Occupational Fraud: A Survey

by
Elizabeth Louise Carroll

A thesis submitted to the faculty of The University of Mississippi in partial fulfillment of the requirements of the Sally McDonnell Barksdale Honors College.

Oxford
May 2015

Approved by

_____
Advisor: Dr. Victoria Dickinson

_____
Reader: Dr. Kendall Bowlin

ABSTRACT
ELIZABETH LOUISE CARROLL: Occupational Fraud: A Survey
(Under the direction of Dr. Victoria Dickinson)

This paper examines the issue of occupation fraud in today's corporations. It provides an overview of the types of occupational fraud and how they usually occur. This paper also explains the attributes of the typical fraudster and describes warning signs that management should look out for in their company. It analyzes the regulations and polices put into place to combat the growing issue of fraud. It also provides a look at cyber-fraud, which is an increasing problem due to society's reliance on technology. It explains why fraud prevention is so important in corporations, whether small or large, and emphasizes the problems that occur when fraud is left undetected. This paper also provides an overview of the assurance opportunities relating to fraud and details a proposal for the implementation of a fraud prevention plan. Overall, it allows readers to gain a general understanding of all of the important aspects of occupational fraud.

TABLE OF CONTENTS

LIST OF FIGURES

Introduction

Fraud is a million dollar business against which most companies do absolutely nothing to protect themselves. KPMG defines fraud as "a misrepresentation properly relied upon by an individual to that person's detriment or to the unfair advantage of the fraudster" (5). Although there are multiple types of fraud, this survey will focus on occupational fraud, which occurs when "an employee abuses the trust placed in him or her by an employer for personal gain" (ACFE, 6). Occupational fraud is a more focused area of fraud that causes many organizations to lose thousands of dollars each year. Occupational fraud has been on the rise and it is predicted that it will continue rising over the next few years. There are many possible reasons for this, with financial problems and new technology being major factors. This survey will provide an outline of how and why occupational fraud is committed. It will also explore possible anti-fraud initiatives that organizations can take to protect themselves against occupational fraud and explain why it would be in their best interest to do so.

Fraud Triangle

The fraud triangle is presented in many business courses as an attempt to answer the question of why fraud is committed. This triangle consists of the three elements which make up the points of the triangle: pressure, rationalization, and opportunity. Donald Cressey developed these three commonalities of fraud in the mid-twentieth century (Singleton, 9). His study showed that these three elements are present in each case of fraud, although in varying degrees. This theory is put into practice today as fraud investigators seek to identify these elements in current cases they are assessing.

Pressure is defined as something that forces or influences someone to a particular end. This element always develops first because it is what motivates a person to even consider committing fraud. Many times this pressure stems from some type of personal financial problem. An example of this element could be a financial strain due to a spouse being laid off and the increased pressure to provide for the families' financial needs. A different type of financial pressure could be a personal addiction to an expensive habit, such as gambling or illicit drugs. Aside from personal issues, an individual could see fraud as a way to meet an unrealistic work incentive or demand from his employer (Singleton, 9). Any increased demand to earn or achieve more could be considered the element of pressure. Once this element begins to take form, then the other elements follow.

According to the Association of Certified Fraud Examiners' *2012 Report to the Nations* (RTTN), 87 percent of people who commit fraud had not previously been charged with any type of fraud related crime (ACFE, 4). Since most fraudsters are first-time offenders, they need to have a reason (in their own minds) which justifies committing the fraud in the first place. This need to justify the crime is what makes rationalization a major element of fraud in the fraud triangle. Rationalization is defined as ascribing one's acts to causes that on the surface seem reasonable but are actually unrelated to the real causes. In *Fraud Auditing and Forensic Accounting*, Tommie Singleton states that "many will steal from employers but mentally convince themselves that they will repay it" (10). In effect, the fraudster is rationalizing his behavior. Therefore, any excuse that convinces a potential fraudster that he will not really be committing a crime will lead him to look for an opportunity to commit the fraudulent act.

The biggest factor regarding opportunity revolves around the internal controls that a company has in place to protect itself from fraud. Internal controls are a focus in any conversation about fraud because they alone play the major role in determining whether or not fraud can occur in that company. Understandably, it is more common for fraud to occur in a company with a weak system of internal controls because there is a greater chance of the fraudster not getting caught (Singleton, 10). Regulations have been developed by governments and companies to help organizations increase the strength of their internal controls because that is the only part of the fraud triangle that is within their control. If companies can develop a strong enough internal control system, then they can at least decrease, if not completely eliminate, occupational fraud.

While the fraud triangle is still a widely accepted fraud assessment tool, there are some professionals who do not believe that it is adequate. This belief stems from the fact that the elements of pressure and rationalization are not always observable by the organizations. An article from *Fraud Magazine* brings up several other models that may be considered more effective than the fraud triangle. One of these is the fraud diamond, which adds capability to the list of fraud elements. The article says that "opportunity opens the door, and incentive and rationalization draw the potential fraudster toward the open doorway, but the individual must have the capability to walk through that opening" (Dorminey). Other faults of the fraud triangle are that it only accounts for first time offenders and it does not consider any element of collusion. The resulting conclusion is that when assessing fraud, particularly outside the realm of a first-time offender, it is important to consider other tools in addition to the fraud triangle.

Types of Occupational Fraud

The three major categories of occupational fraud are asset misappropriation, corruption, and financial statement fraud. Each of these categories has a different level of occurrence as well as median loss associated with them (Figures 1 & 2). As the following graphs indicate, asset misappropriation is the most common fraud category while financial statement fraud is the most costly to the organizations. Since each category of occupational fraud is committed in a different way, they are often committed by different types of fraudsters.

Figure 1

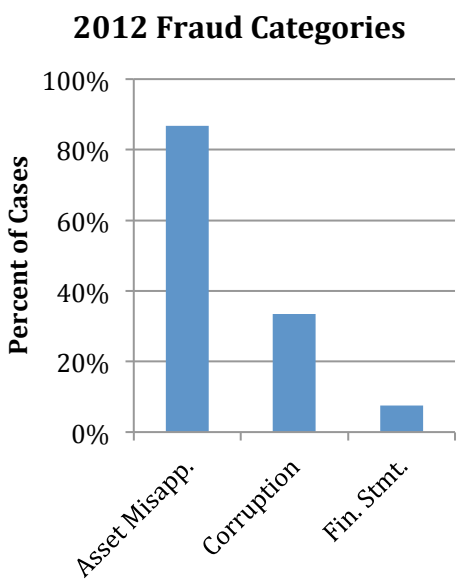
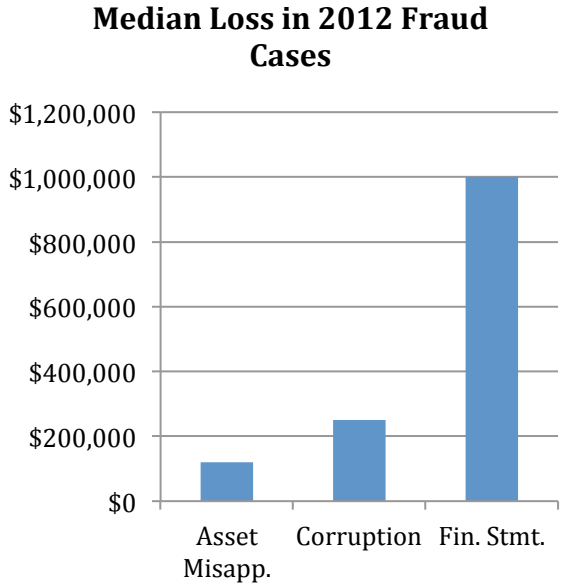


Figure 2



Source: ACFE 2012 Report to the Nations

According to the 2012 RTTN, asset misappropriation is the most common type of occupational fraud, but it is usually the least costly to the company involved (10). Joseph Wells describes asset misappropriation as "the misuse of any company asset for personal gain" (48). It is most commonly associated with theft of a company's assets and does not

always involve cash. One reason that asset misappropriation is the most common type of occupational fraud is because there are so many different ways to accomplish it. The *Corporate Fraud Handbook* describes seven different asset misappropriation schemes: skimming, cash larceny, check tampering, register disbursement, billing, payroll and expense reimbursement, and inventory and other asset mismanagement. These different schemes can all be broken down into further categories (Wells, 47). Billing schemes are the most common, occurring in 24.9 percent of the reported cases, while check tampering schemes are the most costly per case with a median loss of $143,000 (ACFE, 12). The perpetrators of asset misappropriation crimes can be employees, customers and vendors to the companies victimized. They can even be individuals with absolutely no ties to the organization whatsoever (Albrecht 1). Albrecht's research found that, once a fraudster is successful, they began to recruit others in order to increase their gain from the fraudulent activities (8). However, in most cases, the more one tries to steal, the more likely they are to get caught. It has been said that "when an asset misappropriation takes place...the perpetrators are almost always caught" (Albrecht 5). While this may very well be true, it usually takes an extended time for the fraud to initially be discovered. The 2012 RTTN reported the average duration of occupational fraud (from first occurrence to initial detection) was eighteen months (ACFE, 13). Since asset misappropriation is largest segment of occupational fraud, its frequency does make the cost to a victimized company add up quickly. Therefore, it is important for companies to be as prepared as possible to detect this type of occupational fraud as early as possible.

Corruption is commonly known as dishonest behavior and that is what it means when related to occupational fraud as well. While it is not nearly as common as asset

misappropriation, it is still found in 33.4 percent of fraud cases and it causes a median loss of $250,000 to the victimized company (ACFE, 11). Accordingly, this type of occupational fraud costs companies a significant loss of money; it is a continuing cause for concern. The RTTN defines corruption in the context of occupational fraud as occurring when "an employee misuses his or her influence in a business transaction in a way that violates his or her duty to the employer in order to gain a direct or indirect benefit" (10). This broad definition can be broken down into four schemes: conflicts of interest, bribery, illegal gratuities, and economic extortion (Wells, 281). The last three schemes can be lumped together, in a general overview because of their similar nature since they involve decisions made because of a promised reward or a threatened punishment. On the other hand, conflict of interest situations differ since there is no reward for making a certain decision. As Wells describes it, "the crux of a conflict case is that the fraudster takes advantage of the employer; the victim company is unaware that its employee has divided loyalties" (311). This scheme is unlike the other three because both parties are not aware of what is going on. Bribery and conflict of interest are the most common types of corruption, at 56 percent and 52.9 percent respectively (284).

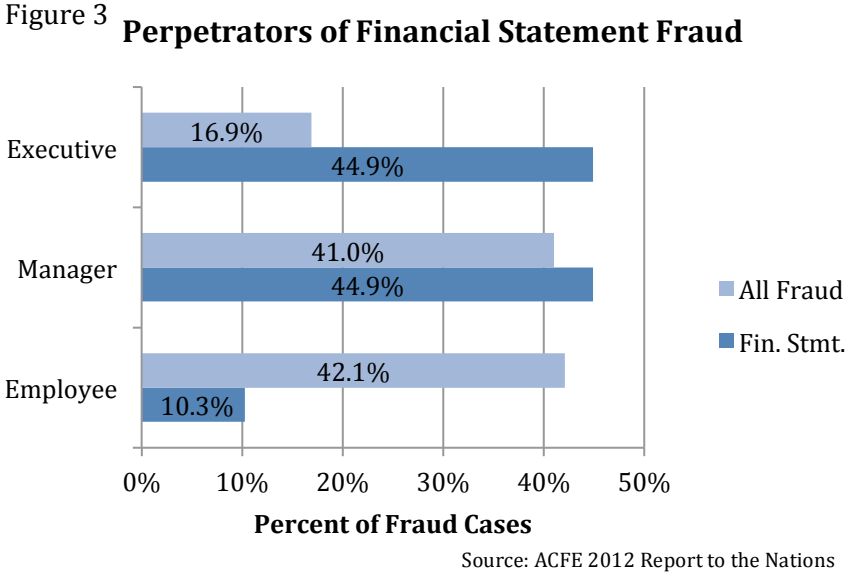
The most common perpetrators for corruption, unlike most other occupational fraud cases, are high level managers and executives since corruption deals with high level decision- making situations and most lower level employees don't have that kind of authority (285). Occupational fraud in the form of corruption is harder to detect when the perpetrator is an executive or high level manager as compared to a lower level employee. The reason for this difficulty is the higher level employees' position of authority and control, which is used to "cover up" the corruption. This difficulty reinforces the

importance of a company establishing a system of checks and balances so that no one person ever has too much control and lack of supervision or review.

The final type of occupational fraud is the use of fraudulent financial statements. This type of fraud is, by far, the most damaging to the victimized investor or company. While it is far less frequent than other types of occupational fraud (only 7.6 percent of reported cases), it has the highest median loss of $1,000,000 (ACFE, 11). Therefore, it is critical for companies to understand this type of fraud in order to detect it as early as possible before the sustained loss increases to such a high level. This type of occupational fraud is also known as "cooking the books" since it involves overstating or understating information on the financial statements depending on the particular situation involved. In most cases fraudulent financial statements are used to make a company appear to be running better than it actually is.

There are five different categories of financial statement fraud: fictitious revenues, asset valuations, concealed liabilities, timing differences, and improper disclosures. The false revenues and asset valuations occur most frequently, in 49.4 and 48.3 percent of reported cases (Wells, 349). Since they are the most commonly altered elements of a company's financial statements, it is extremely important for auditors to give special attention to these areas while going through a company's books. However, this is one of the most difficult types of occupational fraud to detect because of the actual perpetrators, as shown in Figure 3. As with corruption, this type of fraud is most often committed by those with higher power and authority within a company. These fraudsters can make the company's financial statements appear correct and balanced, even though a major fraud is occurring.

Figure 3



Source: ACFE 2012 Report to the Nations

After major corporate scandals, such as WorldCom and Enron, the federal government passed the Sarbanes-Oxley Act of 2002 in an attempt to decrease the amount of financial statement fraud. While this subject will be discussed in further detail, it is important to note at this point of the survey that one of the most important parts of this act requires company executives to sign off on the effectiveness of their internal control system. In larger companies, the external auditor also has to evaluate the control system's effectiveness. Congress hoped this act would help prevent similar corporate scandals caused by financial statement fraud in the future and it seems to have had a good impact so far.

Occupational Fraud in Different Sectors

Since occupational fraud occurs all across the economy, in every possible sector, it is important to compare the differences within these sectors. The most interesting sectors to compare are private companies, not-for-profit companies and governmental agencies. Not only does the amount of fraud among these sectors differ but the way the fraud occurs can differ as well. Occupational fraud also differs within the various industries in our economy. The 2012 RTTN provides some statistics regarding fraud in

different types of organizations. Figures 4 & 5 show the frequency of each organization in fraud cases and the median loss for each organization. It is important to keep in mind that these numbers come from a survey of 1,338 fraud cases, not a complete list of all reported cases. However, they still provide a good insight into the world of occupational fraud in different sectors. The statistics show that occupational fraud occurs most frequently in private companies. One possible explanation for this frequency could be that private companies are not subject to all of the governmental regulations that public companies are, although there are some who voluntarily comply.

Figure 4

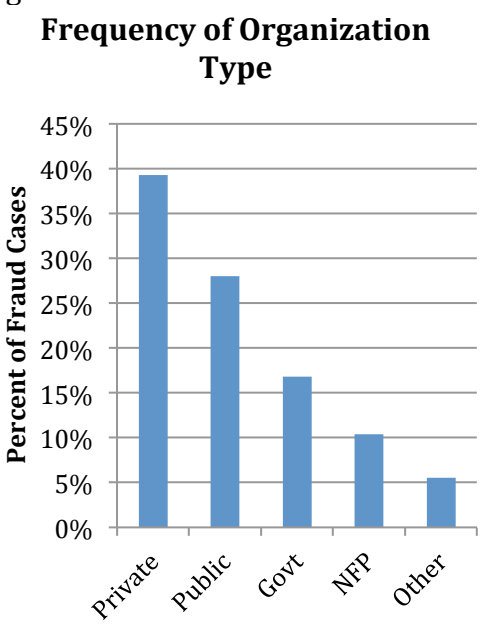
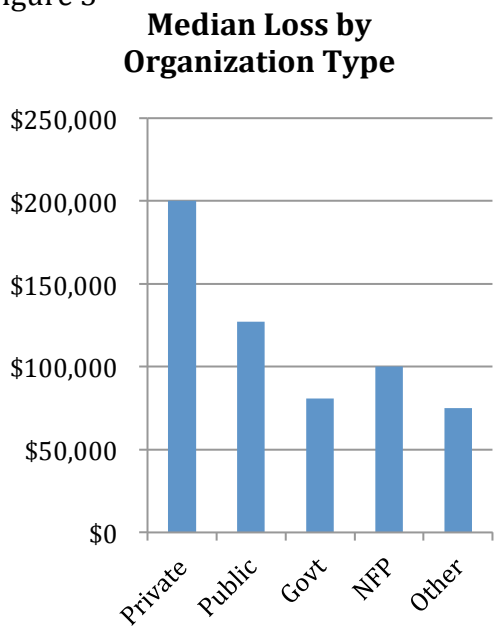


Figure 5



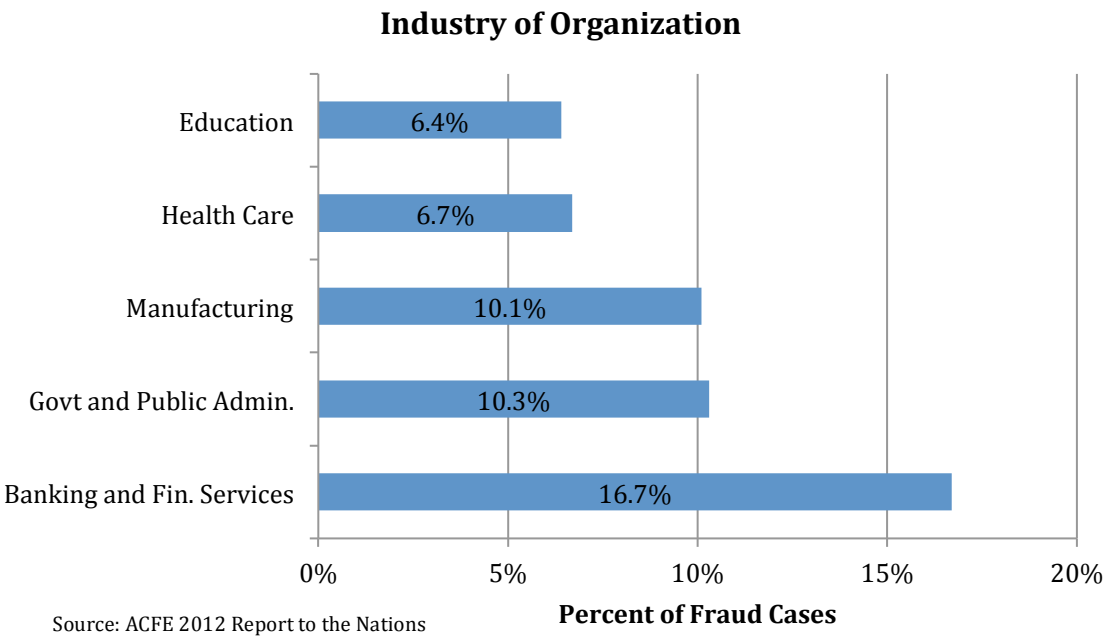
Source: ACFE 2012 Report to the Nations

Governmental agencies are similar to public companies in that they are public organizations and they provide goods and services. However, the major difference is the lack of profit motive in governmental agencies (Dennis, 1-3). According to Lynda Dennis, the pressure that these agencies face is to provide more services using fewer resources (1-2). While many other types of companies are also concerned with cost

reduction, most of their fraudsters commit fraud that shows increases in revenues and earnings. In contrast, governmental agencies are more susceptible to occupational fraud occurring in an attempt to show reduced costs. There is also an increased pressure on government officials because a majority of them are elected by the public and therefore, it is in their personal best interest to keep the public happy. This pressure can, and often does, affect the actions they take and decisions they ultimately make (1-3). Another primary reason that governmental agencies are susceptible to fraud is a lack of necessary accounting staff (3-4). Many of these agencies are operated on a comparatively small budget, which makes it difficult to hire qualified accounting staff. This difficulty makes the agencies more susceptible to fraud, whether intentional or accidental, because of lack of oversight. Even with a small staff, it is important for every public or private organization to keep strong internal controls and to always hire employees with the necessary qualifications to manage and review their financial records.

Not-for-profit companies are different from other companies because they focus on a mission rather than profit. They are still profitable, but the profits do not go to shareholders. They are similar to governmental agencies regarding their susceptibility to occupational fraud because of inefficient internal control systems and small staffs (Dennis 1-5). However, the motivation for occupational fraud in the not-for-profit sector is different from any other sector since they are not profit led. One possible motivation would be to present a more favorable financial situation for potential donors who are the primary source of the funding for this sector. While occupational fraud in this sector is only responsible for about 10.4 percent of reported fraud cases, it still results in a median loss of $100,000 per case (ACFE, 25). This shows that the organizations in this sector

Figure 6



Source: ACFE 2012 Report to the Nations

should still be taking the proper precautions to prevent it.

The last way to really differentiate the sectors of the economy is by industry. Although the 2012 RTTN uses twenty- three different industry classifications, the top three industries consisting of banking and financial services, government and public administration, and manufacturing are responsible for 37 percent of all reported occupational fraud cases (ACFE, 28). The chart above (Figure 6) shows the distribution of the top five industries including healthcare and education. According to their statistics, banking and financial services represent the largest number of occupational fraud cases with a median loss of $232,000 while government and public administration comes in a distant second with a median loss of $100,000. Interestingly, the most common type of occupational fraud in these two industries is corruption, which accounts for about 35 percent of the reported fraud cases (29). This statistic proves that the accountability and oversight of the top level management is critical in both of these industries since they are the ones most likely to commit, or influence, corruption fraud. Another reason these two

industries may be more susceptible to fraud as compared to others could be the larger amounts of money they handle on a regular basis. They both also have an increased pressure from the public to perform well.

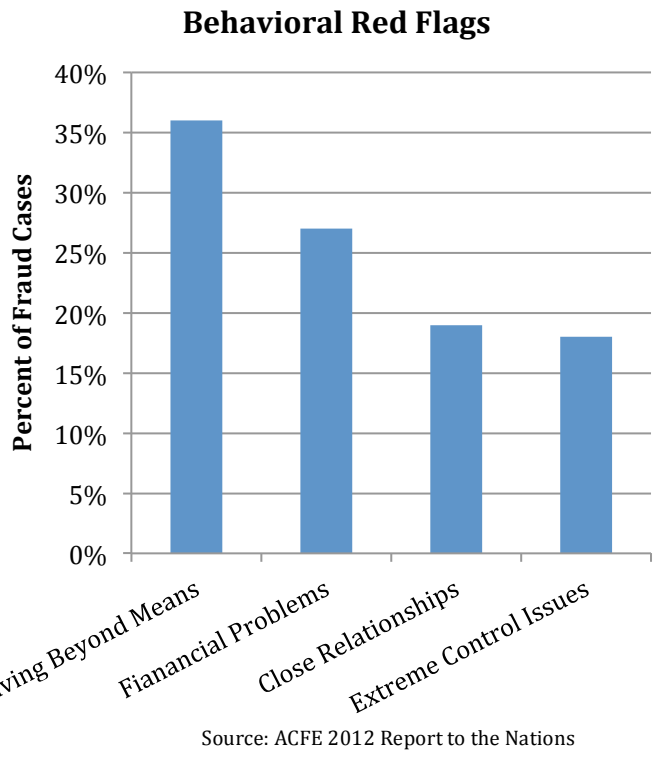
Regardless of the organization or industry, one common theme is the need for internal controls. Research involving all organization types stresses the importance of having an effective internal control system as a key deterrent to occupational fraud. While different studies continue to highlight reasons why one type of organization or industry is more susceptible to occupational fraud than others, these reasons will ultimately relate to the internal controls of the organization. Therefore, the implementation and maintenance of effective internal controls should be a high priority for every company and organization in their efforts to fight occupational fraud.

Typical Fraudster

There are many articles that attempt to define the "typical" fraudster and advise people as to what characteristics to look for. The best that these studies can do is to provide a profile of a typical fraudster as of that particular moment in time because it is a constantly changing concept. KPMG's *Global Profiles of the Fraudster* states the typical fraudster in 2013 was "36-45 years of age, generally acting against his/her own organization...holds a senior management position, employed in excess of six years, and frequently acted in concert with others" (2). The 2012 RTTN found similar results, adding that the perpetrator was more likely to be male, but there were two significant differences. They found it to be more probable that the fraudster worked alone and had only been employed for 1-5 years (44,46,49). As the types of fraud change, so will the

profile of the "typical" fraudster. While it can be difficult to detect a potential fraudster based on the above attributes, there are some common red flags that are easier to detect. Some of these red flags include lifestyle and/or behavioral changes, financial problems, taking no vacation time, a controlling attitude, and unusually close relationships with vendors or customers (Singleton, 128).

Figure 7

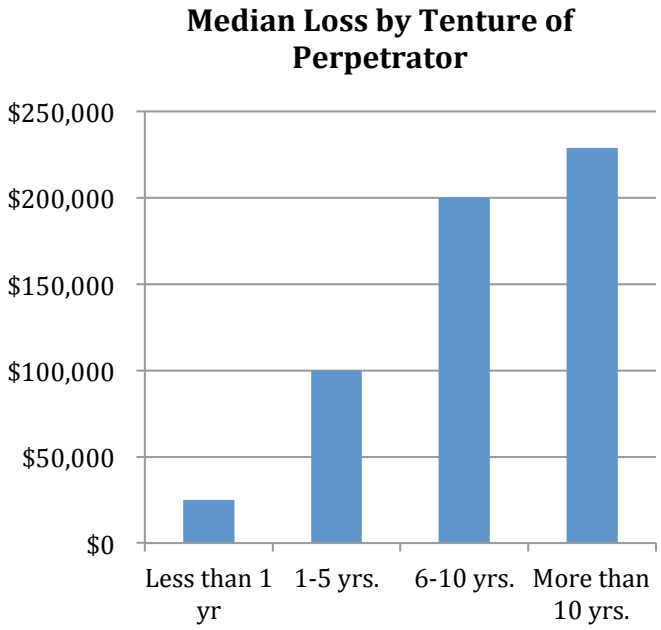


Source: ACFE 2012 Report to the Nations

As Figure 7 shows, living beyond one's means is the most common red flag with financial problems following a close second. Lifestyle changes (living beyond means) are one of the easiest to detect because they are normally very noticeable. The most common example would be the sudden purchase of an extremely nice car or boat out of line with one's household income. Also, if an employee is very controlling of his or her work area and does not like for other people to see what they were working on, that could be another noticeable red flag. When red flags are detected, the best course of action is to investigate further, even if it ends up being a coincidence. It is always best to be safe in those situations than a victim.

An interesting observation made when comparing the various attributes of perpetrators is that there is a direct correlation between those attributes and the financial amount of the fraud. An example of this trend is illustrated in Figure 8 with regard to tenure of employment. An upward trend is also consistent when analyzing position, number of perpetrators working together, gender, and education level. Age is the only demographic that differs because it peaks at the 51-55 year old range with a median loss of $600,000 then starts to decline (ACFE,48). These results lead to the conclusion that the more experienced or higher up in a company a fraudster is, the more fraud they are willing to commit (in terms of dollars). Another factor could be that longer tenure, more education, and/or higher level positions could locate more weaknesses in the internal control systems. The biggest conclusion that can be drawn from this correlation is that many younger, inexperienced fraudsters will start out small so it is important to detect it then, before they gain more confidence and commit greater amounts of fraud.

Figure 8



Source: 2012 ACFE Report to the Nations

Level of Occupational

Fraud Occupational fraud will always be a highly investigated area because it will always be attempted. It is a type of crime that can never be completely stopped, no matter

how much legislation and enforcement exists. One reason for this is the continuing advancement of technology, which allows fraudsters the opportunity to continually develop new and more advanced fraud schemes. Another reason is that there will always be employees with financial problems or job stressors who consider some form of occupational fraud to be their last resort and saving grace.

The frequency of occupational fraud tells an interesting and unpredictable story because one would expect the amount of such fraud to decrease over time. This expectation is due to an increased public knowledge of fraud prosecution and the increasing number of preventive tools made available to every organizational sector. However, the reality is that the frequency of occupational fraud continues to rise. This increase is due primarily to a continuing failure to implement necessary preventive controls. Many organizations are simply too trusting of their employees do not believe that anyone in their organization is capable of committing fraud against them. They believe that the money saved by the company by not implementing as many preventive measures as are needed justify the risk. Unfortunately, most companies do not realize how big of a financial risk they are taking when they make that decision.

PricewaterhouseCoopers' *2014 Global Economic Crime Survey* reports that 45 percent of organizations reported suffering from occupational fraud in the last two years. Of those organizations, over half (56 percent) also reported an increase in the number of fraudulent occurrences over that same time period (PwC, 6). These shocking statistics should serve as an incentive for all organizations to take the necessary actions to protect themselves from fraud.

There are many factors that could influence the level of occupational fraud and one of the main factors is the state of the economy. The rise and fall of the economy has a direct effect on the lives of potential fraudsters and their families. A recession, in particular, would have a significant negative impact because it usually leads to an increase in financial difficulties. Such negative impact, in turn, leads to increased pressure to provide for their families, to make debt payments on time, etc. As previously discussed, pressure is one of the first elements of fraud and once that pressure increases, the rest of the elements begin to fall into place. During such times of crisis in the economy, organizations should implement additional safeguards for an increased awareness of potential red flags for occupational fraud.

Cyber-Fraud

Cyber-fraud is one of the biggest concerns in today's business economy because it is a fast-growing concept. By the same token, cyber-security has become one of the priorities in organizational financial security. The realization that cyber-fraud is a real threat to any company has increased significantly over the last two years, just think about the recent Target® debit card crisis. According to PwC, 71 percent of US respondents indicated their perception of the risks of cyber-crime increased over the past 24 months, rising 10 percent from 2011 (14). It is also important to note that, of the companies reporting occupational fraud incidents, 44 percent had experienced some form of cyber-crime (14). Because of this rising trend, many organizations are making sure that they implement cyber-security initiatives to help deter cyber-fraud.

One continuing problem with cyber-fraud and related cyber-security initiatives is

the ever changing face of technology. Technological changes and advances continually provide fraudsters with new innovative ways to commit fraud. In fact, many people who are tech-savvy can easily find ways around the basic controls that many organizations have in place. Instead of being fearful of the every changing face of technology, companies should embrace it and stay ahead of the game because changing technology contributes just as much to fraud prevention as it does to fraud. The threat of cyber-fraud is not going to disappear so it is up to an organization to use new technology in their favor.

Another concern with new cyber-security initiatives is how varying political views and policies will affect them. One such problem is that cyber-fraud is often times considered borderless because a fraudster does not have to physically be in the United States to commit fraud against an organization. Cloud-computing, using remote Internet servers to store data, also creates numerous challenges because of the many different cloud providers. This diversity creates jurisdictional issues because of the multiple countries involved and various geographical limitations (Manning, 2). Therefore, it is critical that organizations have as much information about any cloud provider they use to store information. Since cyber-fraud is still relatively new, it will be important to see what policies are put into place in terms of creating applicable regulations.

Storing information "in the cloud" also creates an increased fraud risk for companies because their information is more accessible to tech-savvy hackers. As previously mentioned, Target® is a recent example of a company losing important personal information of its customers that it thought was secure. Because of the potential for such security breaches, organizations should have specialists who can stay up-to-date

on security measures to keep the private information of a company as secure as possible. This need for increased security measures is important because the ramifications of this type of security breach are more than just losing private information; they have the potential to cause dramatic financial losses to an organization because potential customers would be afraid that their personal information would not be protected. In the world of ever-increasing technology, data security must be one of the top concerns for any company. Data security is no longer just a minor job of the IT department, but a major concern of the business as a whole.

Laws/Policies against Occupational Fraud

In recent years, numerous steps have been taken, both externally through legislation and internally through company policies, to attempt to combat the growing number of occupational fraud instances. The federal government has enacted several pieces of legislation to increase fraud prevention, such as the Sarbanes-Oxley Act, the Dodd-Frank Act and the Federal Sentencing Guidelines. The AICPA issues standards, such as SAS 99, that relate to fraud in financial statements. While these regulations are important and deter some fraud, they cannot stop it all. For this reason, internal measures a company takes are vitally important beginning with a code of employee conduct and continuing into the establishment of an internal control system and fraud risk management program. As always, the best prevention a company has against occupational fraud is the strength of its internal system.

It is important to have an understanding of the existing external regulations before discussing the necessary internal measures of a company. One of the most important acts

of legislation in the last twenty years is the Sarbanes-Oxley Act (SOX) which was implemented in 2002, following the scandals of WorldCom and Enron. SOX 404 is focused on the internal controls of an organization. The first part of 404 requires the management of a company to regularly evaluate the effectiveness of their internal control system. The second part requires accelerated filing companies (public float of over $75 million) to have an external auditor routinely attest to the effectiveness of their internal control system. These requirements were intended to increase investor safety by making sure a company's internal control system did not have any weaknesses. Overall, the Act highlights the importance of internal controls and attempts to require them to be effective.

The Dodd-Frank Act was put into place in 2010 and is best known for establishing a bounty program for whistle-blowers. Under this Act, if someone provides the Securities and Exchange Commission (SEC) with reliable information about a potential fraud, they can receive a monetary award. This award does not apply to everyone that has a tip of any kind. The information must lead to a large incident of fraud (monetary sanctions over $1 million) and, even then, there are exceptions (KPMG, 33). It is important to note that whistle-blowing is a very successful method of detection. According to the 2012 RTTN, 43.3 percent of fraud cases were initially detected by tips (ACFE, 14). That number has been on the rise illustrating the key role that whistle-blowing has in the detection of occupational fraud.

The United States Federal Sentencing Guidelines establish requirements for an effective compliance and ethics program. The 2012 Guidelines Manual states that "to have an effective compliance and ethics program...an organization shall – 1) exercise due diligence to prevent and detect criminal conduct and 2) otherwise promote an

organizational culture that encourages ethical conduct and a commitment to compliance with the law" (USSC). The guidelines recommend employee training programs so that all employees understand what is expected by the company when it comes to ethics and compliance (KPMG, 32). Their main focus is to create a culture of compliance within a company, starting with top level executives and moving down the ladder from there. If it is well known that compliance is an expected part of company culture, it could serve as a deterrent to future fraudulent activity.

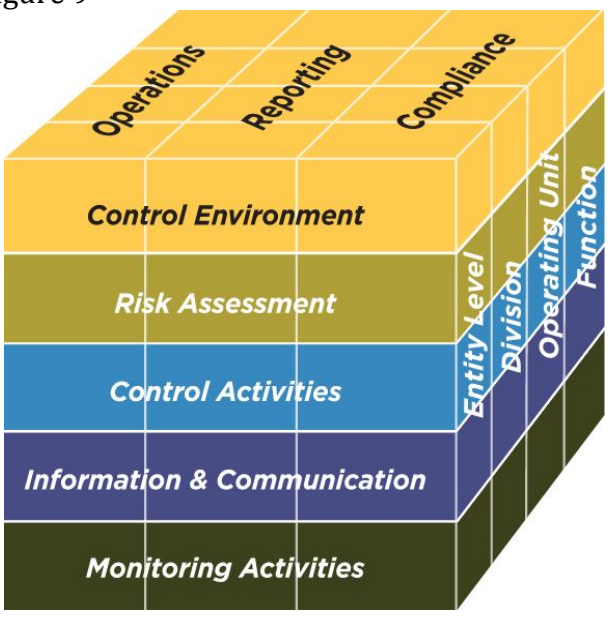
Although many of these external regulations set standards for the internal operations of a company, it is still up to the company to put everything into place. A recent study done by the AICPA found that there are three main actions a company should take to help fight fraud: "(1) creating a culture of honesty and high ethics, (2) evaluating antifraud processes and controls, and (3) developing an appropriate oversight process" (Biegelman 113). The creation of an honest company culture obviously must start with the "tone at the top". It is important for the high level executives to act in a way that reflects the behavior expected from lower-level employees. If a company not only establishes a strong, ethical code of conduct but also makes sure that it is followed throughout the entire company, then they will be one significant step closer to having a strong fraud prevention initiative.

Although there are different elements to the internal measures a company should take, they all fall under the umbrella of fraud risk management. The three sections of any such anti- fraud program are prevention, detection, and response (KPMG, 4). Fraud prevention is the most important of the three because, if properly carried out, detection and response are not needed. Unfortunately, many companies do not realize the

importance of occupational fraud prevention because they do not believe fraud could happen to them. It is critical then that companies are educated as to how necessary a good fraud prevention program is in any industry.

Fraud prevention can encompass many different elements, but the most well-known elements are internal controls and audits. By definition, preventive controls are anything "designed to help reduce the risk of fraud and misconduct from occurring in the first place" (KPMG,11). A key feature of preventive measures is regular training for employees so that they are made aware of the company's fraud prevention values and policies. According to KPMG's 2013 Forensic Integrity Survey, 59 percent of employees said that if they "were to violate standards of conduct, it would be because they lack familiarity with the standards that apply to their job" (KPMG, 15). This high percentage should be a wake-up call to executives that employee training is a must to educate them regarding the code of conduct and other company policies as a part of their fraud prevention program.

Figure 9



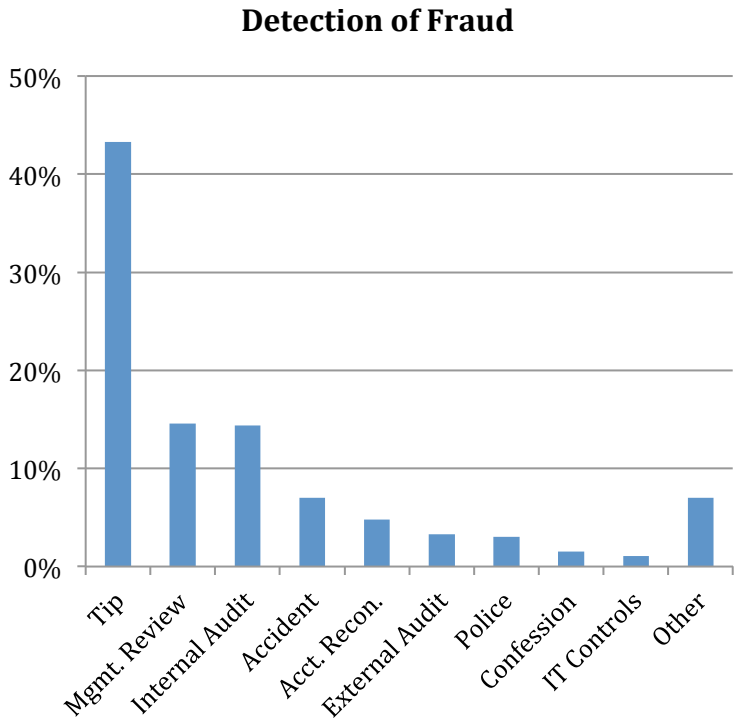
Source: COSO Internal Controls-Integrated Framework

Although internal controls have always been the most important preventive measure, even more importance was placed on them after SOX 404 was implemented. As a result, many companies were forced to reevaluate their internal control system to make it more effective.

The Committee of Sponsoring Organizations of the Treadway Commission (COSO) has created an Internal Control – Integrated Framework that is used to help assist companies in the creation of effective control systems (COSO, 3). The cube in Figure 9 shows the relationship between the objectives (operations, reporting, compliance), components (control environment, risk assessment, control activities, information and communication, monitoring activities), and the organizational structure (COSO, 6). The five components work together as an integrated unit within all areas of a company's organizational structure and through each objective. When a control system consists of all five components working together then it is considered effective under the Internal Control-Integrated Framework. One part of the internal audit function is evaluating these controls. The internal auditors conduct evaluations for both the internal controls and the anti-fraud programs as a whole then report their findings to the audit committee (KPMG, 12). The use of internal audits allows the controls to be tested so their actual operation can be evaluated. The audit results educate company executives as to which areas in the anti-fraud programs need to be strengthened in order to prevent occupational fraud.

On the other hand, detective controls are put into place to find the fraud when it occurs. They are important because, the quicker the fraud is discovered, the lower the financial loss to the victimized company. Figure 10 depicts the most frequent methods of fraud detections and shows that tips are by far the most common method of detection. Accordingly, it is important for companies to have a system in place to receive tips about possible fraud. For this purpose, many companies use a hotline that is both anonymous and confidential (KPMG,17). The 2012 RTTN reported that "organizations with some form of hotline in place saw a much higher likelihood that a fraud would be detected by a

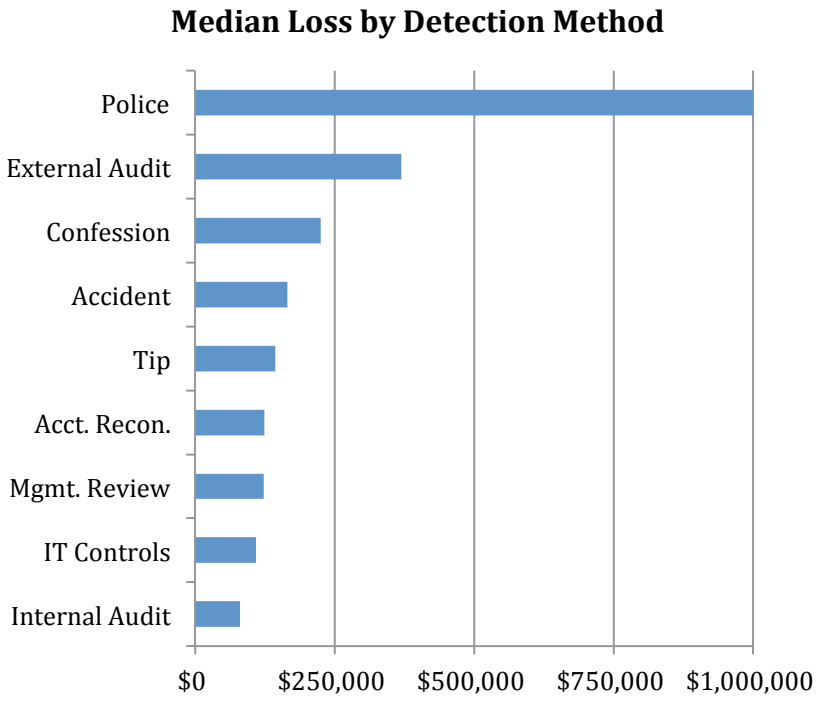
Figure 10



Source: ACFE 2012 Report to the Nations

tip (51 percent) than organizations without such a hotline (35 percent)" (ACFE, 16). It is also important to note that median losses from fraud incidents detected by proactive measures were much less (Figure 11) than those detected by outside factors (ACFE, 15). Those results show the importance of having strong detective controls in case the preventive controls fail. Detecting the fraud early on through internal measures could save companies hundreds of thousands of dollars in losses.

Figure 11



Source: ACFE 2012 Report to the Nations

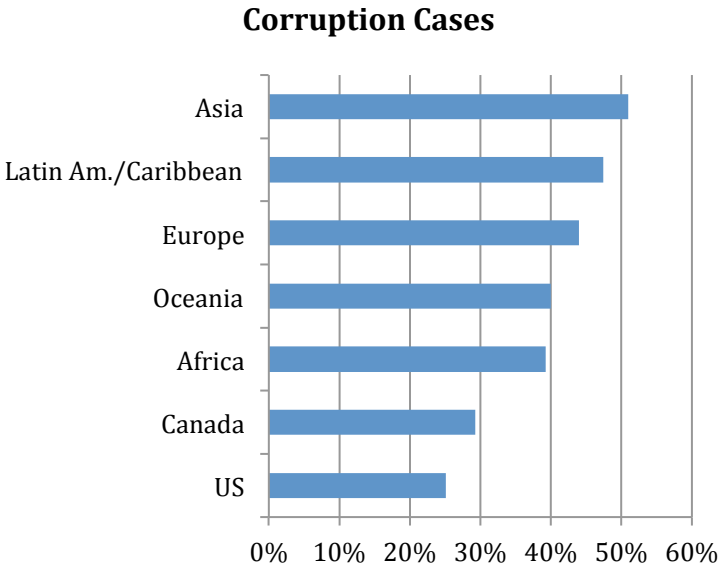
The last element of fraud risk management is response. This element consists of the measures taken after the fraud is detected to attempt to repair the harm caused by the

fraud. Most companies (65.2 percent) choose to report their case to the police. However, the top reasons for companies not reporting incidents of fraud (34.8 percent of cases) were fear of bad publicity and sufficient internal disciplinary actions. In the cases studied in the 2012 RTTN, only 15.8 percent recovered all of the losses related to the fraud while 48.7 percent did not recover any of the losses (ACFE, 61,64). The fact that almost half of the companies who experience fraud are unable to recover any of their losses highlights the importance of strong preventive controls. If those controls are effective and prevent fraud from occurring in the first place, then they will be able to protect a company from the thousands they could lose as a result of occupational fraud.

Global Considerations

The topic of global occupational fraud usually revolves around corruption. This fact is not surprising, considering corruption is the leading type of fraud in most areas (Figure 12). It is important to note that while the information from the 2012 RTTN does not report on all the fraud in those localities, it does give a general idea as to the varying degrees of corruption. Many countries, including the United States, have developed regulations regarding corruption in an attempt to stop this increasing trend.

Figure 12



Source: 2012 ACFE Report to the Nations

The United States implemented the Foreign Corrupt Practices Act (FCPA) in 1977 and it is often thought of as the standard to which other countries refer to when creating their own corruption legislation. The FCPA focuses its provisions on anti-bribery as well as corporate books and records. The anti-bribery provisions "prohibit directly or indirectly offering anything of value to any foreign official for the purpose of corruptly influencing the decision of that official to do anything that assists the offeror in the obtaining or retaining of business or an unfair business advantage" (LexMundi, 13). The books and records provisions require that companies not only keep accurate and detailed records but also have effective internal compliance controls (13). The FCPA is being enforced more heavily now than it was when it was first implemented; most likely as the result of an increase of global corruption. The FCPA also has an expansive reach, which requires all international businesses to be aware of its provisions. The Act applies to any individual or firm "who causes, directly or through agents, an act in futherance of corrupt payment to take place within the territory of the United States" (LexMundi, 13). The extensive reach and strict enforcement make the FCPA one of the most effective pieces of regulation concerning corruption of all time.

The United Kingdom established a similar Act when it enacted the Bribery Act of 2010. That Act has a broader scope than the FCPA in a few different areas. First, it includes all commercial activites, whether public or private. Secondly, it applies to bribes to any perosn, not only foreign officials. Under the Bribery Act, one can also be punished for receiving a bribe. Lastly, an organization is considered to be at fault under the Act if it does not prevent bribery by having effective preventive procedures in place (Gauci). The reach of the Act applies to any individual or organization that gives or receives a bribe in

the U.K. It also applies to any U.K. resident or citizen who commits these acts in a foreign country. The same goes for any act committed by an organization incorporated in the U.K. (LexMundi, 19). The broader scope of the Bribery Act 2010, as compared with the FCPA of 1977, shows that governments are becoming more concerned with the corruption that is occurring all over the world.

The United Kingdom is not the only country that has recently enacted anti-corruption legislation. Many countries throughout the world have taken note of the need for increased corruption policies. There are anti-corruption instruments, such as the *United Nations Convention against Corruption* and the *Convention on Combating Bribery of Foreign Officials in International Business Transactions*, that many countries have ratified. In 2011, China enacted the Eighth Amendment to the Criminal Law, which is similar to the FCPA. All of these efforts by numerous countries to prevent corruption and punish those who engage in it illustrate a growing awareness of the corruption problem and a resulting global initiative to combat said corruption. Many countries are recognizing a need for national regulation surrounding the corruption issue. It is important that most of the international regulations are similar because international companies can implement compliance initiatives that meet the requirements of multiple nations. It is also important that each country enforces a similar policy on corruption because it is such a global problem. Strict enforcement across the globe should help decrease the instances of corruption.

Undetected Occupational

Fraud Occupational fraud is constantly being reported and investigated in

companies all over the world but the unfortunate reality is that most fraud will go undetected. This lack of detection seems reasonable considering the fact that one of the most important aspects of committing fraud is the ability to hide it. Because of that aspect, it is extremely important for companies to have high-quality detection controls. However, there are cases when the perpetrator is experienced and has enough knowledge of company controls that they can make the fraud look legitimate which allows it to go undetected for an extended period of time. This type of undetected fraud can have dire consequences even if it is eventually detected because of the larger losses that usually result.

The most obvious ramification of undetected fraud is the loss of capital. It does not matter whether the fraud is petty theft or a major underreporting of income, there will always be losses to the company. Even if the fraud is detected, it is extremely unlikely that any of the funds will be recovered. Undetected fraud also results in incorrect financial statements, which could lead to problems with the SEC for issuing incorrect information. However, one of the biggest consequences of undetected fraud occurs when it is actually detected, especially in the case of fraudulent financial statements. Occupational fraud can result in major fines and possibly jail time. It can also lead to the ultimate closure of a company. These are just a few examples that illustrate why it is so important to detect fraud as early as possible.

Aside from dire financial consequences, undetected occupational fraud also affects the public image of a company. If the public becomes aware that a company had a large amount of undetected fraud, they may not feel comfortable using the services of that company or providing them with any of their financial information in the future. This

fraud consequence occurs no matter the size of the company or the size of the fraud. The public does not approve of any corporate mismanagement including occupational fraud and, when faced with the decision of which company to use, for their personal or business needs, many would choose the organization that has not had a problem with fraud. The impact of this public perception could put a company out of business just as quickly as financial problems because an organization needs clients and customers to continue making money.

Assurance Opportunities

Fraud creates many opportunities for accounting firms, whether it is helping with the actual detection of fraud or implementing an anti-fraud program. They can provide any type of fraud-related services a company needs. One of the most common assurance opportunities is the investigation of financial activity. The accounting professionals can help companies identify possible instances of fraud by locating inconsistencies in financial statements or records. Another opportunity for assurance professionals is helping test the effectiveness of internal controls. They can help organizations discover which areas of their controls puts them at the most risk for fraud and also help them implement better controls. Companies can receive assistance with creating anti-fraud programs that comply with the different regulations relating to fraud and establishing effective preventive controls and early detection methods. It is also important that the accounting professionals educate the company on the importance of making improvements to their controls to continually keep them up-to-date. While some of these services can be expensive, depending particularly on the size of the organization at issue, it is always better than the potential losses that fraud could cause.

Although there are different methods of fraud investigation, almost every method includes analyzing the company's financial information and interviewing the company's employees. In today's world of ever changing technology, it is necessary to have someone who is familiar with computers to help retrieve needed information because most companies have their financial information stored on computers rather than on paper. It would also be safe to assume that the investigative team would be examining all the computer activity on employees' computers to look for any possible evidence of fraud. This examination could require some expert IT knowledge. Using the information that is gathered, the accounting professionals can run various tests to help highlight possible instances of fraud. The audit interview process is also important because the interviewer could pick up on behavioral cues from different employees or managers. If they notice some potential red flags then it could help focus them on certain employees in the investigative process. It is also possible that some employees will provide information about fraudulent instances they are aware of if asked directly in an interview setting. Assurance professionals use the new technologies available and old-fashioned interview tactics to help get any useful information in fraud investigations in order to provide the most accurate results.

Assurance Work Plan to Investigate Fraud

The first part of planning a fraud engagement is deciding whether or not your audit team is qualified to perform the particular task at issue. You could decide that your team does not have the necessary expertise and seek additional help or you could decide that you are in fact well-qualified. Once a fraud engagement is accepted, it is important to gather the best team. Most fraud investigative teams are made up of people from multiple

staff levels of the firm: a partner, managers, seniors, and associates. Each team member has a different responsibility within the engagement. When investigating fraud, it is necessary to make sure the team includes someone with years of experience dealing with fraud. It is also important to have someone with an IT background because it usually requires some above-average computer skills to obtain all the needed information. Sometimes the engagement requires the help of a consultant or fraud specialist should a situation arise that is above the skill level of the engagement team. It is always better to stay on the safe side and ask for a second opinion.

When planning the fraud engagement, it is imperative to determine what the end goal is and to get a general idea of what you are looking for so you can determine what risks and controls could affect the planning process. It is important to know about any history of fraud in the organization and also any known problem control areas so that the team can identify initial areas to focus on. It would also be helpful to the overall plan if the team evaluated the occupational fraud risk of different areas of the organization. This evaluation means that they should consider which area could be facing the most pressure or have the greatest opportunity for fraud.

A fraud investigation engagement team should consider all possible risks of the organization that could potentially lead to fraud. Some examples of these possible risks are the company's profitability, the tenure of the management, and complex accounting issues. Such risks could all be the initial cause of fraud. It is also important to evaluate the internal controls of the organization because weak internal controls put them at a significantly higher risk for fraud.

When conducting a fraud investigation, most teams will be looking for concrete evidence of whether or not fraudulent activity has occurred. In order to attest to the existence of occupational fraud, the team would have to have substantial evidence so that they could track down the exact fraud and fraudster. When the objective is to help test controls and provide information on what areas are most at risk then the evidence would not have to be quite as concrete. The latter objective is simply their professional opinion on what controls could use improvements and what their recommendations for improvement are. Regardless of what specific services the fraud team is providing, their results should be able to be relied upon by the company paying for their services. As accounting professionals, it is the team's obligation to present accurate findings that stakeholders can trust to reflect the on goings of an organization.

Proposal for Fraud Prevention Business

Obviously, the best way to minimize losses by fraud is through fraud prevention. So many organizations think they do not have to be proactive in their prevention efforts but they are usually the ones who get hit the hardest. The 2012 RTTN reported that organizations typically lose 5 percent of their annual revenue to fraud. It does not matter whether it is a small local business or a large multinational corporation, 5 percent is a lot of revenue to be giving away. It is also important to keep in mind that over half of the organizations with instances of fraud do not recover any of the losses (ACFE, 4). Therefore, it is clear that fraud prevention is necessary in all companies and organizations. In addition, the cost of implementing fraud prevention programs is far less than the cost of having fraud occur. Lastly, once fraud occurs, it is not only money or other assets that are lost but the public image of the company is damaged as well and that

is something a business might never recover from.

There are different methods of fraud prevention; it is not "one size fits all". Accordingly, the business size, industry, and previous fraud risk should all be considered when developing the right anti-fraud initiative. Larger companies usually require the most protection because they have a larger number of vulnerable areas. They also typically have the financial ability to implement a more comprehensive program. Because of this, small organizations suffer the largest median losses and they implement fewer controls (ACFE, 4). This leaves the business as a whole at a higher risk of fraud. It is important for businesses to determine what they can afford and what type of program would be the best fit for their company but they must realize the need for some controls.

There are other measures, aside from costly controls, that companies should take advantage of. The attitude of the company starts with the way the executives carry themselves because it is usually the top-level management or Board of Directors that creates the company's code of conduct. If compliance and ethical conduct starts at the top, it is more likely to get carried out all the way through the organization. Another key to successful fraud prevention programs is having hotlines available to make anonymous reports of suspected fraud. It has been said that "the most effective deterrent to fraud is a strong 'perception of detection'" (Adams, 59). Just having a hotline available can help deter potential fraud because it increases the perception of a company's strong detection controls.

The type of fraud prevention program that is chosen by a company will not matter if it is not implemented effectively. Effective implementation requires extensive training

programs and mandatory meetings with employees to outline what preventive measures are being taken. Employees should also have a firm understanding of the code of conduct and what is expected of them. When management sets an example, it helps the employees know how they are expected to conduct themselves. Another part of successful implementation is continually evaluating the preventive and detective controls and making improvements when necessary. If organizations implement and continually improve an effective fraud prevention program, they could save themselves from all the negative ramifications that fraud can cause. By doing so, they are protecting the future success of their business.

Conclusion

It is hard to understand how fraud can be causing millions of dollars in losses each year when there are so many ways to prevent it. If organizations, big and small, begin to take the threat of fraud seriously then that number could easily be cut in half. Change starts with executives making the decision to educate employees on conduct and potential fraud then implementing anti-fraud programs into their organization. New technology is creating advanced, automated programs that help identify red flags. The most important thing is to let employees and shareholders know that fraud is being taken seriously. This pro-active policy helps deter fraudulent acts from employees and reassures shareholders that they have made a safe investment. Fraud prevention is one of the most important steps to take when creating a successful and long-lasting organization.

WORKS CITED

Adams, Gary W., Campbell, David R., Campbell, Mary, Rose, Michael P. (2006). Fraud Prevention. *The CPA Journal*, 76(1), 56-59.

Albrecht, Chad, Kranacher, Mary-Jo, Albrecht, Steve. *Asset Misappropriation Research White Paper for the Institute for Fraud Prevention*. Retrieved on April 2, 2014, from http://www.theifp.org/research-grants/IFP-Whitepaper-5.pdf

Association of Certified Fraud Examiners. (2012). *2012 Report to the Nations on Occupational Fraud and Abuse.*

Biegelman, Martin T., Bartow, Joel T. (2006). *Executive Roadmap to Fraud Prevention and Internal Control*. Hoboken, NJ: John Wiley & Sons.

COSO. (2013). *Internal Control-Integrated Framework Executive Summary*.

Dennis, Lynda M. (2009). *Guide to Fraud in Governmental and Not-for-Profit Environments*. New York, NY: AICPA.

Dorminey, Jack W., Fleming, A. Scott, Kranacher, Mary-Jo, Riley Jr., Richard A. (2011). Beyond the Fraud Triangle. *Fraud Magazine*. Retrieved April 4, 2014, from http://www.fraud-magazine.com/article.aspx?id=4294970127

Gauci, Geoffrey, Fisher, Jessica. (2011). The UK Bribery Act and the US FCPA: Key Differences. Retrieved April 4, 2014, from http://www.acc.com/legalresources/quick counsel/ukbafcpa.cfm

KPMG. (2013). *Fraud Risk Management*.

KPMG. (2013). *Global Profiles of the Fraudster*.

LexMundi. (2013). *Best Practices in Preventing Fraud and Corruption in a Global Business.*

Manning, Walt. (2011). Investigating in the Clouds. *Fraud Magazine*. Retrieved April 2, 2014, from http://www.fraud-magazine.com/article.aspx?id=4294970016

PricewaterhouseCoopers. (2014). *2014 Global Economic Crime Survey – US Supplement.*

Singleton, Tommie, Singleton, Aaron, Bologna, Jack, Lindquist, Robert. (2006). *Fraud Auditing. and Forensic Accounting*. Hoboken, NJ: John Wiley & Sons.

United States Sentencing Commission. (2012). Chapter Eight – Sentencing of Organizations. *2012 Guidelines Manual*, §8B2.1.

Wells, Joseph T., (2011). *Corporate Fraud Handbook*. Hoboken, NJ: John Wiley & Sons.