FRAUDS, EMBEZZLERS, THIEVES, AND OTHER BAD ACTORS: HOW CRIMINALS STEAL YOUR PROFITS AND PUT YOU OUT OF BUSINESS

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

ABSTRACT

Shoplifting, fraud, embezzlement, and now cybercrimes are only a few of the many types of crimes business owners lose sleep over. Business owners lose profits, sometimes significant profits, and small businesses are affected to any even greater extent. Small businesses often lack the resources to defend their business against various criminal activities and may not be able to recover from large losses. The U.S. Chamber of Commerce reports that as many as 30% of small business failures could be attributed to embezzlement or employee theft. And to make matters worse, thieves are becoming more sophisticated in the use of high-tech tools to steal. In this paper, the authors provide an overview of current criminal activity and offer several ways to address the situation.

Key words: business crime, fraud, embezzlement, white-collar crime, prevention-paradox

INTRODUCTION

According to the U.S. Small business Administration (SBA Small Business Facts), only two-thirds of small businesses will survive the first two years and only about half will survive beyond the first five years of operation. Many others offer an even more gloomy estimate. According to Wagner (cited in Forbes Online, 2013) as many as eight in ten new business fail within the first eighteen months. There might not be agreement on the number of small business failures but certainly, the numbers are cause for concern. Likewise, there is considerable discussion on the causes of small business failure. However, little attention is paid to one of most important causes of small business failure. The U.S. Chamber of Commerce (cited in Simon, 2016) reports that 30 percent of business failures are the result of embezzlement or employee theft.

INTERNAL CRIMES

In the context of small business, white collar crimes typically take the form of fraudulent record keeping, sometimes referred to as “cooking the books”. In many instances, business figures or sales receipts are changed to falsely represent the business as earning less profit than it really is. Small Business Digest reports that the typical business or organizations loses about 5% of revenues to various fraud activities each year (smallbusinessmagdigest.com). For some small

businesses, losing 5% of their revenues could mean the difference between profitability and business failure

Crimes committed against businesses

EXTERNAL	INTERNAL
Robbery	Theft
Burglary	Embezzlement
Fraud	Fraud
Vandalism	Identity theft
Ponzi schemes	Sabotage
Computer hacking	
Shoplifting	
Counterfeiting	
Piracy	

White collar crimes

White collar crimes include bribery, extortion, theft, tax evasion, embezzlement, and miscellaneous frauds, including payroll fraud and pharmacy fraud. In some instances, fraud occurs over long periods of time. A CNBC report on white collar crime cites data from the global insurance specialty company Hiscox, that finds for embezzlement and fraud occurring five or more years, the average loss for was $2.2 million, and for fraud or embezzlement lasting 10 years or more the loss was $5.4 million (www.cnbc.com). Losses exceed $1 million in 20% of cases (www.cnbc.com).

Verschoor (2018) refers to the 2018 Global Economic Crime and Fraud Survey, conducted by Price Waterhouse Coopers, one of the Big 4 accounting and consulting firms. Their survey of more than 7,200 respondents across 123 different territories uncovered some very important findings. The largest cause of fraud (59%) is weak internal controls and only 54% of respondents reported that they conducted a general fraud or economic crime risk assessment within the past 2 years. As the respondents are larger companies, we can assume that small businesses would be even less likely to have conducted a crime risk assessment.

Examples of white-collar crime
Bribery
Extortion
Theft
Tax evasion
Embezzlement
Miscellaneous including payroll fraud and pharmacy fraud

Source: www.legalmatch.com

Embezzlement cases often occurred when an employee would repeatedly divert small sums of money over time, thereby making their theft very difficult to detect. In 28.7 percent of fraud or embezzlement incidents, employee theft took happened over the course of five years or more (Hiscox, cited in CNBC).

Instances of business fraud last an average of 18 months and average $573,000 for executives and $60,000 for other employees. Research found that the longer an incident of fraud lasts and the higher the position in the organization, the greater the losses. In the United States, fraud loss estimates range from $300 to $600 billion. This estimate highlights the difficulty in uncovering and confirming all instances of fraud that occur. In many instances, recovering the funds can be more difficult than finding, researching and prosecuting fraud. More than half (58%) of companies that uncover cases of fraud recover none of the money and overall, only 39% of embezzled funds were recovered on average, through settlements, restitution or insurance (HISCOX, 2018).

The 2018 HISCOX Embezzlement Study research uncovered some interesting findings and although the findings differ somewhat from other studies, nevertheless the results are important to note. Some key findings include: more than one perpetrator in 79% of all cases, with an average of three perpetrators; 33% of cases involved someone employed in the accounting or finance department.

The Association of Certified Fraud Examiners (ACFE) reports the median fraud loss in a small business of fewer than 100 employees to be $200,000 (Report to the Nations, 2018). The most common means of fraud or theft were found to be corruption, billing, check payment tampering, expense reimbursements, skimming, cash on hand, non-cash theft, financial statement fraud, payroll fraud, and register disbursements (Fraud in small business, 2018).

Small Business	Less than 100 employees	Greater than 100employees
Median loss	$200,000	$104,000
Frauds detected by tip	29%	44%
Frauds caused by lack of internal controls	42%	25%
Frauds perpetrated by owner/executive	29%	16%

Source: Report to the Nations, the Association of Certified Fraud Examiners

EXTERNAL CRIMES

External crimes, those committed by persons outside the company, include burglary, robbery, larceny (theft), cybercrime, shoplifting, vandalism, and cargo theft. In addition to the financial cost to the business, sometimes financial crimes are accompanied with other violent crimes including assault or murder.

Burglary-The FBI Uniform Crime Reporting Data indicates that in 2017, there were more than 1.4 million burglaries reported to various law enforcement agencies, resulting in $3.4 billion in property losses (Crime in the United States, 2017). These crimes resulted in an average financial loss of $2,416 per occurrence (Crime in the United States, 2017). Although only about a third of these burglaries (32.8%) occur in businesses, the resulting financial loss can significantly impact smaller businesses.

Larceny-theft-This crime category includes a wide range of thefts ranging from bicycles, auto parts, and other property including pickpocketing and shoplifting, totaling more than 5 ½ million thefts. Together, these thefts $5.6 billion, with an average theft of $1,007 (Crime in the United States, 2017).

Cargo theft-Perhaps the least known crime committed against business is cargo theft. Cargo theft can be costly to businesses in more ways than one. A local small business owner of a swimming pool installation and supply company had their entire opening season inventory on a trailer truck that was hijacked. This caused a delay in receiving goods and a resulting loss in sales for several weeks. According to FBI crime data, reported cargo theft costs businesses more than $21 million per year, with less than 26% of merchandise recovered (Crime in the United States, 2017). The FBI is particularly interested in cargo theft as in some instances, the merchandise involved could include firearms, sensitive high-technology products, or potentially dangerous materials.

Robbery-Robbery can be considered among the more serious property crimes as in many cases a weapon or strong-arm tactics are used in the commission of the crime. The 319,356

robberies in 2017 reported an average loss of $1,373, or a total of $438 million in losses (Crime in the United States, 2017).

Cybercrime-according to Dr. Jane LeClair, Chief Operating Officer of the National Cybersecurity Institute, "Fifty percent of small to medium-sized businesses (SMB) have been the victims of cyber-attack and over 60% of those attacked go out of business." The cost of a cyber-attack to a small business today averages $20,752 and for those businesses whose bank accounts were hacked, those losses were $19,948 (The Impact of Cybersecurity on Small Business). Fruhlinger (2018) also reports that it takes the typical organization an average of 191 days to identify data breaches and the average ransomware attack costs a company $5 million.

Egeland (2015) believes there are four ways that cybercrime can hurt your small business. First, is the loss of your business reputation and consumer confidence. A computer attack that compromises customer financial data can halt business operations and even permanently put a company out of business. The second way that a small business can be harmed is with the cost of fixing the issue. Small businesses that rely heavily on the internet to operate their business would suffer the most while their business is down and for the resulting costs associated with finding and resolving business damage. The third way that a small business can suffer is when the organization's financial information is compromised. Money and credit can be stolen through an online incursion. Finally, a computer breach can result in substantial legal liability for a small business should customer or vendor personal or financial information be stolen.

Shoplifting and inventory shrinkage

Among the most serious problems facing retail businesses in 2019 is inventory shrinkage and shoplifting. Inventory shrinkage typically amounts to 1.33% of gross sales and costs the U.S. retail industry more than $45 billion annually (Tyree, 2019). Inventory shrinkage includes fraud, theft, shoplifting, and organized retail crime (ORC). U.S. grocery stores allocate only 0.36% of sales to reducing shrinkage (Source: National Retail Federation survey).

In fact, according to the National Retail Federation survey, ORC costs the retail industry approximately $30 billion each year and almost all retailers have been impacted by ORC. In addition to costs associated with theft of merchandise, retail crime activity places both employees and shoppers in potential danger. The average cost per shoplifting incident doubled to $559 and the average cost for return merchandise fraud is $1,766.27 (National Retail Federation survey).

TYCO integrated security reports that 40 percent of thefts involve money, ranging from five dollars to $2 million, averaging $20,000 (www.tycois.com). In addition to money, employees sometimes steal products that the company manufactures (about 20% of all employee thefts) and another 6% being equipment and supplies used by the company, ranging from pens, staples, and paper towels.

In a 2016 study by global specialist insurer Hiscox, U.S. businesses affected by employee theft lost an average of $1.13 million. Small and midsize businesses were targeted disproportionately, accounting for 68 percent of employee theft. Last year the median loss amounted to $289,864. Surprisingly, Hiscox found financial services firms reported the greatest total losses across all industries. Collectively, in 2016 they suffered losses of more than $120 million. One instance lasted for 41 years and involved $2.5 million stolen from a bank.

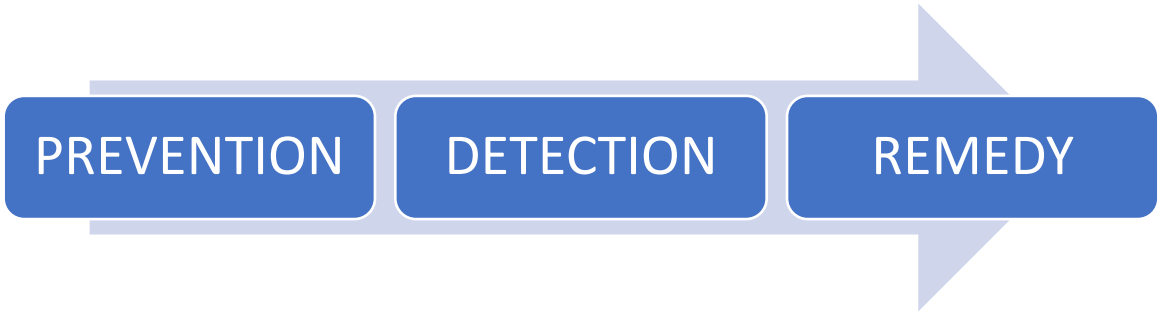
PREVENTION STRATEGIES

The Association of Certified Fraud Examiners (ACFE) indicates that in smaller businesses with 100 or less employees, organizations uncover employee fraud by receiving tips from employees or other persons in 44% percent of cases (Report to the Nations, 2018). 29.3% surveyed said they were allocating new resources to technology, while only 17.3% said they were hiring additional staff dedicated to combatting ORC (Source: NRF Survey)

Not surprisingly, technology is leading the way in protecting business against criminal activity. Experts today consider biometric surveillance technology as one of the most effective means to deter criminal activity in retail establishments Source: Center for Data Innovation 34% decrease in shoplifting reported by retailers using face recognition. 91% decrease in workplace-related injuries from violent assault by retailers using face recognition. 75 million: the number of images FACEFIRST can query in 1/10 of a second.

The figure below highlights the three-step approach to combatting crimes committed against businesses. The first, and most important step is prevention. Prevention is important because when you prevent crime, you do not need to bother with the problems and costs associated with the criminal activity. Although most businesses do not like to spend the money up-front for personnel, technology and other means to prevent crime, the investment pays off. With the average amount of money embezzled in an embezzlement case at $357,650 was the average amount of money embezzled.

The Three-Step Approach to Defending Your Business



Source: Bressler, M. & Bressler, L., 2007.

In addition to technology, prevention techniques should include instituting a review of all bank statements and cancelled checks by someone other than the bookkeeper, ensuring that more than one person sees every transaction. Companies should also perform rigorous background checks, as allowed by law, on all employees — especially those who handle money. Corporate bank statements should be delivered to an owner at their home address. In 65% of embezzlement cases, someone in the company noticed something was amiss and the scheme was uncovered (Hiscox, 2018).

Depending on the type of crime, various technologies can be helpful in preventing crime. For example, to help prevent burglary, exterior lighting, video cameras, and security systems would be the minimum equipment for prevention/detection of burglaries. For other types of criminal activity, sophisticated software programs and special monitoring equipment would help

prevent crime. Because the Price Waterhouse Coopers survey (cited in Verschoor, 2018) reported that the largest cause of fraud (59%) results from weak internal controls, the report recommends investing in people, not just technology.

Some of the more basic preventive techniques include locks, key control, outsourcing payroll, secure websites, secure passwords, drug testing of applicants and/or employees, security guards/dogs, employee background checks, employee I.D. badges, and keeping a minimal amount of cash on hand.

Criminal background checks should be standard procedure for businesses and nonprofit organizations. However, according to the National Small Business Association (2017), 59% of small business employers fail to conduct background checks (https://www.nsba.biz/wp-content/uploads/2017/06/Workforce-Survey-2017.pdf). Background checks not only protect the company against liability, guard the safety of customers and customer financials, they are often required when contracting with larger companies and the federal government (https://www.nsba.biz/wp-content/uploads/2017/06/Workforce-Survey-2017.pdf).

DETECTION STRATEGIES

Technology provides organizations the means to determine who is committing criminal activity and how the activity is committed. Technology is less expensive than employing humans and technology is often able to perform tasks humans are unable to perform. Advancements in technology, such as the developments in biometric technology, provides companies and law enforcement with an important advantage over criminals.

Despite the importance of technology, employees and others play an important part in prevention and detection. HISCOX (2018) reports that someone in the company noticed something was wrong and the embezzlement was uncovered. n 65% of embezzlement cases, someone in the company noticed something was amiss and the scheme was uncovered (Hiscox, 2018).

Standard detection techniques include unscheduled audits, internal auditors, external auditors, alarm systems, financial statement analysis, monitoring employee lifestyle changes, other behavior changes.

Biometrics

Many controls could be used to protect access to a company's digital records (https://www.csoonline.com/article/2130877/data-breach/the-biggest-data-breaches-of-the-21st-century.html; Olson, 2019; Philips, et al, 2000; http://www.upsizemag.com/business-builders/fraud-recovery). Biometric security includes hand movements when working on the computer system, iris or retina scanning, capillary mapping/identification or simple recognitions such as voice or fingerprint identification (Berger, 2007; Robertson, et., al, 2015). Another biometric security which can recently be noted in the news would be Biometric patterns. Steve Jillings, CEO of TeleSign explained how biometric patterns can be identified as legitimate users of the company's system or identified as an intruder. Jillings indicates that their software called Behavior ID can read an individual's manner by which they use a mouse, screen usage, and other employee demonstrates when working on a company's system and not demonstrating the user's biometric patterns can be identified because it is virtually impossible for another person to exactly

duplicate another person's biometric patterns (https://www.cnbc.com/2016/04/05/biometrics-future-of-digital-cyber-security.html).

Biometrics can be very helpful in preventing and detecting fraud in companies, but some authors indicate that unfamiliar face recognition can be prone to error (Robertson, 2015). The author give an example of a younger Asian man utilizing a hyper-realistic silicone mask and he passed by security as an older Caucasian male. In addition, face image manipulation can be purchased for Internet and cell phone users. Apps are available that not only distort a face, but fuse two different pictures into one face while keeping characteristics of both faces intact. Robertson (2015) indicated that acceptance rates for passports merged in this way were significantly higher than a forged passport and the author suggested counter-measures for this type of clever fraud should be researched and perhaps shared with the Department of Defense.

In addition, other authors note that the new security could be use expanded for negative purposes such as racialization (Berger, 2007). Some thought needs be given to protection of privacy with the use of biometric security. Our biometric data should be considered sensitive and personal and that becomes even more difficult with surveillance systems in public areas (Evans, et., al, 2015).

Maguire (2017) noted that biometrics could be expanded to racial identification or racialization and even further, racial profiling. The author noted that even simple fingerprinting can identify races; for example, Jewish persons show whirled fingerprint patterns and although now, no specific identification can be found, as the software becomes more evolved, exact racial matching techniques could be created (Lyon, 2008).

REMEDIES

Cyber Crime & Liability

When an individual, investor, or company experiences financial fraud, they may be dealing with years of recovery from a stolen identity including loss of thousands of dollars, credit ruined, and will most likely be dealing with emotional loss, frustration, fear it could happen again, fear they won't ever recover and, of course, anger toward themselves, the perpetrator, and even the police who will be doing their best to help even though it can be very difficult to help the victims to full financial recovery http://www.accounting-degree.org/scandals/; Pedneault, 2017) ; 2019 http://www.finra.org/investors/highlights/take-action-recover-financial-fraud; https://www.justice.gov/usao-wdwa/victim-witness/victim-info/financial-fraud\; Romanosky et. al., 2011)

But recovery can be possible whether the fraud was perpetrated by employees, management, fraudsters, manipulation, etc. Usually by the time the victims discover the fraud, the stolen funds, will be spent or hidden with little chance of partial or full restitution. If the assets can be identified and located, there can be a better chance of recovery. However, with real estate, the thief may have mortgaged the property to extract all available funds or luxury items may have liens attached to them (Pedneault, 2017)

There can be several ways investors can recover some of the embezzled or stolen funds. (How can investors get money back, 2019). Pedneault (2017) noted it would be a good idea to hire a lawyer not only for their professional expertise, but also to utilize privilege regarding the fraud

and if there would be enough evidence, the victim can imitate criminal as well as civil proceedings at the same time. However, sometimes the only way a victim can recover funds is via insurance. Although many times investors receive only a small percentage of the lost funds, it may be worth the investors' time to investigate the various ways Congress authorized the Securities and Exchange Commission to seek remedies for investors facing fraud. Some of these remedies include receiverships whereby the SEC will file a court action asking a judge to appoint someone to safeguard recovered assets. Another could be the company utilizing Chapter 11 of the Bankruptcy code to reorganize their business rather than a Chapter 7 liquidation whereby only pennies on the dollar lost would be recovered by victims.

A third remedy could be private class action lawsuits which private individuals initiating a lawsuit without the SEC's involvement (How can investors get money back, 2019; Wilt, 2018). In the article *Take Action* (2019), a fourth remedy suggests reporting the fraud to other agencies such as the North American Securities Administrators Association, the National Futures Association or the U.S. Commodity Trading Commission. Black (2013) notes that although some successful private class action lawsuits prevailed in court, it can sometimes be difficult for plaintiff's to even have their day in court because the victims could not specify damages from the unauthorized use of their information being hacked. The author gave an example about the Third Circuit Court upholding a dismissal of charges because the court found "that indefinite risks of future harm and mitigation costs were too speculative to give the plaintiffs standing…"

There can be two schools of thought as to who is to blame when a company has experienced losses from a cybercrime. Gupta and Hassib (2019) indicate that there is the thought process that the blame lays only on the perpetrator as the company did not solicit the crime. The second school of thought deals with whether the company did their due diligence in safeguarding their assets (employees' private information as well as the company's assets including intellectual property and cash or cash equivalents). If the company dealt with cyberthreats by initiating best practices in their industry, the answer could be no, they are victims also. The authors also discussed partial blame to the company noting that there might be special circumstances whereby it was not reasonable to follow industry safeguards against cybercrime and they believed further research would be warranted on this topic because partial blame to companies enduring losses from cybercrime is a new area in digital harm and cybersecurity.

CONCLUSION

Businesses today are more likely to fall victim to more types of crime, including cyber-crimes, and by criminals using more sophisticated techniques and technologies. Smaller businesses often suffer proportionately larger losses and are less able to weather those losses. The Hiscox (Hiscox, 2018) study reports that the typical fraud or embezzlement loss to a small business averages $200,000 and the average cyber-crime loss is $80,000 (Guta, 2018). This can substantially erode profits and even cause some small businesses to close their doors.

Unfortunately, fewer remedies are available to the business owner who becomes a crime victim and those remedies are generally limited to insurance, criminal prosecution of offenders, employee dismissal, negotiations and settlements, and punitive damages. However, small business

owners sometimes fail to protect their business with adequate prevention and detection systems. In addition, some businesses and non-profit organizations become part of the "prevention-paradox" when failing to prosecute criminal acts committed against their business.

Business owners might not want to file charges with the police when the criminal acts are committed by friends, relatives, or long-service employees. This is especially true among non-profit organizations. However, when the business or organization fails to prosecute, the criminal goes free to potentially commit the crime again and again. All too often, smaller businesses choose not to pay for criminal background checks but even when they do, incidents where the business or organization failed to prosecute will not appear.

The best defense is the best defense you can afford. In other words, purchase and use the best prevention and detection technologies and methods available to you. Remedies can help to mitigate losses and serve as a deterrent to help prevent future crimes. In addition, be sure to prosecute offenders rather than letting criminals escape to continue harming businesses and their employees. Finally, be sure to purchase enough insurance coverage to cover all losses and liabilities.

REFERENCES

Armerding, T. (2018). The 17 biggest data breaches of the 21st century. *CSO Online*. Retrieved 02/23/2019 from http://www.accounting-degree.org/scandals/

Berger, V. (2007). Biometrics security technology: The future now. *Security*, *44*, 10-60.

Black, J. (2013). Developments in data security breach liability. *The Business Lawyer*, *69*(1), 199-207.

Bressler, M. & Bressler, L. (Fall, 2007). A Model for Prevention and Detection of Criminal Activity Impacting Small Business. *The Entrepreneurial Executive*, *12*, (1) 23-36.

Crime in the United States, 2017. FBI Uniform Crime Report. Retrieved 02/01/2019 from https://ucr.fbi.gov/crime-in-the-u.s/2017/crime-in-the-u.s.-2017

Egeland, B. (September 4, 2015). Four Ways Cyber Crime Can Hurt Your Small Business. Retrieved 02/01/2019 from https://www.businessknowhow.com/security/cybercrime.htm

Evans, N., Marcel, S., Ross, A., & Teoh, A. B. J. (2015). Biometrics security and privacy protection [from the guest editors]. *IEEE Signal Processing Magazine*, *32*(5), 17-18.

Fraud in small business. Association of Certified Fraud Examiners. Retrieved 01/27/2019 from https://www.acfe.com/uploadedFiles/ACFE_Website/Content/rttn/2018/Fraud-in-Small-Business.pdf

Fruhlinger, J. (October 10, 2018). Top cybersecurity facts, figures, and statistics for 2018. CSOonline. Retrieved 02/02/2019 from https://www.csoonline.com/article/3153707/security/top-cybersecurity-facts-figures-and-statistics.html

Gupta and Hasib (2019). https://healthmanagement.org/c/healthmanagement/issuearticle/when-a-cybercrime-takes-place-who-s-to-blame

Guta, M. (December 3, 2018). Small Businesses Lose $80K on Average to Cybercrime Annually, Better Business Bureau Says. Small Business Trends. Retrieved 02/26/2019 from https://smallbiztrends.com/2018/12/cost-of-a-cyber-attack-small-business.html

Hiscox Embezzlement Study™ (2018). An Insider's View of Employee Theft workplace-crime- costs-us-businesses-50-billion-a-year. Retrieved 01/25/2019 from https://www.cnbc.com/2017/09/12/workplace-crime-costs-us-businesses-50-billion-a-year.html

How can investors get money back in a fraud case involving a violation of the federal securities laws? 2019 https://www.sec.gov/fast-answers/answersrecoverfundshtm.html

Lyon, David. (Nov 2008). Biometrics, Identification and Surveillance. *Bioethics. 22*(9). 499-508.

Maguire, Mark. (Sep 2012). Biopower, Rationalization, and New Security Technology. Social Identities. 18(5), 593-607.

National Small Business Association. (2017). Small Business Workforce and Labor Survey. Retrieved 02/19/2019 from https://www.nsba.biz/wp- content/uploads/2017/06/Workforce-Survey-2017.pdf

Olson, Jason (2019). How to prevent, detect, investigate fraud at your firm. Retrieved 02/23/2019 from http://www.upsizemag.com/business-builders/fraud-recovery

Pedneault, S. (2017). Recovering Losses from Employee Theft and Embezzlement. Retrieved 02/23/2019 from https://www.ctcpas.org/content/27648.aspx

Phillips, P. J., Martin, A., Wilson, C. L., & Przybocki, M. (2000). An introduction to evaluating biometric systems. *Computer*, (2), 56-63.

Provided by HG.org. (2019) https://www.hg.org/legal-articles/security-breach-how-businesses-may-be-liable-44358

Report to the Nations. 2018 Global Study on Occupational Fraud and Abuse, Fraud in Small Business. The Association of Certified Fraud Examiners. Retrieved 01/27/2019 from https://www.acfe.com/rttnresources/

Robertson, D. J., Noyes, E., Dowsett, A. J., Jenkins, R., & Burton, A. M. (2016). Face recognition by metropolitan police super-recognisers. *PloS one*, *11*(2), e0150036.

Romanosky, S., Telang, R., & Acquisti, A. (2011). Do data breach disclosure laws reduce identity theft? *Journal of Policy Analysis and Management*, *30*(2), 256-286.

SBA Office of Advocacy, Small Business Facts. Retrieved 01/25,2019 from https://www.sba.gov/sites/default/files/Business-Survival.pdf

SBIR/STTR The Impact of Cybersecurity on Small Business. Retrieved 02/02/2019 from https://www.sbir.gov/sites/all/themes/sbir/dawnbreaker/img/documents/Course10- Tutorial1.pdf

Simon, M. (March 3, 2016). 30% of businesses will fail because of employee theft. Hill & Hamilton Insurance Blog Retrieved 01/26, 2019 from https://www.hillandhamilton.com/ohio-insurance-blog/30-percent-of-businesses-will-fail- because-of-employee-theft

Small Businesses Can Be Hit With White Collar Crime Retrieved 01/26/2019 from http://smallbusinessdigestmag.com/content/small-businesses-can-be-hit-white-collar- crime

Take Action to Recover http://www.finra.org/investors/highlights/take-action-recover-financial-fraud

Tyree, W. (January 15, 2019). 30 Shocking Retail Loss Prevention and Violent Crime Statistics for 2019. FACEFIRST. Retrieved 01/27/2019 from https://www.facefirst.com/blog/retail-loss-prevention-and-violent-crime-statistics/.

Verschoor, C. (June 2018). Striking jump in business fraud and crime. *Strategic Finance*, 17-18.

Wagner, E. (September 22, 2013). Five Reasons 8 Out Of 10 Businesses, Forbes online. Fail Retrieved 01/26/2019 from https://www.forbes.com/sites/ericwagner/2013/09/12/five- reasons-8-out-of-10-businesses-fail/#38e7d1a16978

Wilt, J. (2018). Cancelled Credit Cards: Substantial Risk of Future Injury as a Basis for Standing in Data Breach Cases. *SMUL Rev.*, *71*, 615.

APPENDICES

Table 1

Financial	impact	of crime	activity
CRIME	Number of offenses	Total value	Cost per offense
Robbery	319,356	$438 million	$1,373
Burglary	1,401,840	$3.4 billion	$2,416
Larceny-theft	5,519,107	$5.6 billion	$1,007
-shoplifting		20% of all theft	$260
Embezzlement-fraud	1,021,226	$300-600 billion	$200,000

Source: 2018 Hiscox Embezzlement Study

Table 2

ANTI-FRAUD CONTROLS
Code of Conduct
Management Review
Management certification of financial statements
Fraud training for executives and managers
Fraud training for employees
Rewards for Whistleblowers
Job rotation/mandatory vacation
Dedicated fraud detection department
Formal fraud risk assessment
Proactive data monitoring/analysis
Surprise audits
Hotline
Independent audit committee
External audit of internal controls
Internal audit department
Anti-fraud policy
External audit of financial statements

Table 3

TOP 5 MANAGEMENT CHANGES DUE TO EMBEZZLEMENT	
1) Employee layoffs	29%
2) Increased spending on auditing	27%
3) Lost customers	26%
Time spent discussing security	26%
Added security & audit requirements	26%
4) Purchased or increased insurance	25%
5) Switched auditors	24%

Source: Report to the Nations, 2018