The Impact of Crime on Business: A Model for Prevention, Detection & Remedy

Martin S. Bressler
Houston Baptist University

Abstract

Since the nineteenth century, sociologists have studied the relationship between economic business cycles and increases in crime. According to the U.S. Chamber of Commerce, crime may be a factor in as many as 30 percent of all business failures. Despite other variables that may contribute to increases in criminal activity, the current economic recession will likely accelerate criminal activity ranging from shoplifting and robbery to fraud and embezzlement. In this paper, the researcher examines the role of prevention and detection of criminal activity and offers prevention as the most cost-effective means to reduce the impact on business.

Keywords: crime, white collar crime, crime prevention crime cost, crime impact

Introduction

Economic cycles indicate that during more difficult economic times, criminal activity increases. Experts (Levisohn, 2009) believe that fraud in particular, increases during recessionary times. James Short (1980) compiled a number of comprehensive studies on the relationship between crime and economic cycles examining a series of studies dating back into the 1800's. Although numerous variables and circumstances make comparisons difficult, Short concluded that "some connection" exists.

According to the National White Collar Crime Center, the two most recent recessions recorded significant increases of arrests for fraud and embezzlement (Business Week Online, January 12). In 1990, just after the savings and loan crisis, arrests increased 52% and in 2000, after commercial Internet development, arrests increased 25% (Business Week Online, January 12). Arvanites and Defina (2006) examined business crime activity and economic cycles from 1985 to the early 2000's and also report a relationship between the two.

Businesses, already susceptible to a wide variety of crimes, need to be on their guard to prevent the impact of criminal activity from impacting profitability to the point that the viability of their business comes into question. Crimes against companies range from shoplifting and vandalism to piracy and counterfeiting. In some instances, crimes committed against businesses are committed by outsiders while in many other situations; employees at all levels commit crimes against their employers. In some cases, companies become unwitting accomplices of money-laundering crimes.

Crimes committed against business are nothing new. The literature records numerous examples throughout history. By 1995, the SBCI survey found 35% of retailers reporting customer theft with similar percentages for manufacturing and wholesaling industries. In all, 75% of surveyed businesses reported one or more incidents of crime, with 3.5 incidents on average (Burrows & Hopkins, 2005).

Small businesses may be particularly vulnerable to crime as small businesses often do not have safeguards in place to prevent and detect criminal activity. As early as 1996, (prior to Internet crime) a survey of 400 firms conducted by the U.S. Small Business Administration found nearly 13% of surveyed businesses became crime victims. Further, less than half (48%) employed any security measures and many incidents, especially employee thefts, went unreported (Small Business Research Summary, 1997).

How much does crime against business cost? According to the 2007 report Crime in the United States, stolen office equipment alone totaled a staggering $656,982,032. Burglaries on average cost businesses $1,989 and shoplifting which recently increased 11.2% cost businesses an average $205 per incident. Several recent high-profile cases of fraud include the Madoff investment scandal ($50 billion) and the Stanford investment scandal ($20 billion). Just a few years ago, newspaper headlines shocked readers with news of the Enron and WorldCom financial scandals (Off to Jail, 2005; Schickel, 2005). By 1991, cost estimates of crimes committed against businesses reached $128 billion in direct costs (Thompson et al, 1992). Estimates are difficult to determine as many business crimes go unreported (especially in small businesses) for fear of bad publicity and loss of investor confidence but by 2006, even prior to the current recession, Federal Bureau of Investigation crime data list the figure at $652 billion annually (cited in Bressler, 2007).

Literature Review

Types of crimes

Crimes committed against business can be separated into two categories: those committed by employees against businesses and those committed by others. Table 1 lists some of the more common crimes committed by employees which include theft, fraud, and money laundering.

According to Marten and Edwards (2005), three conditions must be present for employees to commit fraud. The first condition is incentive, often in the form of some type of pressure. Pressure may be due to financial reasons, sometimes associated with extra money needed for an adulterous relationship. In other cases, financial pressure could be due to excessive medical bills, gambling debts, or drug addiction. Opportunity exists when businesses fail to develop safeguards or become too trusting of employees. Rationalization occurs when an employee justifies their action as the company "owing them".

In each of these three conditions, company's management can institute safeguard procedures to reduce the possibility of an employee to use these conditions as an entry to committing fraud. Background and credit checks can identify employees who might be more prone to financial pressures. Fraud hotlines can be established to allow reporting of suspicious employee behaviors, including recent expensive purchases. Opportunity can be lessened when companies develop safeguards through unscheduled audits, use of Accounting Information Systems (AIS) software, and basic procedures such as check approvals. Rationalization may be more difficult to prevent, however, Ethics Statements and management setting good examples may be effective ways to thwart employee rationalization.

Embezzlement may perhaps be the most serious crime impacting business, in that many times the crime goes undetected for years. Embezzlement affects not only large business but small business, government agencies and non-profit organizations. As so many instances of embezzlement go unreported to police, experts can only estimate the extent of embezzlement activity. Costello (2003) reported that according to an estimate by the National White Collar Crime Center, embezzlement may cost companies as much as $90 billion each year. An employee working at the cafeteria of a state prison in Georgia reportedly skimmed $1.5 million from the cafeteria cash registers over the course of several years (Costello, 2003). In another Georgia case, an employee stole $300,000 worth of postage stamps from the University of Georgia (Costello, 2003).

Table 1. Typical Crimes Committed by Employees

Type of Crime
➢ Theft, or "skimming" of cash ➢ Theft of inventory, merchandise or equipment ➢ Writing company checks ➢ Falsifying revenue reports ➢ Processing fraudulent invoices ➢ Customer identity theft ➢ Money laundering ➢ Intellectual property theft ➢ Credit card fraud ➢ Overstated expense reports ➢ Payroll fraud

Source: Albrecht et al, 2006

Table 3 highlights some of the more common crimes committed against businesses including vandalism, shoplifting, and theft. Today, however, more businesses fall victim to attack through computer systems. These "hack-attacks" may take the form of sabotage, customer identity theft, or theft of funds.

Since the development of the Internet, cybercrime activity is increasing at an alarming rate. The 1995 National Computer Crime Survey reported 67 percent of the 7,818 businesses surveyed fell victim to at least one cyber attack (Bureau of Justice Statistics, 2008). Many of the cyber attacks involved theft (60%) while other incidents included viruses uploaded to the business computer system. Sixty-eight percent of the cyber attack thefts resulted in a monetary loss of $10,000 or more (Bureau of Justice Statistics, 2008).

Yueh (2004) reports businesses suffered a 40% increase in computer attacks over the previous year. The 150,000 computer attacks resulted in a cost to business of $42 billion (Yueh, 2004). Security consultant Richard Stiennon (cited in Elms, et al.) believes cybercrime to be the major threat to computer infrastructure, business processes and businesses themselves. Another study, conducted in 2001 by IDC in Massachusetts, found 95% of IT managers at medium and large U.S. companies experienced various computer attacks.

According to a study conducted by IDC computer consultants in 2000, 95% of IT managers experienced at least one incident of computer systems breach (Gantz, 2001). By 2004, companies increased spending on information technology security systems to an estimated $30 billion, more than double since 2001, to protect corporate websites (Gantz, 2001). Despite the increased need for computer security, only 30% of companies reported that their company encrypted email.

The 2005 National Computer Crime Survey prepared by the U.S. Department of Justice finds 67% of surveyed companies indicated at least one cybercrime committed against their business (U.S. Department of Justice). According to the survey, 68% of crime victims reported

losses of $10,000 or more from cyber-attacks. Surprisingly, only 15% of businesses reported the cyber-attacks to police or other law enforcement agencies. The Federal Bureau of Investigation now lists cybercrime their third-highest priority, just behind terrorism and espionage (Elms, 2008)

Banks can be especially vulnerable to criminal activity. Criminal activities ranging from robbery and money laundering to ATM fraud will send banks scrambling to increase security measures. One estimate indicates the costs of crime that businesses incur amounts to "69% of after- tax corporate profits" (Thompson et al, 1992).

While vandalism may not seem to be especially serious when compared to other crimes committed against businesses, the U.S. Small Business Administration reports the average vandalism incident costs small business $3,370 (http:www.nfib.com/object/IO_31210.html). Put another way, a small business with revenues of $500,000 per year and a net margin of 5% would lose approximately 13.5% of their annual net profit. Table 2 highlights some examples of how much certain crimes cost businesses overall and per incident.

In a study for the National Federation of Independent Business, Dennis (2008) reports 52 percent of businesses became victimized by crime within the previous three years. The report also noted vandalism as the most common crime committed against small businesses in general, and shoplifting most common to the retail industry.

The U.S. Chamber of Commerce (cited in Kuratko et al., 2000) in 1995 reported that employee dishonesty accounted for as many as 30% of all small business failures. Their report also goes on to state that small businesses are 35 times more likely to become crime victims than larger companies. The National Council of State Legislature's publication reports retail crime now exceeds $30 billion dollars per year, resulting in $1 billion in lost tax revenues (National Federation of Independent Business).

Crimes committed against retail establishments come to our attention more often as they may occur locally and upon businesses we frequent. According to Casteel et al. (2004) certain businesses, such as liquor and convenience stores experience significantly higher rates of crimes, particularly employee death. The recent economic downturn may also account for increased shoplifting. In a news story just before Christmas, Shafer (2008) reported that a source at the Mall of America indicated an 18% increase in shoplifting reported over the previous year. Shafer also mentioned a Post survey of 52 national retailers by the Retail Industry Leaders Association indicating an 84% increase in shoplifting at their stores.

Recently, Best Buy was swindled out of $31 million in an elaborate bid-rigging scheme (Best Buy Swindled, 2009). Best Buy became a victim of the scheme in part due to a lack of internal controls that otherwise would have sent "red flags" to the attention of auditors. In another case, as if the housing market slump wasn't enough, Lennar homebuilders recently became victim to a Ponzi scheme (American Banker, 2009). A Ponzi scheme refers to a fraudulent investment that returns money only to early investors by using money obtained from later investors, rather than actual investment profits (Wikipedia). In a 2005 study, the Association of Certified Fraud Examiners found the average business loss due to fraud or embezzlement to $159,000, although the average loss for a business with fewer than 100 employees to be $190,000 (cited in Larimer, 2006).

According to the Federal Bureau of Investigation, during the period from 1994-2002, intellectual property theft increased 26%. In addition, increased money laundering activity also includes small businesses, often facilitated by an employee or third-party. The FBI further goes

on to state that money laundering often couples with other felonies including drug trafficking, fraud or embezzlement (Crime in the United States, 2007).

Inventory shrinkage

A 1994 University of Florida study (cited in Kuratko et al.) examined causes of inventory shrinkage and found employee theft accounted for 42.1 percent and 32.4 percent to shoplifting and improper paperwork. Shoplifting affected 695,387 retailers with an average loss of $194 per incident (Sourcebook of Criminal Justice Statistics Online). The U.S. Small Business Administration reports stock loss ranging from 1.3% to 7% of sales. That means for a small business with sales of $1 million per year, stock losses may account for as much as $70,000. Put another way, a small business with a net profit of 5% could actually lose money (Curtailing Crime). A study by the U.S. Chamber of Commerce reports as many as 30% of small business failures the result of crime (U.S. Chamber of Commerce, 1995).

Economic downturns often may account for an increase in shoplifting. Just before Christmas a source at the Mall of America reported a 19% increase in shoplifting (Shafer, 2008) and several police departments in the Philadelphia area also reported increased shoplifting at area stores. A Post survey of 52 national retailers conducted by the Retail Industry Leaders Association reported an 84% increase in shoplifting (Shafer, 2008).

To reduce inventory shrinkage, companies need to employ two different tactics. Preventing shoplifting calls for surveillance cameras, mirrors and security guards. Preventing employee theft of merchandise or equipment may use those same techniques but in addition companies can also utilize background checks, honesty tests and regular inventory checking.

Table 2. Cost of selected Crimes against Business, 2007

Type of Crime	No. of incidents	Cost	Average per incident
Burglary	700, 239	$1.4 billion	$1, 991
Shoplifting	785, 228	$1.6 billion	$205
Embezzlement	15, 151	$20-90 billion*	

*estimated, many unreported

Source: Crime in the United States, 2007

Small Businesses, Big Targets

Despite fewer employees and smaller revenues, small businesses may be more susceptible to business crime. As most businesses are small businesses, nearly half of the U.S. workforce is employed in small businesses. The Association for Certified Fraud Examiners indicates 39% of reported instances of fraud occur in companies with 99 or fewer employees (Bank Technology News). The U.S. Small Business Administration reports 13% of small businesses become crime victims, yet less than half (48%) instituted any preventive measures (Small Business Research Summary). This could be a major reason why crime is a major factor in up to 30% of small business failures (U.S. Chamber of Commerce). In addition, small business ventures with less than $5 million in annual revenues may be up to thirty-five times

more likely to become a crime victim than their larger counterparts (U.S. Chamber of Commerce).

Unfortunately, small business owners prosecute less than 30% of fraud cases (Larimer, 2006). Many crimes committed against small business go unreported to police for a variety of reasons. In some cases, crimes committed by employees or local persons known to the business owner go unreported as the business owner might not want to press charges for fear of negative publicity or loss of confidence in the business. In other instances, such as vandalism, small business owners might assume that police would be unable to apprehend and charge the vandals.

Discussion

Crime Prevention Strategies

Welsh & Farrington (1995) offer four crime prevention strategies: situational, developmental, community and criminal justice prevention. Situational strategy refers to surveillance techniques using employees, alarms or video monitors. A Developmental Strategy involves examining the root causes of crimes against businesses such as juvenile delinquency, poverty and economic cycles. Community strategies utilize various social experiments and neighborhood watch programs. Criminal Justice prevention programs develop partnerships between law enforcement and the community.

A model program in New York City (Kugel, 2003) designed to help bodegas (Mom and Pop grocery stores) by installing security cameras secured backing from the mayor and the police. According to a survey by a bodega owner's association, nearly 35% of crimes went unreported to police. Despite the fact that bodega owners typically do not report crime to police, a recent surge in killings during robberies prompted store owners to become more involved in working with law enforcement (Kugel, 2003).

Among retailers, liquor stores report higher rates of employee injury or death than other types of retail establishments (Casteel et al, 2004). Comparing two groups of stores, one with an environmental design intervention and the other group without, researchers found a significant reduction in robberies and shoplifting among stores using environmental design. Environmental design programs utilize structural design methods for both outside buildings as well as interior layouts. Without cover, criminals are more visible to surveillance cameras and security guards and it is also more difficult to surprise employees on duty.

The best strategy to defend against business crime should focus on preventive measures. For many businesses, simple actions such as improving security lighting or requiring employee identification may reduce crime. Crime preventive actions can be categorized into external measures, to include security lighting, surveillance cameras, locks, and key control; employment policies that include background checks, drug testing, employee identification, and separation of duties; computer defenses that include secure websites, access authorizations through secure passwords, computer firewalls, and secure Internet payments. Finally, everyday work practices such as keeping minimal amounts of cash on hand, requiring employee identification, paying everything by check and not delegating check signing provide basic defenses against internal and external crime (see Figure 1).

With recent headline stories of investment fraud impacting individuals, businesses and non-profits, government at the state and national level will begin to more closely scrutinize

investment activity. At this point, however, the U.S. Government Accountability Office admits that the current oversight system is too fragmented to be effective (Levisohn, 2009).

Employee crime prevention can begin with establishing sound hiring practices including background checks and drug testing. A 2002 Association of Certified Fraud Examiners study (cited in Wells, 2003) revealed that 7% of employees in the workplace have a history of theft or fraud. Background checks should also include a credit history report as some employees may resort to embezzling company funds when financial pressures from drug addiction, adultery, gambling or medical expenses seem insurmountable (Costello, 2003).

In one example, during the routine background check a company preparing to hire a new financial director found the applicant did not have the industry experience or the MBA degree he claimed (Business Week). Due to time and expense, many small companies skip background checks. However, Hogsett and Radig (cited in Kuratko et al, 2000) found 30% of employees steal from their employers and another 30% might be tempted to do so under certain circumstances.

Wade (2002) discovered some interesting findings in a South Carolina study of employee drug abuse. Employee drug abusers are injured on the job 2-5 times more often than other employees, are 26-31% less productive in their work, and are cited as a factor in 33-39% of product or service quality problems. Study findings also report a return of $4 for every dollar invested in that treatment.

Table 3. Crimes committed against businesses

External	Internal
Robbery	Theft
Burglary	Embezzlement
Shoplifting	Fraud
Counterfeiting	Customer identity theft
Piracy	Sabotage
Money laundering	
Vandalism	
Ponzi schemes	
Computer hacking	

Source: Bressler, 2009

Detection

Regardless how many preventive measures are employed, businesses will likely still become crime victims. The number and size of occurrences will likely be smaller. Detection techniques also tend to be low-cost and as simple as frequently checking bank statements, unscheduled audits and use of accounting information systems (AIS) software. AIS software uses “red flags” to indicate to the auditor where potential problems might exist. Despite the importance of unscheduled internal audits, the Association of Certified Fraud Examiners indicates that only 20% of internal audit departments actually perform unscheduled audits (Larimer, 2006).

Monitoring employee behaviors, especially radical changes in employee lifestyle may also indicate fraud activity. Employees suddenly purchasing luxury cars or boats, taking expensive vacations or giving lavish gifts often warrant investigation. Fellow employees may assist and are now protected by whistle-blower protection afforded under the Sarbanes-Oxley Act (Yormak, 2004). Because most employers find out about instances of fraud from employees, vendors or customers, the Association of Certified Fraud Examiners suggests instituting a fraud hotline can reduce embezzlement by as much as 50% (Costello, 2003).

The importance of forensic accountants cannot be overstated. Because many white collar crime activities are often carefully concealed through numerous complicated business transactions, forensic accountants with their expertise can uncover criminal activity that otherwise might go unnoticed during routine audits. In addition, forensic accountants can be especially helpful when a firm plans a merger or acquisition to determine a company's true worth and insure that financial data is not misrepresented (DiGabrielle, 2008).

Remedies

When prevention isn't sufficient and detection activities find criminal activity, the business must determine the best way to minimize loss to the company. A Department of Commerce study of 400 small firms cited by the U.S. Small Business Administration, found that many crimes committed against small businesses went unreported. In fact, none of the businesses reporting employee theft reported the incidents to police (Small Business Research Summary). This, despite a study by the National Federation of Independent Business where 79% of small business owners reported confidence in local police (Dennis, 2008). Prosecution of criminal acts is important as otherwise the perpetrator simply moves on to the next corporate target. Many smaller businesses are uninsured or underinsured; therefore prosecution may assist the business in recouping some of the financial loss.

Expert witnesses, in many cases forensic accountants, play a key role in providing court testimony. As expert witnesses will be challenged by defense lawyers, forensic accountants should be trained in audit procedures, possess the necessary professional certification (such as Certified Internal Auditor, Certified Fraud Examiner, etc.) and be able to prepare findings in a professional manner that will sustain cross-examination by defense attorneys.

Usually the last resort for the business owner is to file an insurance claim. Smaller businesses may not have insurance or sufficient insurance to cover losses. According to a 2002 study by the National Federation of Independent Businesses, 15% of surveyed businesses do not carry business insurance at all and only 34% have business-interruption insurance.

Many types of business insurance coverage are available. The U.S. Small Business Administration recommends business owners purchase criminal insurance, general liability insurance, product liability insurance, worker's compensation insurance, Internet business insurance, key person insurance, home-based business insurance and malpractice insurance (U.S. Small Business Administration, Small Business Planner).

Figure 1

A Three-Stage Model for Prevention and Detection of Business Criminal Activity

Source: Bressler, 2009

Implications

Several important implications can be drawn from this study. First, every business is potentially a crime victim. Crimes committed against your business can impact profitability and even lead to business failure. According to the U.S. Chamber of Commerce, as many as 30% of businesses fail as a result of crime, preventive measures should be taken to reduce the incidence and severity of crimes committed against your business (U.S. Chamber of Commerce, 1995).

Second, preventive measures cost significantly less than the cost to remedy crime committed against the business. Even small businesses can reduce the likelihood of becoming a crime victim and the severity of criminal activity with some fairly low-cost actions. Larimer (2006) reported that small businesses suffered greater losses from fraud than larger businesses, $190,000 per incident versus $159,000 for larger businesses. One study (Kuratko et al, 2000) found the typical small business spent $7,805 on security measures. In other words, currently

their losses are twenty-five times the amount spent on security measures. Increased spending for security measures could result in smaller losses.

Finally, those businesses that defend themselves against crime are less likely to become targets of criminal activity. While prevention tactics do not prevent your business from becoming a crime target, appropriate safeguards can reduce the likelihood and severity of criminal activity. Insurance companies often reduce insurance premiums when businesses install appropriate security measures. The business becomes safer for the owner, investors, and employees.

Conclusion

Even before the recession started, criminal activity directed at businesses began increasing at an alarming rate. In the past, the most common crimes committed against businesses included shoplifting, vandalism and embezzlement. Today, criminal activity occurs more often and includes a wider range of crimes including mortgage fraud, counterfeiting and piracy.

As the cost of crime continues to escalate and cuts further into profits, businesses must increase preventive measures and develop more sophisticated methods to detect crime. Without employing a new crime prevention and detection strategy, many businesses could become unprofitable and susceptible to business failure.

Dr. Martin Bressler Biographical Sketch

Dr. Martin Bressler is Professor of Marketing & Entrepreneurship at Houston Baptist University. Dr. Bressler previously taught at Thomas College, Bryant University, Nichols College and Quinsigamond College. Prior to his career in teaching he worked for Sears Merchandise Group in a variety of management positions. Dr. Bressler is a Fulbright Senior Scholar, Price-Babson Fellow, Sam Walton Fellow and served as Resource Panel Expert to the 1995 White House Conference on Small Business. The immediate past president of the Association for Small Business & Entrepreneurship, Dr. Bressler was named the Maine Small Business Advocate of the Year in 1991 and Media Advocate of the Year in 1995 by the U.S. Small Business Administration.

References

Albrecht, W.S., Albrecht, C.C. & Albrecht, C.O. (2006). *Fraud Examination 2e.* Mason: Thomson Southwestern Publishers.

American Banker. Lennar Shares Hit by Ponzi Scheme. New York, NY. January 12, Volume 174, Issue 7, 11.

Arvanites, T. & Defina, R. (2006). Business Cycles and Street Crime. Criminology, Volume 44, Number 1, 139-164.

Best Buy Swindled out of $31 million. AOL Money and Finance. http://money.aol.com/news/articles/tech_news/_a/bbdp/best-buy-swindled-o0ut-of31-million/367215 accessed March 1, 2009.

Bressler, L. & Bressler, M. (2007). A Model for Prevention and Detection of Criminal Activity Impacting Small Business. Entrepreneur Executive, Volume 12, 23-36.

Bureau of Justice Statistics, 2008. Sixty-seven percent of responding businesses detected cybercrime in 2005. U.S. Department of Justice, Office of Justice Programs. September 17, 2008.

Burrows, J. & Hopkins, M. (2005) *Business and crime* in Tilley, N. (2005) (Ed.) *Handbook of crime prevention and community safety*. Devon, Willan Publishing.

Casteel, C., Peek-Asa, C., Howard, J., Kraus, J. (2004). Effectiveness of Crime Prevention Through Environmental Design in Reducing Criminal Activity in Liquor Stores: A Pilot Study. Journal of Occupational Medicine; May, Volume 46, Issue 5, 450-458.

Costello, J. (2003). When the economy worsens, embezzlers cash in on poor business practices. American City Business Journals. http://atlanta.bizjournals.com accessed March 2, 2009.

Crime in the United States 2007. http://www.fbi.gov/ucr/cius2007/data/table/23.html

Dennis, W. (2008). 411 Small Business Facts, Volume 8, Issue 5. ISSN-1534-8326.

DiGabrielle, J. (2008). An Empirical Investigation of the Relevant Skills of Forensic Accountants. Journal of Education for Business, July/August, 331-338.

Elms, E., LaPrade, J. & Maurer, M. (2008). Hacking of Corporate information Systems: Increasing threats and Potential Risk Management Techniques. CPCU eJournal, February, 1-9.

Gantz, J. (2001). Take a Bite Out of Crime on the Web. Computerworld, February 19, Volume 35, Issue 8, 29.

Keeping Tricksters Away 10/31/2006 http:www.nfib.com/object/IO_31210.html

Kugel, S. (2003, July, 6). Devoted to Mom and Pop. New York Times, p. CY4.

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; July, 2000; 38, 3; ABI/Inform Global pg. 1.

Larimer, R. (2006, October 13). American Businesses Lose Nearly $652 billion to Fraud and Embezzlement Each Year. *Colorado Springs Business Journal*.

Levisohn, B. (2009). Experts Say Fraud Likely to Rise. Business Week Online [serial online]. January 12, 2009: 14-14. Available from: Business Source Complete, Ipswich, MA. Accessed February 18.

National Federation of Independent Business, New Hampshire Hot Topics. February 13, 2009. http:www.nfib.com/object/IO_9662.html accessed March 1, 2009.

Off to jail. (2005, June 25). *Economist*, 375, 61-62.

Schickel, R. (2005, June 20). How Enron's Big Shots got into trouble. *Time*, 165, 62.

Shafer, J. (2008, December 24). (Another) Bogus Trend of the week: a Plague of Shoplifters! Slate (USA)

Short, J. (1980). An Investigation of the Relationship Between Crime and Business Cycles. Ayer Publishing. ISBN: 0405129939.

Small Business Planner (2007). Get Insurance. U.S. Small Business Administration, http://www.sba.gov/smallbusinessplanner/getinsurance/SERV_INSURANCE.html

Small Business Research Summary, 1997, Office of Advocacy, U.S. Small Business Administration, No. 176, March.

Sourcebook of Criminal Justice Statistics Online http://www.albany.edu/sourcebook/pdf/t31112006.pdf

Thompson, T., Hage, D., Black, R. (1992). Crime and the Bottom Line. U.S. News and World Report, April 13, 1992).

U.S. Department of Justice, Office of Justice Programs. National Computer Crime Survey, 2005. http://www.ojp.usdoj.gov/bjs/pub/press/cb05pr.htm accessed 02/18/2009.

U.S. Small Business Administration, Curtailing Crime Inside and Out. http://sba.gov/idc/groups/publ;ic/documents/sba_homepage/serv_pubs_cp_pdf_cp1.pdf

Wade, R. (2002). The Impact of Drug Intervention on the Bottom-line in Business. February 5. http:www.nfib.com/object/3157720.html retrieved March 1, 2009.

Welsh, B. & Farrington, D. (2000). Monetary Costs and Benefits of Crime Prevention Programs. Crime and Justice, 27, 305-361.

Wikipedia online reference http://en.wikipedia.org/wiki/Ponzi_scheme

Yueh, T. (2004). Worms and Viruses-Are You Under a Constant Security Siege? Get Smart about Network Security. 08/01/2004 http:www.nfib.com/object/IO_17267.html

Yormak, K. (2004). Making the most of an internal investigation. *Journal of Investment Compliance*, 5, 64-67.