ACCOUNTING FOR PROFIT: HOW CRIME ACTIVITY CAN COST YOU YOUR BUSINESS

Linda A. Bressler, Southeastern Oklahoma State University
Martin S. Bressler, Southeastern Oklahoma State University

ABSTRACT

Starting a new business venture and still being in operation after five years can be a significant challenge. According to the U.S. Small Business Administration (SBA), half of all small businesses fail within the first five years, and according to the U.S. Chamber of Commerce, as many as 30% of small business failures can be attributed to crime.

Today, small business owners are subject to assault by many different types of criminal activities ranging from shoplifting and vandalism to fraud, embezzlement, money laundering and of course, cybercrime. Crimes committed against businesses fall into two broad categories—internal and external. Internal crimes include crimes such as theft and embezzlement, while external crimes include activities such as robbery and cybercrime. Each type of crime has its unique characteristics, and each calls for a different approach to prevent and detect criminal activity, along with various remedies to criminal acts.

Accountants can play a significant role in these activities including development of comprehensive audits, utilizing specialized computer software, and vigilance in looking for suspicious activity by employees, customers, suppliers, and others. In this paper, the authors provide an introduction to criminal business activity, and a variety of counter-measures businesses can employ to safeguard their profits.

INTRODUCTION

Small and medium-sized enterprises (SME's) can be considered to play an essential role in a country's economy (Chakraborty, 2015). Effective internal controls can help these companies be successful in reducing fraud in their organizations. SME's will most likely put into place a few controls, but these entrepreneurs probably will not be trained in the latest fraud prevention techniques and internal controls that would benefit small businesses (Oseifuah, 2013). Small companies will often be targets of fraud and theft as they lack the means, experience, proficiency to set up security systems to protect their businesses (Stone, 2016). The author also indicated that the informality of how many small businesses operate could cause havoc regarding the implementation of access and authorization internal controls. Jackson, et al. (2010) noted that small companies often expect employees to function in various jobs within the business and that can be almost impossible to create an adequate segregation of duties. The authors told of an owner of a small trucking company who was very confident that his employees could not steal from him because he only had the authority to write checks. The owner seemed to forget that he gave his bookkeeper the responsibility to reconcile his checkbook as well as a wide-variety of accounting and financial responsibilities.

Also, a small business may not know to keep essential transaction records or may not know how to hire/find ethical employees through the use of credit checks, police records, etc. Another important point could be how employees at a small business may be able to access records they need not be viewing. So, the inherent risk of small business could make it easier for employees to steal, sell company information and commit fraud (Jackson, 2010). Joseph (2009) spoke of an employee at a local pawn shop caught loading merchandise into his truck after hours. Now, this employee's behavior was particularly brazen, but fraud can be considered more commonplace in recent years.

Can there be a fraud profile for which entrepreneurs can be aware of when hiring employees? Eaton & Korach (2016) indicates that one exists. The authors suggest that criminal profiling can be helpful when noting attitudinal and personality aspects of prospective employees. The first trait will be a classic use of power for personal or company gain. Now, not all leaders should be considered unethical, and many do indeed have integrity and behave honorably. Two types of authority dealing with fraud profiling can be traditional and charismatic. Traditional power can be noted in family-owned businesses or private businesses and subordinates working for a manager or owner with traditional power will not oppose the authority figure previously established as the boss or the son or daughter of the boss. Charismatic power comes from the manager's personality which should not be considered a negative attribute, but can decrease or eliminate an established internal control environment.

It would be natural for an entrepreneur who will usually be capable, ambitious, focused, and self-confident with a passion for success to possibly pressure their employees to look away when the entrepreneur chooses to act unethically (Eaton & Korach, 2016). The authors noted that specific industries are correlated with being more likely to employ unethical practices. Also, studies indicated (Daboub, 1995) that specific industries follow the norms and trends of fraudulent activity. Also, (Simpson, 1986) noted that certain industries demonstrate certain cultures and norms and in (Dalton & Kesner, 1988) and Ramamoorti's (2009) study the authors provided ABC's to aid individuals with sociological perspectives on how culture may facilitate crime. The authors' theory described: A: (individuals), B: bad Bushels (subgroups), and C: bad Crops (overall group) and that "with opportunity, a firm's culture can facilitate the creation of bad bushels or bad crops that influence unethical or even criminal behavior on an individual level" (Eaton & Korach, p 135, 2016).

As a business matures, survival rates drop to about half within five years (U.S. Small Business Administration, Small Business Facts). After years of gathering information and intensive study, two meaningful conclusions can be drawn from the Small Business Administration (SBA) data. First, business survival rates have not changed much over the last twenty years or so. Second, survival rates are similar across various industries. This suggests that both downturns and upturns in the economy have little effect and that certain types of new business ventures are not necessarily riskier than others to start.

Small businesses are victims of many types of crimes. One of the most significant studies of small business crime, Kuratko et al. (2000) found annual cost of crime prevention to be $7,805 and the yearly average crime loss to be $9,010. Despite crime being a factor in small business survival, many small business owners appear to be reluctant to report crime. Kennedy & Reilly

(2014) found only 16% of small business owners who had victimized by employee theft reported the incident to the police. In their study, the researchers also found that most theft occurs over time, in some cases as many as twenty years. The researchers also found that on average, employee theft took place over a period of 16 months.

Of course, this is not a problem only in the United States but rather a global issue. According to the National White Collar Crime Center, in 2013 losses worldwide are reported to be $3.7 trillion. Corporate security experts also estimate employee theft to be as high as 25-40 percent of all employees stealing from their employers. An estimated 30 to 50 percent of business failures are attributed to employee theft, making employee theft two to three times more costly than all crimes combined. Security experts also estimate that as many as three-quarters of all employees steal from their employers at least once (National White Collar Crime Center).

Table 1. Crimes committed against businesses

EXTERNAL	INTERNAL
Robbery	Theft
Burglary	Embezzlement
Shoplifting	Fraud
Counterfeiting	Customer Identity Theft
Piracy	Sabotage
Money laundering	
Vandalism	
Cyber-crimes	
Ponzi schemes	

DISCUSSION

Crimes from within

Internal crimes are those committed by employees, including family members. The most common crime committed by employees is fraud and for fraud to occur, Marten and Edwards (2005) state that employees can commit fraud when three conditions are present. The incentive is the first condition, that is, an employee might be motivated to commit fraud due to *financial pressures* resulting from costly medical bills or some form of addiction, or even an adulterous relationship. The second condition is *opportunity* which exists when there is a lack of safeguards or preventive measures, oftentimes resulting from too much trust of their employees. The third condition, *rationalization*, occurs when an employee believes their actions to be justified as the employer "owes them." These conditions are described in Cressey's Fraud Triangle in Figure 1 below.

The Association of Certified Fraud Examiners (ACFE), reports fraud losses in small businesses to be 100 times greater than larger companies. According to the ACFE's "2006 Report to the Nation on Occupational Fraud and Abuse," "The median [fraud] loss suffered by

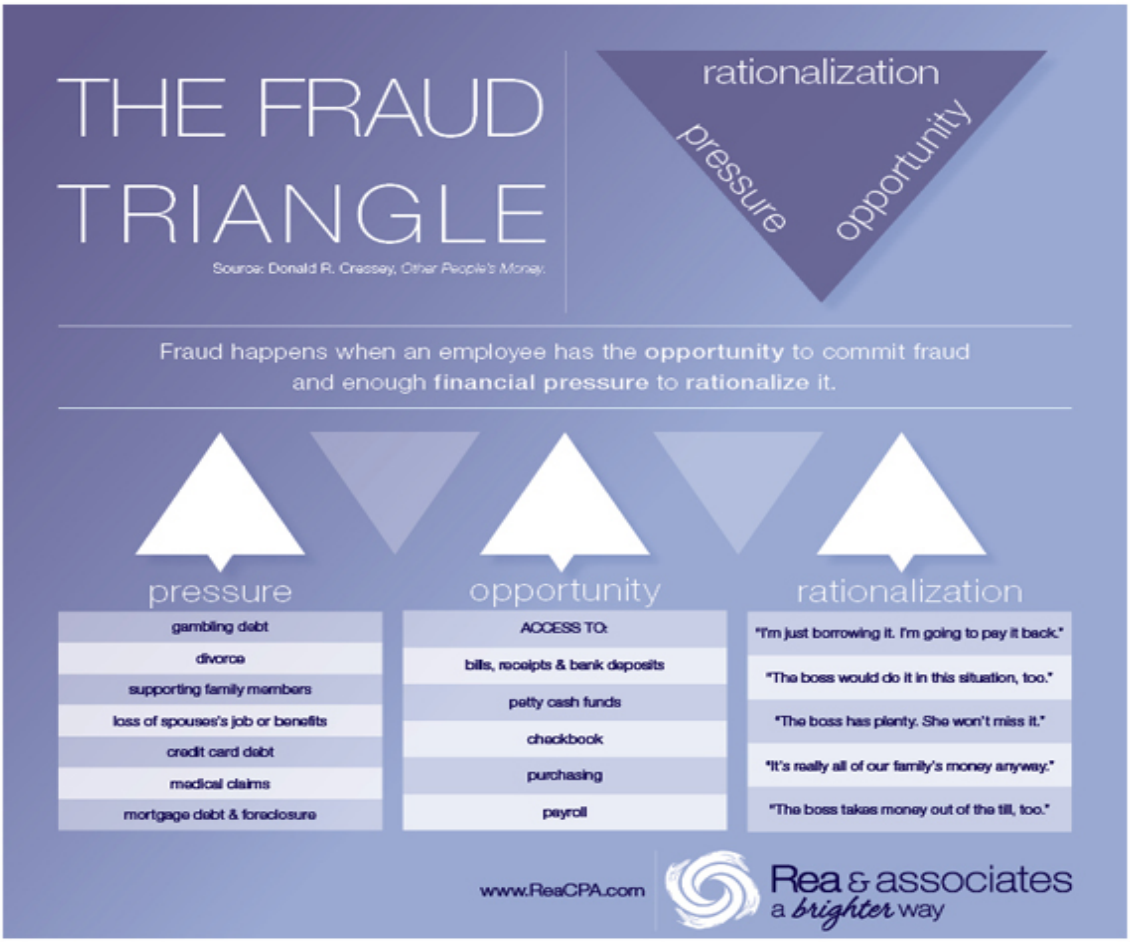
organizations with fewer than 100 employees was $190,000 per scheme...higher than the median loss in even the largest organizations. Small businesses continue to suffer disproportionate fraud losses."

According to the National Insurance Crime Bureau, by 2008, workers' compensation fraud exceeded $5 billion per year (cited in Workers' compensation fraud and the small employer). Workers' compensation fraud impacts not only the insurer, but also the business in the form of higher insurance premiums, which are based primarily on claim experience. As with many crime incidents, the best approaches to fight fraud are preventive measures. Employers can begin with better screening procedures when hiring employees to include a thorough examination of the candidate's background, work history, and references.

Typically, crimes from within also include theft, embezzlement, fraud, sabotage, and customer identity theft. Many of these crimes can be prevented by establishing good policies and procedures. Locks, passwords, and security cameras are low-cost to the small business owner, but are proven ways to reduce crime. Also, employees may be involved in pharmacy fraud or payroll fraud. Sometimes, small businesses are also involved in money laundering, knowingly or unknowingly by the owner. Clarke (2017) offers that many forms of white collar crime can be prevented through sound management practices.

White collar crimes are becoming more sophisticated and crossing national boundaries. Hendricks (2013) reports that environmental schemes are ranging into the billions of dollars targeting credits for carbon emissions and other environmental activities. Telemarketing fraud and kickbacks

Figure 1-the Fraud Triangle



Fraud can be addressed through leadership, management controls, and culture. Effective leadership includes not exerting excessive pressure on business units to meet performance targets and developing rewards systems that do not encourage employee fraud. The second aspect of the approach, management controls, including accounting procedures designed to promote compliance assurance and preventing fraud. The third means to address fraud is through an established culture where employees understand acceptable and unacceptable behaviors, thereby reducing rationalization.

Among the most critical management controls that serve as preventive measures are employee background checks and employee drug testing. Background checks should include both arrest records and credit check. Unfortunately, many small business owners fail to prosecute employees as some are family members or long-time friends. In fact, Larimer (2006) reports that only 30% of small business owners pursue instances of fraud committed by employees. In a more recent study, Reilly (2014) found that although 64 percent of small businesses reported employee theft, only 16 percent of those companies reported the incidence of employee theft to the police. Reilly's study (2014) further found that employee theft occurs over time, sometimes over a period

of years and the average theft amount to be $20,000. Theft of money accounts for 40% of employee theft, followed by theft of products and materials.

Preventive measures should begin with employee background checks and drug testing but should also include key control, computer firewalls, secure websites, secure passwords, alarm systems, and surveillance cameras. Again, a necessary means to address fraud is through an established culture where employees understand acceptable and unacceptable behaviors, thereby reducing behavior rationalization.

Embezzlement

According to Carniello (2008), embezzlement differs from fraud in that fraud is "a deception made for personal gain". Embezzlement, in contrast, is defined as "the act of dishonesty appropriating goods, usually money, by one whom they have been entrusted."

Table 1: Cost of Selected Crimes Committed Against Businesses, 2007

Type of Crime	Number of Incidents	Cost	Cost per Incident
Embezzlement	15,151	$20.9 Billion	$1,379,447
Burglary	700,239	$1.4 Billion	$1,991
Shoplifting	785,228	$1.6 Billion	$205

Source: Crime in the United States, 2007

External Crimes

Many crimes are committed by others outside the business organization and consist of a wide range of criminal activities including shoplifting, vandalism, robbery, burglary, piracy, and cargo theft. In 2015, businesses reported more than 1.1 million shoplifting incidences totaling $293 million (Crime in the United States, 2015). Even a relatively minor crime can have a significant impact on small business. The SBA reports that the average incidence of vandalism costs the small business $3,370 (http://www.nfib.com/object/IO_31210.html). More severe crimes can range from cargo theft to theft of intellectual property or trade secrets.

Cyber-attacks on the rise

With cyber attacks costing small businesses $86 billion in losses averaging $188,000 per incident, small business owners need to develop sophisticated defenses to protect against these threats. According to the U.S. House of Representatives Committee on Small Business report *Protecting Small Business*, 20% of cyber-attacks are directed toward small businesses with fewer than 250 employees and that 60% of those companies will close their doors within six months of a cyber attack. Further, 77% of small business owners consider their business safe from a cyber-attack, despite 87% of those businesses not having a written security policy in effect (Protecting Small Business, 2013).

The Bureau of Justice Statistics (2008), reported that sixty-eight percent of the cyber-attack thefts resulted in a monetary loss of $10,000 or more (Cybercrime against Businesses, 2008). In fact, Experian reports that small businesses experienced a 300% increase in cyber-attacks from 2011 to 2012 (2014 Data Breach Industry Forecast).

RECOMMENDATIONS FOR SMALL BUSINESS CONTROL

Piskunov, et al. (2016) noted that small businesses many times will be innovators in their fields and should be aware of inherent risks of entrepreneurial endeavors. The authors indicate small companies could benefit from a risk-oriented control arrangement which would entail implementing controls through systematic and situational methodology. Jena (2016) suggested that corporate governance might not only improve internal controls, but also provide a stronger system of internal control and accountability. Aldehayyat, et al. (2016) noted that corporate governance should include procedures such as internal control system, policy manuals and budgets which affect the actions of top management. How senior management deals with controls currently in place would be a component of "Tone at the Top" (Schwartz, 2005).

Stone (2016) suggested several recommendations for small business control. The author first mentions the importance of understanding the small business environment. The entrepreneur should identify any high-risk fraud areas in his company. As cash is an inherent risk in itself, a small business owner should carefully review the procedures dealing with cash, accounts receivables, and inventory. Secondly, the author strongly suggests that the entrepreneur implement internal controls, especially segregation of duties which can be very difficult to achieve in a small business with limited staff. Job sharing was one of the ways Stone (2016) indicates could be helpful, and cross-training was another suggestion and very important, yet simple to establish would be enhanced supervision of staff members.

Another control deemed necessary by the author would be adequate security and compliance software for the small business. If manual tasks can be automated, staff members can spend their time on more critical tasks and the risk of error decreases (as long as the computer programs are checked/audited for accuracy). Perhaps Bressler (2009) stated the best recommendation when he noted that there are more means to prevent crimes than methods of detection or remedies, and that prevention methods cost significantly less than the cost of crime.

SUMMARY & CONCLUSION

In this paper, the authors have presented the current situation regarding crimes against small businesses. The article highlights the major types of crimes and their sources, and the authors offer strategies for detecting and resolving crime issues. However, the authors stress the importance of crime prevention as the most effective approach to reducing crime. Prevention has been found to be significantly less expensive than the costs resulting from criminal activity.

The authors also pointed to a critical issue. In many cases, small business owners do not report crimes or fail to press criminal charges as the illegal activity is committed by a family member or long-service employee. In fact, Kennedy (2014) found that despite 64% of small businesses surveyed experienced theft, only 16% of those reported the theft to the police.

Small businesses can be considered the underpinning of our nation's economy. When small businesses survive and thrive, the economy is stronger as the business expands and jobs are created. Small business owners can increase their chance of success by developing sound management processes and controls.

REFERENCES

Aldehayyat, J. S., Alsoboa, S. S., & Al-Kilani, M. H. (2016). Investigating How Corporate Governance Affects Performance of Firm in Small Emerging Markets: An Empirical Analysis for Jordanian Manufacturing Firms. *International Business Research*, *10*(1), 77.

Bressler, M. S. (2009). The impact of crime on business: A model for prevention, detection & remedy. *Journal of Management and Marketing Research*, *2*, 1.

Carniello, G. (2008, August). Avoid Fraud and Embezzlement in the Small Business Environment, Construction Business Owner, Retrieved 02/10/2017 from http://www.constructionbusinessowner.com/topics/accounting/accounting-finance/avoid-fraud-and-embezzlement-small-business-environment

Chakraborty, A. (2015). Impact of poor accounting practices on the growth and sustainability of SME's. *International Journal of Business & Management, 3*(5), 227-231.

Clarke, P. (2017). Small businesses and white collar crime. Retrieved 1/27/2017 from http://www.legalmatch.com/law-library/article/small-business.

Cressey's Fraud Triangle depicted in Figure 1, Rea & Associates. www.reaCPA.com.

Cressey, D.R. (1973). *Other People's Money.* Montclair: Patterson Smith.

Crime in the United States, 2015. Retrieved 1/27/2017 from https://ucr.fbi.gov/about-us/cjis

Daboub, A. J., Rasheed, A. M., Priem, R. L., & Gray, D. (1995). Top management team characteristics and corporate illegal activity. *Academy of Management Review*, *20*(1), 138-170.

Dalton, D. R., & Kesner, I. F. (1988). On the dynamics of corporate size and illegal activity: An empirical assessment. *Journal of Business Ethics*, *7*(11), 861-870.

Eaton, T. V., & Korach, S. (2016). A Criminological Profile Of White-Collar Crime. *Journal of Applied Business Research*, *32*(1), 129.

Experian 2014 Data Breach Industry Forecast.

Hendricks, D. (2013, October 21). 5 Little known business crimes and scams. Retrieved 1/27/2017 from https://smallbiztrends.com/2013/10/rarely-known-business-crimes.

Jackson, K., Holland, D. V., Albrecht, C., & Woolstenhulme, D. R. (2010). Fraud isn't just for big business: Understanding the drivers, consequences, and prevention of fraud in small business. *Journal of International Management Studies*, *5*(1), 160-164.

Jena, S. K. (2016). Corporate Governance and Sustainability of Small Scale Enterprises (SSEs) in Odisha–An Analysis. *International Journal of Research in Social Sciences*, *6*(2), 504-525.

Joseph, J. "Employee theft after closing time." WOWT News. 18 Nov. 2009. Retrieved on 30 Aug. 2009.

Kuratko, D., Hornsby, J., Naffziger, D., & Hodgetts, R. (2000). Crime and small business: An exploratory study of cost and prevention issues in U.S. firms. *Journal of Small Business Management*, *38*(3),1-13.

Larimer, R. (2006, October 13). American businesses lose nearly $652 billion to fraud and embezzlement each year. *Colorado Springs Business Journal*.

National White Collar Crime Center Embezzlement/Employee Theft (March 2016) http://www.nw3c.org/docs/research/embezzlement-employee-theft.pdf?sfvrsn=16

Oseifuah, E.K. & Gyekye, A.B. (2013). Internal control in small microenterprises in the Vhembe District, Limpopo Province, South Africa. *European Scientific Journal, 9*(4), 241-251.

Piskunov, V. A., Manyayeva, V. A., Tatarovskaya, T. E., & Bychkova, E. Y. (2016). Risk-oriented internal control: The essence, management methods at small enterprises. *Mathematics Education*, *11*(7).

Protecting small business against emerging and complex cyber-attacks (2013). Hearing before the Committee on Small Business, U.S. House of Representatives, 113th Congress, Document number 113-008.

Ramamoorti, S., Morrison, D., & Koletar, J. W. (2009). Bringing Freud to Fraud: Understanding the state-of-mind of the C-level suite/white collar offender through "ABC" analysis. *The Institute for Fraud Prevention*, 1-35.

Reilly, M. & Kennedy, J. (2014). Surprising survey: most small businesses remain silent rather than report employee theft. Retrieved 02/03/2017 from http://www.uc.edu/news/NR.aspx?id=19231.

Schwartz, M. S., Dunfee, T. W., & Kline, M. J. (2005). Tone at the top: An ethics code for directors?. *Journal of Business Ethics*, *58*(1-3), 79.2710-2731.

Simpson, S. S. (1986). The decomposition of antitrust: Testing a multi-level, longitudinal model of profit-squeeze. *American Sociological Review*, 859-875.

Small Business Facts https://www.sba.gov/sites/default/files/Business-Survival.pdf

Stone, R. (2016). Fraud, Security, and Controls in Small Businesses: A Proposed Research Agenda. *Journal of Business*, *1*(3), 15-21.

Workers' compensation fraud and the small employer (2009, January 12). Fairfield County Business Journal, 48(2), 28.