therefore, insurers need to collect information from many people in order to have a number of people to join the risk pool. With a sufficient number of insureds, insurers can evaluate the risk more accurately and charge appropriate premiums for different insureds. However, adverse selection creates a scenario where only bad risks with high severity and frequency of loss stay in the risk pool. That situation tremendously reduces the

insurers' profitability which may be detrimental to the sustainability of the insurance model. Adverse selection can only happen when insureds have a good understanding and estimation of their own risks to decide their insurance decision. For employee theft, a company is not that knowledgeable about the frequency and severity of its risk. Therefore, employee theft is relatively fortuitous and adverse selection is not a significant issue for this type of crime insurance.

Internal funds (risk retention)

While risk transfer is a viable option, a significant amount of small to mid-sized companies do not have coverage for employee theft. For these firms, they can practice either active and funded retention, active and unfunded retention or passive and unfunded retention. In terms of risk, active retention refers to the firm being aware of the risk that it faces. On the contrary, passive retention indicates a lack of knowledge of said risk. The difference between unfunded and funded is rather explicit; unfunded retention is when the organization does not set aside finances for covering the loss, and funded retention is when there is financial coverage prevalent for the loss. The funds in this case are from within the company rather than coming from external sources.

Victimized companies' common approaches

For many high frequency and low severity risks, companies would use active and funded retention since they do not want the potential loss from these risks to hurt them financially. This method works for these risks as the expected loss can be accurately estimated through a large number of losses. However, employee theft is not a typical high frequency and low severity risk. While employee theft is a high frequency and low severity risk, that classification is not practical

for any specific firm. The high frequency of employee theft comes from the aggregation of many types of employee theft exposures, all of which have different severity and hence cause the low average severity of employee theft. For the most part, each exposure of employee theft has a low frequency and thus most firms do not know exactly the frequency of their employee theft risks. As a result, they cannot accurately predict the expected loss (p*) to set aside money to pay for future losses. Therefore, the option of active and funded retention is not viable. The obvious consequence is that many firms will practice unfunded retention, regardless of their awareness of the risk (active or passive). The Association of Certified Fraud Examiners (ACFE) reports that 40% to 50% of victimized organizations have no plan in place to pay for losses from employee theft. Therefore, when employee theft occurs, most firms will pay for loss from current revenue or borrowed funds.

With the majority of victimized companies using unfunded retention to finance the risk of employee theft, small firms are generally considered to be more susceptible to this risk than bigger firms. Small firms have worse loss control methods as they do not have the money to invest in those practices. When employee theft occurs, small firms have less revenue to pay for losses. Hence, they are more vulnerable. However, that does not mean big firms can be safer with unfunded retention. For big firms, employee theft tends to have a higher severity with a bigger financial value, such as the Enron scandal with the total losses of $40 billion. Therefore, unfunded retention is not a recommended way to manage the risk of employee theft.

Advantages and disadvantages of self-insurance

In addition to firms that use unfunded retention, there are still companies with active and funded retention. The method of self-insurance has its own positives and negatives. The big advantage can be the lower expenditure on managing the risk of employee theft. With self-

insurance, the estimation of expected value (p*) can be higher due to smaller size of loss sample. However, companies can save money from risk charges and administrative costs. For example, insurance companies have marketing expenses while self-insured companies do not have to spend on marketing. Moreover, self-insured firms can save a lot of money from insurance premiums. The money which could have been paid to insurers now can be used to invest at a higher rate of return. Also, the self-insured organization can gain all the benefits of its successful implementation of loss control methods. If a firm can reinforce its policy to reduce the frequency and severity of employee theft, it can enjoy lower premiums than other insureds that buy commercial insurers. The flexibility in designing the insurance program is another advantage for companies when considering self-insuring its employee theft risk.

On the other hand, there are inherent disadvantages of self-insurance for firms in managing the risks of employee theft. The first one would be a catastrophic loss due to employee theft. If an employee steals a large amount of money from the company, a disaster can happen. The case of Enron would be a salient example for catastrophic loss because it went bankrupt after the loss of $40 billion dollars. More than just the risk of catastrophic loss, self-insureds do not have supportive services from insurers like other insureds. Commercial insurers are more likely to have a team of experts to help with internal auditing, risk identification and risk control implementation. With self-insurance, the firms do not have as much experience as the companies who specialize in insurance. The final disadvantage is that self-insured premiums are not tax deductible. If a firm pays premium to a commercial insurer, it can reduce its earnings before tax and hence decrease its tax liability. A self-insured company does not have that benefit. Obviously, self-insurance can be a method of risk retention for many firms. However, each firm

has to take into consideration the advantages and disadvantages of this approach as well as the firm's needs to choose the most appropriate risk management option.

Conclusion of risk financing method

As seen, various approaches to financing the risk of employee theft are available and utilized by companies. A firm can choose to transfer the risk to insurance companies through insurance or to retain the risk. While insurance is a viable risk transfer option, only a minor portion of the market (16%) chooses to buy full insurance. A majority of firms (40%-50%) decide to retain the risk with unfunded retention. While each company has its own rationale in the risk management process for employee theft, risk financing options should be considered in the decision making process.

Conclusion

Employee theft is a criminal risk that can severely affect a company. Firms' awareness of the characteristics of this risk, methods to control losses, and multiple ways for a company to finance losses that may occur cause a firm better able to manage employee crime.

The risk of employee theft is an established risk in the risk portfolio of businesses in various industries like financial services, municipalities, real estate or even non-profit. Because of its long existence, employee theft is regulated by many legislatures and statutory acts. Moreover, there are methods to identify this risk through loss history, background checking, screening in the hiring process, internal audits, peer-review surveys and contract or flow chart analysis. Despite all of the mentioned risk identification methods, employee theft is becoming harder to identify due to new and more complex schemes that are developed by employee thieves to steal property from

companies. Moreover, employee theft has distinct exposures such as skimming, embezzlement, fraudulent disbursement, larceny and stealing business opportunity, all of which have different frequencies and severities. Still, employee theft is a static, speculative risk of high frequency and low severity. It falls under both TRM (as a property risk and net income risk) as well as ERM (as a hazard risk). The risk of employee crime varies among firms of different sizes and industries. From data-supported evidence, employee theft can have an enormous impact on many firms, especially firms in financial services or small to mid-sized firms.

This risk is important and must be taken control of by active businesses. There are an assortment of options that aid in decreasing a firm's frequency and severity of employee theft. These options incorporate the firm's loss prevention and reduction methods that decrease frequency and severity, respectively. Many of the actions that are put into place for employee theft loss control are simple concepts that are many times overlooked. Some of the most significant breaches regarding employee theft occur due to negligence or lack of security, such as spot checks by managers, inventory systems, firewalls, etc. To control losses from these breaches, both methods of loss prevention and loss reduction are utilized. Prevention is used to decrease frequency while reduction is used to decrease severity, both of which are major components of employee infidelity risk. Prevention includes methods such as screening employees for dishonest backgrounds and other such actions that reduce frequency. Reduction techniques, which composes of pre-loss loss reduction and post-loss loss reduction, are mostly within the realm of technological security. Between loss prevention practices and loss reduction methods, prevention strategies are more abundantly utilized within firms. This is due to the fact that it is easier to prevent a theft from taking place rather than controlling the amount which is stolen in a given theft.

In addition to risk control methods, many firms take into account approaches to finance the risk of employee theft. The type of risk financing for employee crimes varies based on the type of business. A larger company would use a more stable risk financing strategy, such as insurance, while smaller companies are often unable to finance this risk. There are two major types of insurance for employee theft. Firms generally use either crime/fidelity insurance or financial institution bonds to finance the potential loss. Moral hazard and adverse selection tend to be negative side effects of financially insuring against this risk. However, moral hazard is not a big concern for employee theft risk due to the risk's fortuitous nature. Additionally, companies do not have enough knowledge of the frequency and severity to have much adverse selection. The smaller firms generally retain their risk because insurance for employee crimes is expensive. Shareholder satisfaction is not a concern for these companies because they are not corporation. Therefore, they have more flexibility in financing their potential loss.

Employee theft risk is necessary for companies to consider because of its complexity. To effectively manage this risk, a company needs to deeply understand its aspects when choosing and implementing appropriate options.

Works Cited

Ali, Vicki. "The High Cost of Low Morale — and What To Do About It."*Barrett Rose & Lee*. BarretRose, 21 Oct. 2010. Web. 18 Apr. 2016.

Balmer, Steven. "Employee Theft On The Rise In Recession". *National Underwriter* (2009): n. pag. Web. 11 Apr. 2016.

Brooks, Chad. "Employee Theft: Why Most Small Businesses Don't Report It." *Business News Daily*. Purch, n.d. Web. 11 Apr. 2016.

Burnson, Forrest. "How Inventory Software Can Aid Employee Theft Prevention". *Software Advice*. N.p., 2015. Web. 11 Apr. 2016.

Cream.hr. “The Most Common Lies People Tell On Their Resumes.” *BusinessInsider.com*. Business Insider, 5 Mar. 2013. Web. 09 Apr. 2016.

Davis, Richard. "10 Cyber Security Measures That Every Small Business Must Take". *Tech.co*. N.p., 2014. Web. 12 Apr. 2016.

Draz, Daniel. "Fraud Prevention: Improving Internal Controls". *CSO Online*. N.p., 2011. Web. 10 Apr. 2016.

Employee Theft - Part Two. 1st ed. Insurance Publishing Plus, Inc., 2009. Web. 11 Apr. 2016.

“Employee Theft Statistics.” Association of Certified Fraud Examiners. 07 Sep. 2015. Web. 09 Apr. 2016.

“Fidelity Claims Scenario.” Financial Lines. AIG. Web. 11 Apr. 2016.

Karpp, Doug. *Hiscox Broker*. 2015 Embezzlement Watchlist. Hiscox, 2015. Web. 11 Apr. 2016.

Klein, Hubert. "Occupational Fraud – Still A Big Issue For Business". *EisnerAmper*. N.p., 2014. Web. 11 Apr. 2016.

Levine, Arthur. "A Negative Loss Ratio." *DrLevineLaw.com*. Dr. Arthur J. Levine, 9 Sept 2014. 16 Apr 2016.

MacLeod, Andrew. "Market Conditions." *AJG.com.* Arthur J. Gallagher & Co, Mar. 2016. 13 Apr. 2016.

Magrann-Wells, Richard. "Guide to Financial Institution Bonds" Willis Towers Watson, 31 Aug. 2015. 11 Apr. 2016.

"Many midsize companies go without coverage for employee theft." *BusinessInsurance.com*. Business Insurance. 27 Mar. 2013. Web. 11 Apr. 2016.

Murphy, Pat. "Employee Theft." *Practical Business Knowledge*. Wordpress, 03 Mar. 2011. Web. 11 Apr. 2016.

Preventing Employee Theft. 1st ed. Central Insurance Companies, 2015. Web. 11 Apr. 2016.

"Report to the Nations." ACFE. 2014. Web. 9 Apr. 2016.

Schaefer, Patricia. "Employee Theft: Identify & Prevent Fraud Embezzlement & Pilfering." *Business Know-How*. Attard Communications, 2012. Web. 11 Apr. 2016.

Tanker, Nancy. "Strategies To Prevent Shoplifting And Employee Theft - Specialty Retail Report". *Specialty Retail Report*. N.p., 2016. Web. 9 Apr. 2016.

"The Employment Situation – March 2016." U.S. Department of Labors. Bureau of Labor

Statistics. 1 Apr. 2016. Web. 9 Apr. 2016.

Theoharis, Mark. “False Imprisonment.” CriminalDefenseLawyer.com. Criminal Defense Lawyer. 2014. Web. 9 Apr. 2016.

Walsh, Justin. "Employee Theft". *International Foundation for Protection Officers*. N.p., 2000. Web. 18 Apr. 2016.

"Workplace Rules Protect Your Business and Maintain a Positive Employee Environment." *Workplace Rules Protect Businesses & Maintain a Positive Employee Environment*. BizFilings, n.d. Web. 18 Apr. 2016.

"Wells Fargo Insurance 2016 Market Outlook." *Wfis.WellsFargo.com*. Wells Fargo, 2 Dec. 2015. 11 Apr. 2016.

Willis North America. “Executive Risks Alert.” May 2008. Web. 11 Apr. 2016.