Issues in Information Systems
Volume 14, Issue 2, pp.39-46, 2013

EXPLORING ACCOUNTING INFORMATION SYSTEMS AND EMBEZZLEMENT FROM NONPROFIT ORGANIZATIONS

Natalya Goreva, Robert Morris University, goreva@rmu.edu
Elaine Luther, Point Park University, eluther@pointpark.edu
George Bromall, Point Park University, gbromall@pointpark.edu

ABSTRACT

This paper makes a case for designing a study to determine if the adoption of Accounting Information Systems (AIS) has contributed to the incidents of embezzlement in small nonprofit organizations. The annual losses to nonprofits attributable to these incidents have been estimated to be 6% of fund raising revenues or 13% of operating budgets; not including unreported events. The total annual losses could be as high as $40 billion. For this paper, we reviewed the literature related to risk management. We reviewed articles and studies related to theft, fraud, and embezzlement in nonprofits. We also reviewed the product features highlighted in promotional material for popular accounting software packages for nonprofits. We concluded that an investigation into the use of accounting software by nonprofits to address our research question (How do nonprofits use accounting information systems to control theft and embezzlement?) could help in the identification of underlying causal factors leading to embezzlement. The goal of the research would be to develop a model for mitigating the risk, based on suggested features for accounting software coupled with recommended human resource and management related practices to be adopted by nonprofits.

Keywords: Accounting Software, Nonprofit Organizations, Financial Theft and Embezzlement

INTRODUCTION AND BACKGROUND

The use of Accounting Information Systems (AIS) has obvious advantages: it significantly reduces the time requirements for accounting activities, decreases the amount of required personnel, and minimizes the chance of error, among other advantages. However, the same advantages often show their negative side when it comes to security. Electronic systems may increase the chance of theft, embezzlement, fraud, and other type of crimes, which become possible for the same reasons: lack of personnel and therefore control, compromised information, and the ease of access to financial assets. Even with no malicious intent from employees, their negligence and failure to comply with security policies is admitted to be one of the most serious problems [13]. The consequences of employees' intentional crime, fraud, theft, and embezzlement, are just as serious. According to the US Chamber of Commerce, American companies lose between $20 and $40 billion a year due to theft by employees [6]. The theft occurs with the help of (not in spite of) Information Systems, such as AIS, electronic bookkeeping, and electronic banking. A survey by Ernst & Young [5] shows that 90% of companies experience such theft, so obviously companies face a serious challenge in preventing it.

The situation is more serious in nonprofits. The estimated annual theft from nonprofit organizations is approximately $40 billion, or 6% of their income [15], which is higher than in for-profit organizations. What causes such a high percentage? Supposedly there are many factors, including a less restrictive environment, little (or no) IT security, and low internal control, among others. Very often there is only one "trusted person" who is in charge of all financial operations with no one assigned to oversee the function.

For-profit organizations are often more focused on security; having to comply with the Sarbanes-Oxley act, they allocate enough resources to provide at least adequate IT security management. Since the adoption of Sarbanes-Oxley in 2002, for-profit organizations have to adhere to specific regulatory requirements regarding risk management and audit control. These rules do not apply to nonprofits; although since 2008, the IRS has required nonprofits to report any losses that have occurred because of theft, fraud, or embezzlement. The very features that make the adoption of accounting software packages attractive, such as ease of use, cost savings, and productivity improvements, might result in the loss of traditional risk management/audit control methods such as separation of duties, and functional oversight. Recognized features to address risk management in AIS could include exception

reports for unusual activities and transactions, forced separation of duties, user access control, multiple user signoffs for select activities, and random screen capture [12]. Additional features could include using AI (artificial intelligence) to recognize transaction patterns, similar to the systems used for fraud detection by credit card companies.

Recent research concerning risk management and security has focused on the prevention, deterrence, and detection of outside threats, or focused on human resource solutions such as training and development and the adoption of ethics statements and security policies. Assuming that all employees are divided into groups that either do or do not comply with security policies, we can further divide the non-complying group into malicious or non-malicious, based on whether they show unintentional negligence/ignorance or deliberate misconduct. Willison and Warkentin [18] admit that the malicious group is less researched than the other groups.

For the purpose of this study we accept the classification where all employees fall into one of the three categories: employees that comply with policies, employees that fail to comply for non-malicious reasons without financial gain (such as negligence, unawareness, and simply unwillingness to comply), and the ones that have criminal intent (Figure 1). What exactly makes employees commit theft, embezzlement, or fraud? Devaney and Tenenbaum [4] argue that employee theft from nonprofit organization occurs because of motivation, rationalization or opportunity. Motivation is primarily for financial reasons, often resulting from low salaries or even no salary in the case of volunteers (very typical for nonprofits). The way employees rationalize their behavior may impact their compliance with security policies [13]. Finally, opportunity is largely based on lack of controls and excessive trust, which is higher in nonprofits [10].

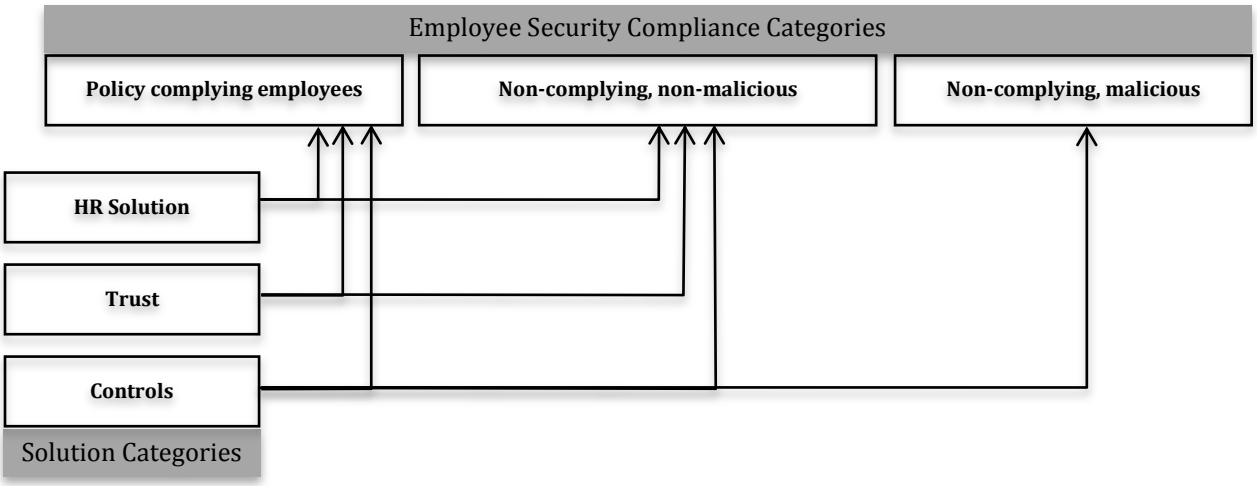

Figure 1. Classification of employees in terms of IT Security compliance

HR solutions such as policies, training sessions, and email updates impact only non-malicious employees, both complying and non-complying. Often, the adherence to policy is based on fear (mainly of losing the job and in some cases being legally responsible), but even though fear may stop some crime in the workplace [7], there is much less fear in nonprofits. Similar reasoning applies to trust and work ethic. In general, HR policies and trust are not sufficient to achieve security compliance [11]. Security controls need to be in place to reduce employee embezzlement and theft, and the goal of our research is to give recommendations as to which accounting software controls need to be implemented.

ACCOUNTING SOFTWARE USED IN FOR-PROFITS AND NONPROFITS

The AIS software offered for financial purposes differs from for- to nonprofit organizations. In for-profit, the emphasis is on governance, compliance, control, and risk management (e.g. SAP and Oracle). On the other hand, the

vendors that advertise AIS for small and nonprofit businesses promote product features such as ease of use, productivity improvements ("headcount reductions"), and cost savings. While there are over 2000 small accounting software packages available in the market, many of which are tailored to specific nonprofit activities or industry applications, there is little information on market share or adoption practices for these products. Information gathered from third party resellers of accounting software and other nonprofit resource providers indicate that there are clear industry leaders. However, of the leading software packages recommended for nonprofits, only 50% are specifically designed for that purpose. An equal number are designed for small for-profit businesses or as a tool for entrepreneurs. The risk management features built into these software packages may be different because of the unique requirements of the targeted users. For example, security concerns for an entrepreneur/sole proprietor might not include embezzlement. Based on the product features that are touted in the advertising materials for the leading 25 software packages selected for this research, the top considerations by nonprofits for adopting software is ease of use, productivity improvements, and cost savings. Only 25% highlighted security features such as audit trails, and Financial Accounting Standards Board (FASB) and general regulatory compliance. When reviewing the product features presented in the marketing literature of the two leading accounting software packages for large for-profit organizations – Oracle and SAP, risk management and security leads the list.

PROFILING THE CASES

No cross-company studies were found that contained a detailed report of nonprofit theft and embezzlement; however, there are many case studies that investigate the specific cases. Many of the recent cases of embezzlement or theft at nonprofits fall into two categories: those either perpetrated by top-level employees such as directors, or by low-level employees or even volunteers such as bookkeepers.

One of the most popular methods of embezzlement found in case studies is writing checks to a person or to a fake company and having the systems set up to not trigger such checks, as in the Kids House of Seminole case where the finance director wrote checks to himself [16]. Another way is to forge checks, signing them on behalf of an authorized person or a person in charge, as in the Pueblo Hispanic Education Foundation where the director forged the board president's signature on the checks issued to himself [1]. Finally, the third method, which is often used in small organizations where only one person is in charge of finances, is to simply expropriate the funds hoping that the transactions will not be audited. This type of embezzlement is often committed by the top management, as in the Caribbean Woman's Health Association case [9], where the executive director expropriated funds by increasing her salary. Another popular case is the Discovery Counseling Center case [8], where the president and the executive director stole more than $150,000 from the grants received by the organization. All methods of embezzlement become possible due to lacks of controls in organizational AIS and to unlimited access by one person to AIS.

The recent cases of embezzlement by directors illustrate how easy it is for those holding top-level positions to divert inventory and cash contributions, misuse credit cards, or even establish payments to fictitious accounts, because of their unlimited access to all financial records. For these cases, the use of budgets or other benchmarks and the routine audits of accounts payable are recommended ways to manage the risk. As an example, an investigation into the embezzlement of $46,000 by an Executive Director of North Carolina's Historic Downtown North Wilkesboro Inc. nonprofit revealed of 270 fraudulent transactions [17]. But this is only a small percentage of the multiple cases of embezzlement by Salvation Army Directors at various locations [14]. A financial manager cut fraudulent checks for over $380,000 in Newark, New Jersey; an executive director in Ottawa Canada was responsible for $240,000 in missing funds, and in Toronto Canada, over $2 million in missing toys was attributed to the director.

If nonprofits regularly used AIS features such as budget development and tracking to actual activities, the risk related to these activities could be reduced. AIS features could also be used to automatically identify financial patterns, using behavior biometrics. Once established, these budgets or benchmarks could be used to trigger exception reports to be reviewed by board members or outside auditors [19].

In the case of bookkeepers, financial constraints and the productivity improvements afforded by adopting AIS at nonprofits, have enabled budget conscious organizations to eliminate positions, resulting in situations where only one person has sole responsibility for all the financial tracking activities, with little or no routine oversight. In a similar case, a bookkeeper at a church in Jacksonville Florida, embezzled $161,000, by writing and cashing

fraudulent checks, inflating her paychecks, and falsifying financial statements. It took nine years for this activity to be discovered by the nonprofit [2].

AIS have allowed nonprofits to reduce operating expenses by reducing the number of employees working on financial records. However, this has resulted in the violation of one of the basic rules of audit control, separation of duties. If nonprofits used AIS features to require two part approvals for select transactions, and audit trails and exception reports to highlight unusual transactions, the routine oversight of these employees could be established [19].

The research into security and risk management often focuses on employee behavior. Deterrence Theory focuses on the use of fear to influence employee behavior [7]. While this can be effective, research into Neutralization Theory shows that that employees often develop ways to deny their guilt or to justify their behavior [13]. This is especially true for low paid or volunteer employees at nonprofits. It is also true for directors or other top employees who recognize the extent of their control and autonomy at an organization. The results of these types of studies show that traditional methods of security and risk management, such as the signing of security policies, training of employees, and even encouraging organizational cultures of security and risk management are not enough. A white paper published by Deloitte [3] identifies five factors to be included in a plan to control fraud, based on the COSO's Internal Control-Integrated Framework: (1) Performing Fraud Risk Assessments, (2) Create a Control Environment, (3) Design and Implement Antifraud Control Activities, (4) Share Information and Communicate, and (5) Monitor Activities.

Deloitte states that establishing an ethical culture, and a clear attitude toward fraud, need to be supported by enforcing established policies for disciplining security and risk violations, and by establishing and promoting controls to prevent, deter, and detect fraud. AIS features can be used for those controls. But it is the use of all these factors that will provide the best level of risk management.

Our research will be looking at how nonprofits use all of these factors in security and risk management to prevent embezzlement and theft. Until recently, nonprofits did not have an incentive to report and discipline or prosecute those involved in embezzlement or theft. Since 2008 nonprofit organizations must report these incidents to the IRS. So, in addition to the obvious financial incentive there are now regulatory and public relations pressures to focus on fraudulent activities.

METHODOLOGY

The following section summarizes the steps we took to support the case presented in this paper. In addition to developing the research question, "How do nonprofits use accounting information systems to control theft and embezzlement?" and reviewing the literature related to theft, embezzlement, and fraud and ethics, and security or risk management related to accounting systems, we also did an investigation into the usage of accounting software by nonprofit organizations.

We reviewed AIS vendor, AIS reseller, and nonprofit resource websites to identify the leading accounting software packages used by small nonprofits. We discovered that unlike AIS selections for large for-profit organizations, where Oracle, SAP, and a small percentage of other vendors share the market, market share and usage information is not readily available for AIS adopted by small nonprofit organizations. There are over 2000 options in this software category, and often nonprofits use accounting software that is designed for entrepreneurs or sole proprietors managing small for-profit organizations, rather than for nonprofits. We narrowed our focus by relying on two nonprofit resources websites (About.com and CPA Practice Advisor) and one reseller (Find Accounting Software) to identify leading or popular accounting software packages used by nonprofits.

We identified 25 accounting software packages, 15 designed specifically for nonprofits, and 10 designed for small for-profit businesses and bigger corporations, to review for this paper. We performed a content analysis on the product features highlighted by the software providers in their marketing materials to identify those features that were important to the vendors and the customers. We then outlined the atomic features that were mentioned in the software descriptions and marketing material (e.g. ease of use, increased productivity, and audit trails). Then we

compared the product claims to the actual features of the software to see if we could confirm if the features existed or if other features might have been overlooked. The results of the content analysis and software package reviews are presented in the Results and Discussion Section below.

In addition, we reviewed the literature and the regulatory requirements for for-profit organizations, namely FASB, Securities Exchange Commission (SEC), and the Sarbanes-Oxley Act of 2002 to identify security features that have been built into accounting and other software. We also identified other practices that can be adopted by organizations to manage risk. The results of this review are presented below and were used to inform the next research steps we have proposed in this paper.

RESULTS AND DISCUSSION

In support of our research question, we anticipated that important product features would include simplicity, low cost, and productivity improvements resulting from headcount reductions or other efficiencies. We also anticipated that security would not be emphasized as much, especially since nonprofit organizations and small, private for-profit businesses are not subject to the same regulatory rules as are large, public, for-profit organizations.

We first did the analysis of the features advertised in both corporate and nonprofit software, without breaking them into two categories. Not surprisingly, less than 25% of all software packages mentioned Security and Compliance, 40% of organizations mentioned Controls/Regulatory considerations, 28% mentioned Audit Trails and only 16% – FASB. In fact, one of the packages claimed to "eliminate tedious and expensive paper trails." Ease of Use, Flexibility, and Productivity Improvements were the most frequent features mentioned in the marketing materials both for corporate and nonprofit software. This supports the case of investigation into if the features or use of existing accounting software packages used by small nonprofits may facilitate or contribute to the incidents of fraud and embezzlement would be important to the industry. The results support the query, but obviously more research is required in order to discover if any relationships exist between AIS and employee embezzlement, and if a model of recommended features could be developed.

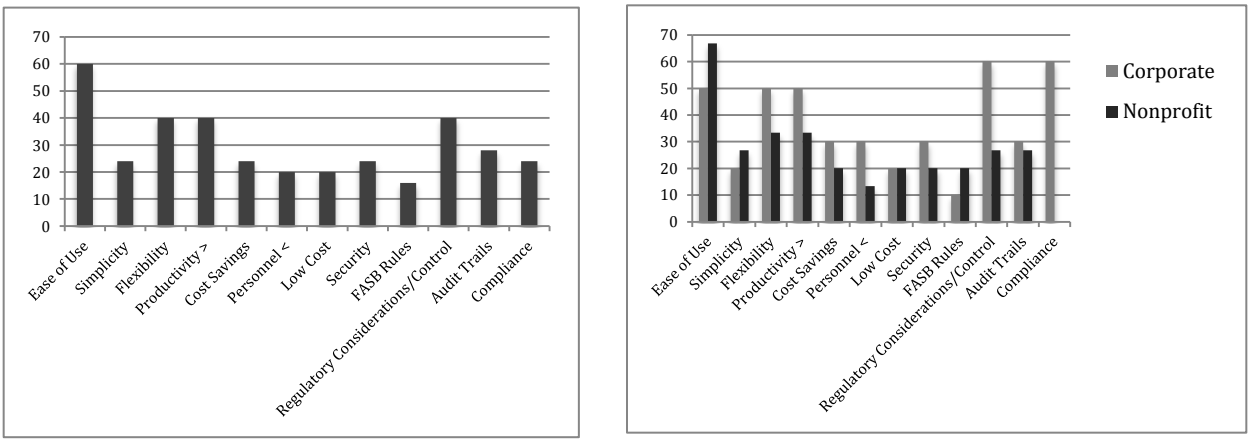

Figure 2. Features advertised in all AIS software (left) and Corporate/Nonprofit (right)

The comparative analysis of corporate and nonprofit software showed that ease of use was the only feature that was emphasized more in nonprofit software advertisement (67% of nonprofits mentioned it as opposed to 50% of for-profits). There was a dramatic difference in favor of for-profits in security-related features, such as Compliance, Security, Regulatory Consideration and Controls. Audit Trails were slightly more emphasized in corporate software. It is worth noting that none of the nonprofit software ads mentioned Compliance.

In reviewing the actual features of the software, we were interested only in the features that enhance the risk management and decrease the possibility of embezzlement (Figure 3). These features were identified as "Security", "FASB Rules", "Regulatory Consideration/Controls", "Audit Trails", and "Compliance". Upon review of these features of the software packages, it was found that, as expected, 100% of for-profit software packages had all the features. The percentage was significantly lower for the nonprofit software. While many nonprofit AIS still have the security features, comply with FASB rules, and provide user controls, less than 60% of nonprofit packages comply with standards and allow audit trails. The results for the software only (without moving to the organizational rules and controls) cause serious concerns about the possibility of embezzlement. However good the organizational controls are, the software flaws negate the attempt to reduce embezzlement and do not add to security.

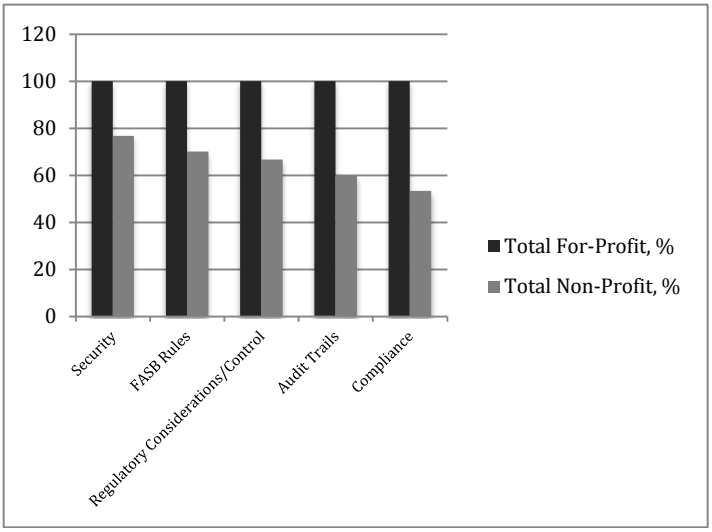

Figure 3. Features actually present in AIS software

CONCLUSIONS

The selection of an appropriate AIS package by a small nonprofit is very difficult. The options are overwhelming and the vendors themselves who are understandably driven by a profit motive often supply the existing advice. Some small nonprofits might select AIS packages designed for small businesses because of the recommendations of board or staff members who have had previous experience or knowledge of those packages. Because of financial considerations, product features such as ease of use and productivity improvements are the factors driving software selection. Since nonprofits are not subject to Sarbanes-Oxley at the present time, security and risk management are not as important when evaluating accounting software packages, despite the evidence that fraud and embezzlement continues to be a significant threat.

As a result, this is how the vendors design and market their software packages. As many of them tout in their marketing materials, their software packages are so simple that the accounting function can be handled by one employee, even one not trained in accounting, perhaps even a volunteer. Of course this makes an AIS package attractive based on short-term financial considerations. But it could possibly place nonprofits at greater risk of fraud and embezzlement because traditional accounting controls such as separation of duties, and multiple approval levels, might be eliminated as part of the resulting productivity improvements obtained from the implementation of AIS packages. This is what we propose to study.

The next step in our research will be to use both quantitative and qualitative methods to discover what practices are being used by nonprofits related to the use of AIS packages, and to the implementation of risk management activities, focusing on employee/staff related fraud and embezzlement. The tool used for this research will be a survey consisting of demographic, AIS and risk management related questions, and subjective questions about the

organizational accounting policies and procedures. A draft of the proposed survey is provided below. Our potential sources for reaching these nonprofits include the Pittsburgh High Tech Council, and local Nonprofit Foundations.

Since the IRS now requires nonprofits to report incidents involving fraud and embezzlement, we also plan to identify a group of nonprofits that have had incidents of fraud and embezzlement. By administering the same survey to this group as well, we could see if there were any significantly different factors between the two groups.

Goals and Objectives

Our objective for this research is to identify and describe how nonprofits use accounting software and manage risk in their organizations. Then to use this information to establish if the practices surrounding the use of AIS in nonprofit organizations, if not the actual designs of the accounting software packages themselves, may be facilitating or contributing to the incidents of employee related fraud and embezzlement.

This research will focus on the exploring the following:

1. What accounting software is being used, if any?
2. Who has responsibility for the accounting function?
3. How the software selection was made?
4. What is their level of security awareness?
5. What are their risk management policies?
6. What are their ethics policies?

Using this information, we plan to develop a model consisting of two parts; suggestions for features to be included in accounting software designed for nonprofit organizations to enhance risk management, and suggestions for steps to be taken by nonprofit organizations when selecting and implementing an accounting software package. Currently, the decision facing nonprofits when select accounting software can be very daunting, with over 2000 options. A model to support this decision making process could be helpful to all nonprofits. If nonprofits begin to focus on the magnitude of potential losses from fraud and embezzlement, this would be a first step in improving their risk management activities. By recognizing that the development of embedded accounting software controls would complement risk management activities and ethics policies, software vendors would be encouraged to adopt these features. Additional costs resulting from these changes would be justified given the existing costs of losses reaching 6% of nonprofit revenues or 13% of operating budgets.

REFERENCES

[1]. Bonham, N. (2010). Nonprofit director arrested. The Pueblo Chiftain, June 5, 2010. Retrieved from http://www.chieftain.com/news/local/nonprofit-director-arrested/article_95df01fa-7074-11df-ae56-001cc4c03286.html on April 10, 2013

[2]. Broward, C. (2012). House arrest for 78-year-old woman who embezzled $161,000 from Jacksonville church. Retrieved from http://jacksonville.com/news/crime/2012-04-05/story/house-arrest-78-year-old-woman-who-embezzled-161000-jacksonville-church on June 20, 2013

[3]. Deloitte. Antifraud programs and controls (report). Retrieved from http://www.deloitte.com/assets/Dcom-Shared%20Assets/Documents/us_assur_Antifraud%20whitepaper.pdf on June 19, 2013

[4]. Devaney, W.H and Tenenbaum, J.S. (2011). Preventing Embezzlement and Fraud in Nonprofit Organizations. Retrieved from http://www.venable.com/files/Publication/32c6e77c-7510-48c1-84fb-7844ede28d5e/Presentation/PublicationAttachment/73aabc87-0653-46c3-a158-7d30f298a994/NYS_Society_of_CPAs__Preventing_and_Detecting_Fraud.pdf on April 12, 2013

[5]. Ernst & Young (2008). Ernst & Young's 2008 global information security survey. Retrieved from www.ey.com/security on April 1, 2013

[6]. Inc.com (1999). Employee theft still costing businesses. Retrieved from http://www.inc.com/articles/1999/05/13731.html on April 12, 2013

[7]. Johnston, A.C. and Warkentin, M. (2010). Fear appeals in information security behaviors: an empirical study. MIS Quarterly, 34(3), pp. 431-433
[8]. Louie, E. (2011). Former Discovery Counseling Center head pays restitution in embezzlement plea deal. Mercury News, September 15, 2011. Retrieved from http://www.mercurynews.com/breaking-news/ci_18903877 on April 8, 2013
[9]. McCann, N. (2010). Cavalcade of Corruption Continues in NYC. Courthouse News Service, July 20, 2010. Retrieved from http://www.courthousenews.com/2010/07/20/28958.htm on April 10, 2013
[10]. Mingers, J., Walshum, G. (2010). Toward ethical information systems: the contribution of discourse ethics. MIS Quarterly, 34(4), pp. 833-854
[11]. Puhkainen, P. and Siponen, M. (2010). Improving employees' compliance through information systems security training: an action research study. MIS Quarterly, 34(4), pp. 757-778
[12]. Romney, M. and Steinbart, P. (2006). Accounting information systems, 10th Ed. Pearson, Prentice Hall, Upper Saddle River, NJ
[13]. Sipponen, M., Vance, A. (2010). Neutralization: new insights into the problem of employee information systems security policy violations. MIS Quarterly, 34(3), pp. 487-502
[14]. Snyder, G. (2012). Nonprofit fraud: is the Salvation Army worthy of our contributions? Retrieved from http://nonprofitimperative.blogspot.com/2012/11/nonprofit-fraud-is-salvation-army.html on June 20, 2013
[15]. Strom, S. (2008). Report sketches crime costing billions: theft from charities. The New York Times, 3/29/08. Retrieved from http://www.nytimes.com/2008/03/29/us/29fraud.html?pagewanted=all&_r=0 on March 20, 2013
[16]. Taylor, J. (2010). Accused Kids House embezzler: I'm a compulsive spender. Orlando Sentinel, June 18, 2010. Retrieved from http://articles.orlandosentinel.com/2010-06-18/news/os-former-finance-director-kids-house20100618_1_compulsive-spender-embezzler-oliver on April 10, 2013
[17]. Technology Insight (2013). Executive director accused in nonprofit embezzlement case. Retrieved from http://www.technology-insight.com/news/accounts-payable-analysis/executive-director-accused-in-nonprofit-embezzlement-case.aspx on June 20, 2013
[18]. Willison, R., Warkentin, M. (2013). Beyond deterrence: an expanded view of employee computer abuse. MIS Quarterly, 37(1), pp. 1-20
[19]. Woodard, J. (2008). Protect your business from fraud: keep your financial information secure. Retrieved from http://http-download.intuit.com/http.intuit/CMO/qbes/resources/pdfs/Intuit_Security_Whitepaper.pdf on May 1, 2013