2011

An Analysis of QuickBooks Internal Control Utilization

Andrew J. Steckel
University of Northern Iowa

AN ANALYSIS OF QUICKBOOKS
INTERNAL CONTROL UTILIZATION

A Thesis

Submitted

in Partial Fulfillment

of the Requirements for the Designation

University Honors with Distinction

Andrew J. Steckel

University of Northern Iowa

May 2011

This Study by: Andrew J. Steckel

Entitled: An Analysis of QuickBooks Internal Control Utilization

has been approved as meeting the thesis or project requirement for the Designation
University Honors with Distinction

________ ____
Date Dennis Schmidt, Honors Thesis Advisor, Department of Accounting

________ ____
Date Jessica Moon, Director, University Honors Program

AN ANALYSIS OF QUICKBOOKS INTERNAL CONTROL UTILIZATION

Introduction

The QuickBooks software created and sold by Intuit, Inc. is the most predominantly used accounting software among small businesses. According to a June 19, 2008 press release issued by Intuit, more than 3.7 million businesses use QuickBooks, and it held a 94.2 percent market share for retail units in the business accounting category as of March 2008 (Intuit, 2008). As such, large amounts of financial data and information are created, edited, and stored using QuickBooks. A large majority of these companies will rarely, if ever, have their financial statements or internal control structures audited. However, the accuracy and security of this information is still vitally important.

I studied the QuickBooks software in particular courses included in the accounting curriculum, and I experienced the use of QuickBooks in the small business environment firsthand while employed as an accounting and research assistant at the university’s John Pappajohn Entrepreneurial Center. These experiences, coupled with my appreciation for the importance of internal controls in the field of accounting, motivated me to design my research study.

The purpose of my research was to explore the built-in information security features within the QuickBooks software that companies utilize. After developing a list of internal control measures available to companies that use QuickBooks, I authored and administered a survey to area businesses to determine how often these features are utilized in practice. The responses provide a useful understanding of the level of security maintained over the financial information of small businesses and highlight areas where improvement is needed.

My paper is organized as follows. First, in a literature review, I will discuss the existing research pertaining to the use of internal controls in QuickBooks. I will examine internal controls and fraud in the small business environment, discuss the relevant legal and regulatory requirements to which companies must adhere regarding information security, and discuss my process of discovering internal control related software features within QuickBooks. Next, I will formally introduce the hypothesis to be tested and the research question to be answered. Then, I will discuss my methodology, and finally, I will analyze the results of my study while making suggestions for further research.

Literature Review

Internal Control and Fraud in a Small Business Environment

Occupational fraud is defined by the Association of Certified Fraud Examiners (ACFE) in its *Report to the Nations* (ACFE, 2010) as "The use of one's occupation for personal enrichment through the deliberate misuse or misapplication of the employing organization's resources or assets" (p. 6). It involves an employee violating the employer's trust and abusing his or her position within the company for personal gain. Survey participants in the 2010 ACFE *Report* estimated that the typical organization loses five percent of its annual revenue to fraud, which amounts to an approximate loss of more than $2.9 trillion when applied to the 2009 Gross World Product. Moreover, the report estimated that fraud schemes lasted a median of 18 months before detection at a median loss of $160,000.

To mitigate the incidence and severity of occupational fraud within an organization, internal controls can be established. The Committee of Sponsoring Organizations of the Treadway Commission (COSO) authored a comprehensive report and framework for understanding and implementing internal controls. COSO broadly defined internal control in its *Integrated Framework* (COSO, 1992) as:

> a process, effected by an entity's board of directors, management and other personnel, designed to provide reasonable assurance regarding the achievement of objectives in the following categories: (1) Effectiveness and efficiency of operations (2) Reliability of financial reporting, and (3) Compliance with applicable laws and regulations. (p. 1)

Included within the first objective are profitability goals and considerations for safeguarding a company's resources.

Even defined as such, internal control is a very broad and sweeping initiative that includes organizational culture, risk assessment, effective communication and information gathering, and various control and monitoring activities. These activities include "approvals, authorizations, verifications, reconciliations, reviews of operating performance, security of assets and segregation of duties," all designed to eliminate employee opportunities to misappropriate assets and detect such occurrences (COSO, 1992, p. 2). The ACFE's *Report* acknowledged that "Anti-fraud controls appear to help reduce the cost and duration of occupational fraud schemes….Victim organizations that had these controls in place had significantly lower losses and time-to-detection than organizations without the controls" (ACFE, 2010, p. 4).

Small businesses may be particularly vulnerable to occupational fraud because they lack the expertise, financial resources, or personnel to implement effective controls. In many instances, small businesses may not have enough employees to separate authorization activities, recording activities, and custody of assets to properly protect themselves. As noted in the *Report* (ACFE, 2010):

> Small organizations are disproportionately victimized by occupational fraud….In general, these organizations have far fewer controls in place to protect their resources from fraud and abuse. Managers and owners of small businesses should focus their control investments on the most cost-effective mechanisms, such as hotlines and setting an

> ethical tone for their employees, as well as those most likely to help prevent and detect the specific fraud schemes that pose the greatest risks to their businesses. (pp. 4-5)

As previously mentioned, a vast majority of small businesses use QuickBooks as their accounting software. Specific features and capabilities have been built into the software by Intuit that can be used to aid in implementing preventive, corrective, and detective internal control measures. Therefore, utilization of these features provides a cost-effective means for pursuing strong internal controls.

Legal and Regulatory Requirements for Businesses Regarding Information Security

In addition to ensuring reliable financial records and the safeguarding of assets, companies that accept debit and credit cards must adhere to certain legal and regulatory requirements. The Payment Card Industry (PCI) has issued a set of Data Security Standards (PCI Council, 2010), and all companies accepting payment cards *must* comply with them as of July 1, 2010 (Sleeter, 2010). Moreover, data breach notification laws have been enacted in recent years in all states except Alabama, Kentucky, New Mexico, and South Dakota. According to these laws, companies would be required to inform customers if a possible breach has occurred (National Conference of State Legislatures, 2010).

Discovery of Internal Control Related Software Features

Through the accounting curriculum at the University of Northern Iowa, students in the major have the opportunity to develop a working knowledge of these built-in features in Accounting Information Systems (120:136) and Advanced Accounting Systems (120:236). Some literature does exist that identifies these features and discusses the importance of their utilization by businesses using the software. Intuit, as part of its *Intuit Academy*, published a manual entitled *Internal Controls for Small Businesses to Reduce the Risk of Fraud* (Intuit, 2009a). The manual provides a lengthy discussion of internal controls in a small business environment, but more than half of the 55-page manual discusses how to implement internal controls in QuickBooks. K2 Enterprises, a company located in Louisiana, specializes in offering business training and continuing professional education, and it created a 63-page manual entitled *Internal Control Procedures for QuickBooks Users* (K2 Enterprises, 2006). The manual is part of a paid curriculum and is not publically available, but K2 Enterprises was kind enough to provide it to me for research purposes. These two manuals proved beneficial in understanding and developing a list of internal control test items.

In addition to educational endeavors as an accounting major and the aforementioned manuals, a column in *The CPA Technology Advisor* entitled “The QuickBooks Advisor” occasionally mentions internal control aspects of the QuickBooks software. An article from the August 2010 issue (Sleeter, 2010) discussed measures companies can take to use QuickBooks internal controls in complying with the recently issued Data Security Standards of the PCI. This, coupled with an implementation guide for complying with the standards using QuickBooks issued by Intuit QuickBooks Support (Intuit, 2010), allowed for the expansion of the internal control list to include test items within a function previously not considered. Companies must comply with the PCI standards as of July 1, 2010, so utilization of control features related to payment cards and customer sensitive data is an important issue.

Several other normative articles have been written discussing the importance and availability of software features within QuickBooks aimed at promoting effective internal controls. DiVito (2008) discusses some essential control features for combating fraud. Likewise, Vetter (2009) notes 25 elements of appropriate controls in QuickBooks. Stephens (2006) discusses the prevalence and cost of occupational fraud and identifies some key QuickBooks features to utilize to mitigate fraud. Nagayama (2008) discusses the importance of usernames and passwords for protecting company data within QuickBooks and limiting employee capabilities and access to data. QBalance, LLC (2008) also notes available internal control features in an e-newsletter to customers. Clearly, the existence and importance of these software features are readily recognized.

Despite the ready existence of built-in internal control features within the QuickBooks software, no empirical research currently exists measuring whether these features are utilized in practice. It does, however, provide for a unique research experience and an opportunity to make a valuable contribution to the field of accounting. Based on my review of the literature and my exposure to the QuickBooks software, I identified 24 internal control features within the software that can reasonably be tested:

- Establish a unique username and password for each employee required to use the software
- Require a complex password to be created and used by each user
- Require frequent changing of passwords
- Limit employee access to only necessary software functions and features
- Disallow the editing or deletion of transactions for users other than the Administrator
- Routinely check for updates to download and install on QuickBooks software
- Enable the preference “Don’t allow any applications to access this company file”
- Enable the preference “Notify the User before running any application whose certificate has expired”
- Use regularly scheduled local backups
- Use online backups
- Set a closing date
- Password protect the closing date
- Regularly update the closing date
- Install QuickBooks on only necessary workstations in the office
- Disable the display of employee social security numbers on reports
- Activate “Require Accounts” setting to avoid unassigned amounts
- Set default bank accounts for deposits and checks
- Utilize the Audit Trail Report to detect unusual transaction edits or deletions
- Utilize the Journal Report to detect unusual transactions
- Utilize the Closing Date Exception Report
- Enable “Customer Credit Card Protection”
- Ensure that users of QuickBooks store customer credit card numbers only in the *Credit Card No.* field of the *Payment Info* tab of customer records

- Refrain from storing sensitive authentication data such as card validation codes (the three digit number near the signature panel), personal identification numbers (PIN), or magnetic strip data
- Establish an External Accountant User (2009 version or later) to hide customer sensitive data from accounting professionals using the company file (for audit, tax, or consulting purposes)

Research Question to Be Answered & Hypothesis to Be Tested

In developing a list of internal control features available in QuickBooks and selecting specific items from that list to test, I hoped to gain at least some initial indication as to whether the features are actually utilized in practice. A large portion of commerce in the United States is conducted by and between small businesses. Many of these companies will rarely, if ever, have their financial statements or internal control structures audited. However, it does not mean that accuracy and information security are unimportant for these businesses. Because a vast majority of small businesses in the United States use the QuickBooks software, I believe that understanding the level of QuickBooks internal control feature utilization will provide a valuable indication about the level of information security maintained by small businesses. Moreover, the results could be used to identify areas where improvement is needed. With such a large number of businesses using a version of the software, the security of a large portion of business- and customer-related data and resources is dependent upon the utilization of these features. As such, my study is aimed at answering the following research question:

> **Q:** What level of security is maintained by small businesses over financial, customer-sensitive, and other proprietary information?

Companies can employ internal control features within the software to reasonably safeguard against employee fraud and error. They can also take active steps using software features to detect employee fraud and error. As previously mentioned, companies can implement strategies within QuickBooks to protect payment card data (and other customer sensitive information) from malicious security breaches. A measurement of internal control test items within these areas will provide insight into levels of information security at small businesses. Efficient and effective information security is in the best interest of consumers, who want personal information protected from fraud and identity theft, but it is also in the best interest of each business because it protects its valuable data for optimum decision making and safeguards its assets. Additionally, due to the Data Security Standards of the PCI and data breach notification laws enacted in recent years by most states, companies would be forced to inform consumers if a possible breach has occurred (National Conference of State Legislatures, 2010). Such a breach would undoubtedly damage customer trust and could even result in costly fines.

Companies may fail to utilize the internal control related features within the QuickBooks software due to several factors, such as a poor understanding of the software, a failure to appreciate the risks associated with fraud or regulatory requirements, an undervaluing of the impact and significance of sound financial records, or time constraints. As a result, my hypothesis is stated as follows:

H: Internal control features within the QuickBooks software are underutilized.

Methodology

I conducted my research using a survey instrument administered via the online survey tool SurveyMonkey. I wanted to create a survey to test only the 10 most essential features from the list of 24 test items mentioned above. Using my own knowledge of internal control and the QuickBooks software, and after speaking with UNI accounting professors Dennis Schmidt and Ronald Abraham, I created my final list of 10 test items. Those 10 survey questions, along with the possible responses are included in Appendix A. Two qualifying survey questions are included at the outset to facilitate use of the survey with SurveyMonkey, and two demographically-oriented questions close the survey. The use of this online survey tool allows for ease of dissemination to area businesses and easier compilation and analysis of results. Because my survey asks purely descriptive questions about company operations, and does not instead ask any behavioral questions of human participants, IRB approval was not necessary for my research according to Anita Gordon, the UNI Director of Research Services.

My initial plan for identifying and contacting area businesses was to contact local CPAs and request that they forward my survey URL to their small business clients who use QuickBooks. However, after contacting some area CPAs with my request, I did not receive any responses from them. Therefore, my next approach was to contact the Greater Cedar Valley Chamber of Commerce and request an e-mail contact list for its membership directory. E-mail contact information for the Chamber's membership, however, is not made publicly available. As such, I obtained a print listing of the Chamber's membership directory which included the business name, mailing address, phone number, and, where applicable, internet address.

I visited the websites of all those member companies that listed them and searched the website for e-mail contact information. If I was able to locate an e-mail address for the owner or a staff member, I sent an e-mail to that address with my survey URL requesting the company's participation in my study. On other occasions, I was only able to find a general information request e-mail (e.g., info@companyname.com); I sent an e-mail to these addresses as well. In addition to using the Cedar Valley Chamber of Commerce directory, I used the online membership directory for the Cedar Rapids Chamber of Commerce to search company websites and find e-mail contact information.

Results

Response Rate

Using this methodology, an e-mail requesting a company's participation in my research study and including a URL hyperlink to my survey was sent to 200 businesses. Of the 200 possible respondents, 144 companies were Greater Cedar Valley Chamber of Commerce members and 56 companies were Cedar Rapids Chamber of Commerce members. A total of 36 responses were received, indicating an overall response rate of 18 percent. Of the 36 responses, only 21 of those companies used a version of QuickBooks as their accounting software.

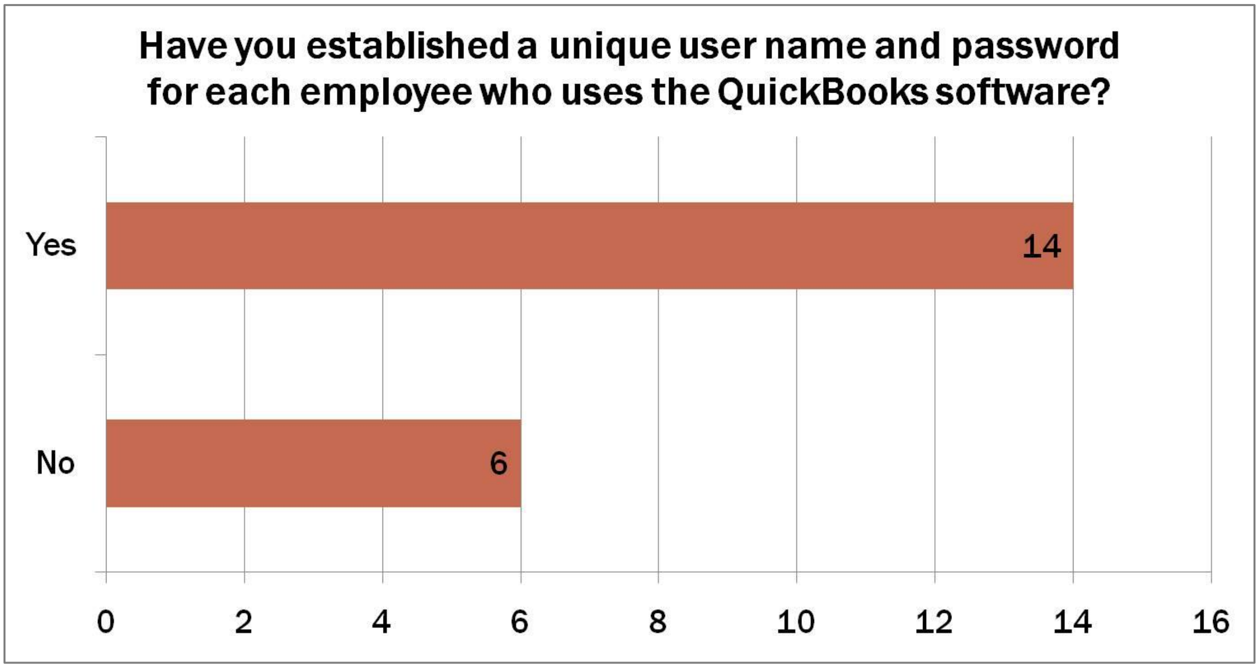
The nature of the survey and the e-mail request sent to potential respondents may have contributed to a lower response rate than what would have been achieved otherwise. Because the survey was sent to companies blindly, without any knowledge of size or sophistication, several of the request recipients may not use QuickBooks. This fact is illustrated by 41.7 percent of the respondents being non-QuickBooks users. Moreover, because the request specifically mentioned a QuickBooks-related survey, non-QuickBooks companies may have been more inclined to ignore the participation request.

Survey Items

The first survey item related to whether a company used the desktop version of the software or QuickBooks Online. Recently, individuals and businesses are increasing their use of cloud computing, whereby software programs and other computing services are provided over the Internet (or "cloud") (NIST, 2011). Therefore, the first survey question provides an interesting indication of how quickly QuickBooks customers are switching to the cloud. Of the 21 QuickBooks users responding to the survey, only one company uses the online version, while

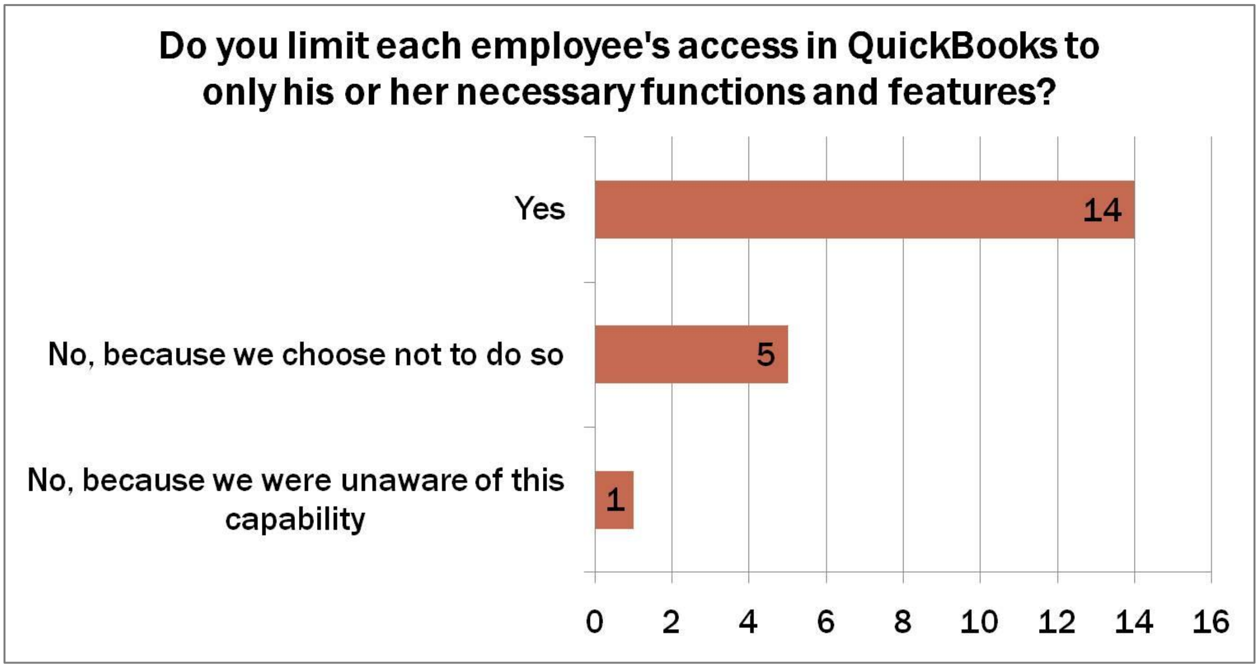
20 used the desktop version of the software. Because only one survey response was received from an online user, no definitive or reliable conclusions could be drawn regarding the use of QuickBooks internal control features in the online environment.

The next survey item examines the use of a very basic, yet imperative control – the use of unique usernames and passwords for each employee using the software. For the 20 respondents from the desktop software environment, the results were as follows:



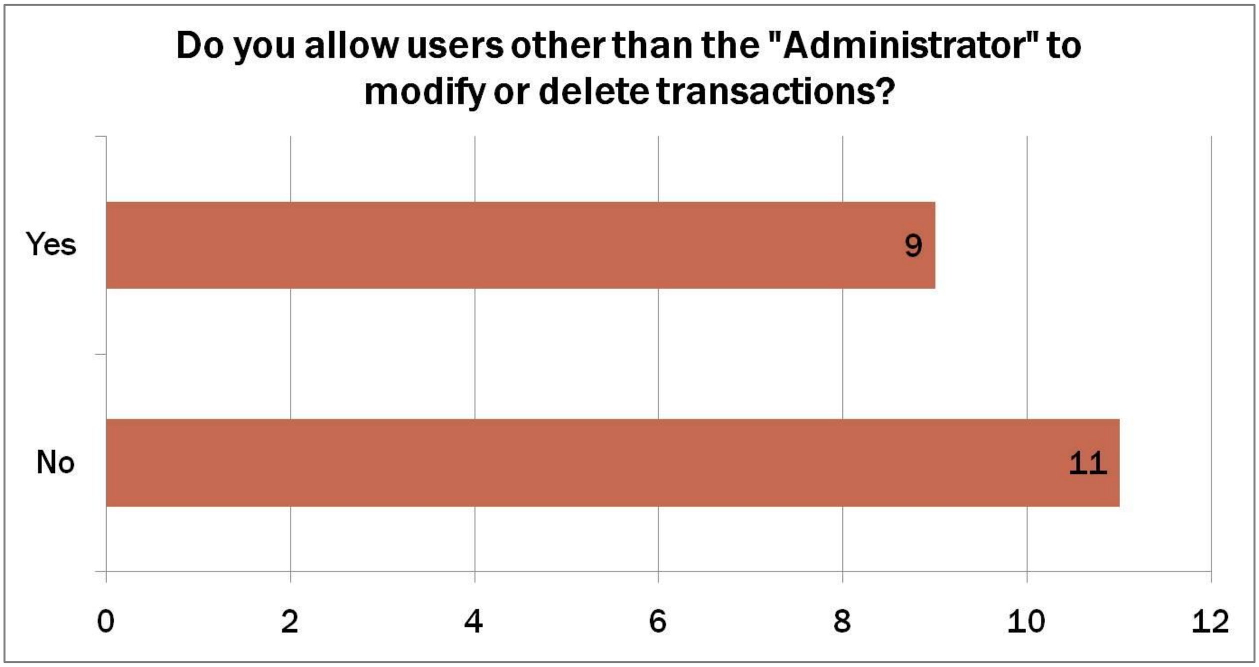
The use of usernames and passwords allows for two important control-related activities – identification and authentication. The username identifies the employee attempting to access the software, and requiring a password authenticates that user. While this is indeed a very base level control, it can assist in preventing unauthorized access to a company's financial records. Even in a one-employee or one-user environment, utilization of a username and password provides important protection. Without this control in place, the QuickBooks file could be opened by anyone with one click, or could be stolen and easily opened. While a 70 percent utilization rate appears to indicate a strong level of control, the desirable level would be 100 percent given that using the control requires no additional cost to the company.

The next survey item pertains to restricting each employee’s software access to specific functions and features. Because the ability to restrict each user’s access to functions within the software is dependent upon having a unique username, the responses to this survey item closely resemble those of the previous item.



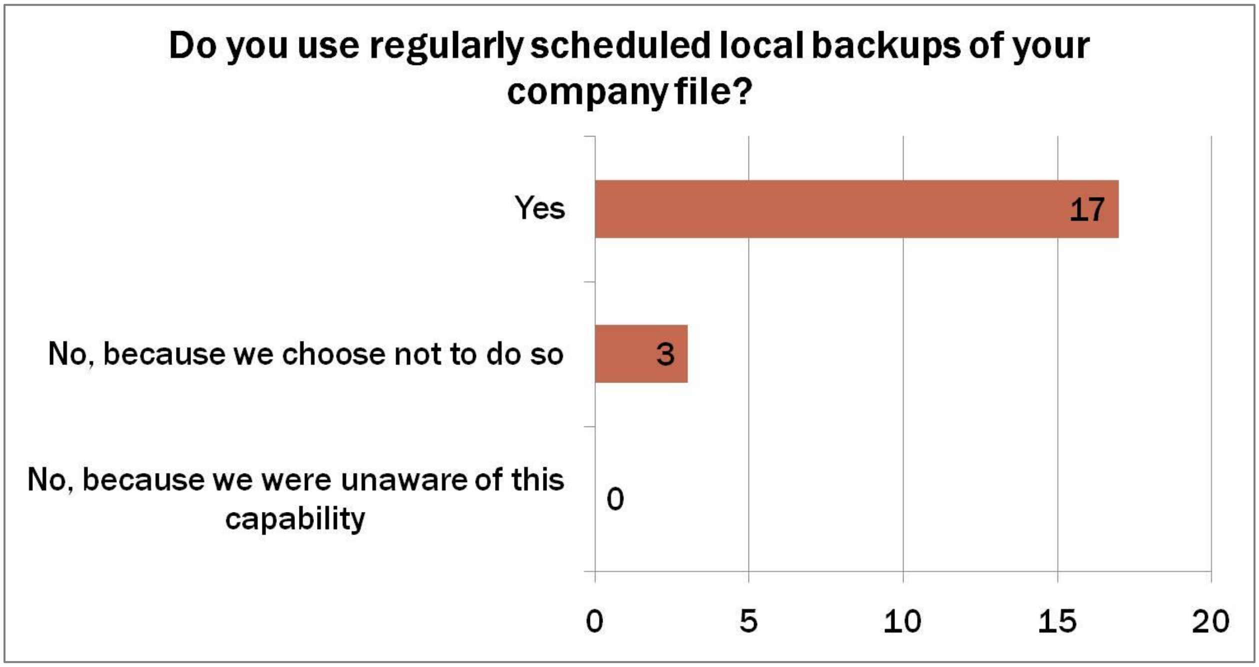
While a clear similarity exists between this survey item and the one preceding it, it nevertheless is an important question because establishing a unique username and password for each user does not necessarily indicate restricting an employee’s access. For example, when an additional user is created in a company file, the administrator can choose to give the new user full access or selective access. In theory, a company could create unique usernames and passwords for each employee using the software but still allow full (administrator-level) access to all users. Obviously, if this is the case, a weaker internal control environment exists, and the maximum benefits of QuickBooks internal controls are not being realized.

The next survey item again relates to the restriction of a user's access rights and capabilities within the software – the ability to modify or delete transactions in the company file. Restricting users other than the Administrator from modifying or deleting transactions can aid in preventing unauthorized manipulation of accounting data used to perpetrate or cover up fraud.



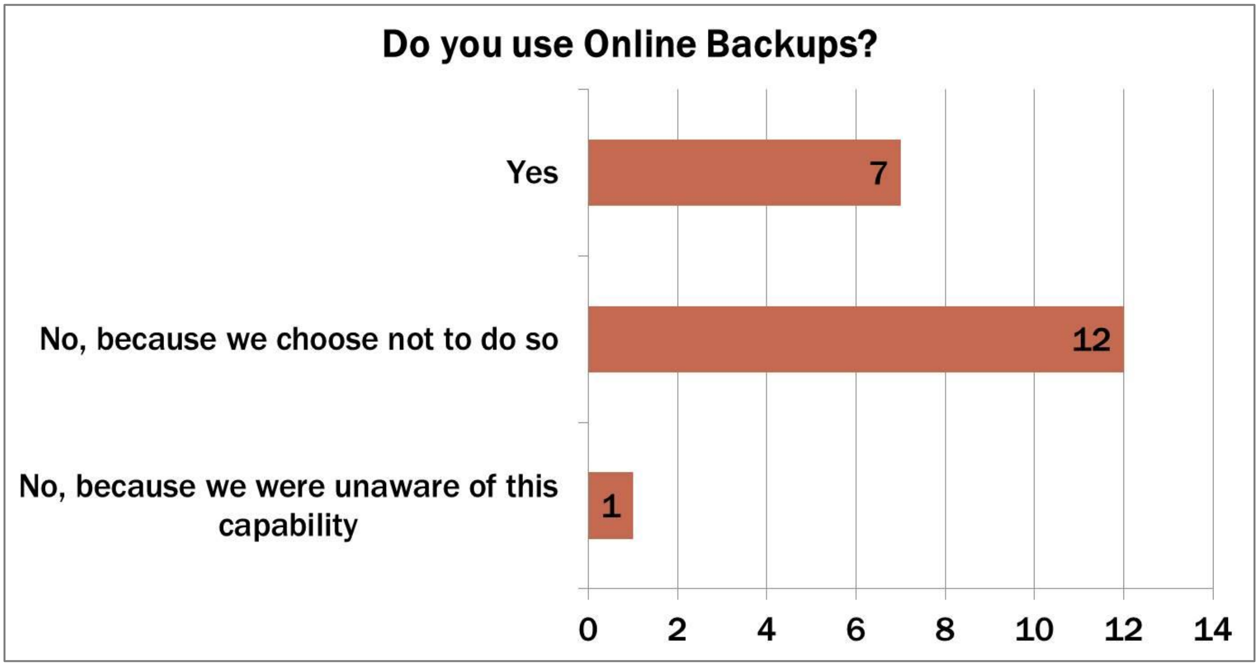
While greater than half of the respondents restrict user capabilities in this way, still nine companies responding did not employ this control. However, neglecting to do so may be more a matter of administrative convenience than failing to understand the importance of controls.

The next two survey items relate to control activities over the backup of company data. These controls are important in the context of disaster recovery and business continuity. Using the software, a company can schedule automated backup of the QuickBooks file at regular intervals (daily, weekly, monthly, etc.). The practice of periodically creating a backup version of a company file to be saved locally accomplishes several goals. First, it establishes a point from which accounting data can be reconstructed should an error or series of errors be committed in the software that cannot be easily corrected. Second, it creates a backup file in case something would happen to the hardware meant to store the operational version of the file. Of course, this control is limited in that any event affecting all of a company's IT resources in a single location will destroy both the operational and backup file. This control appears to be more highly utilized than some others.

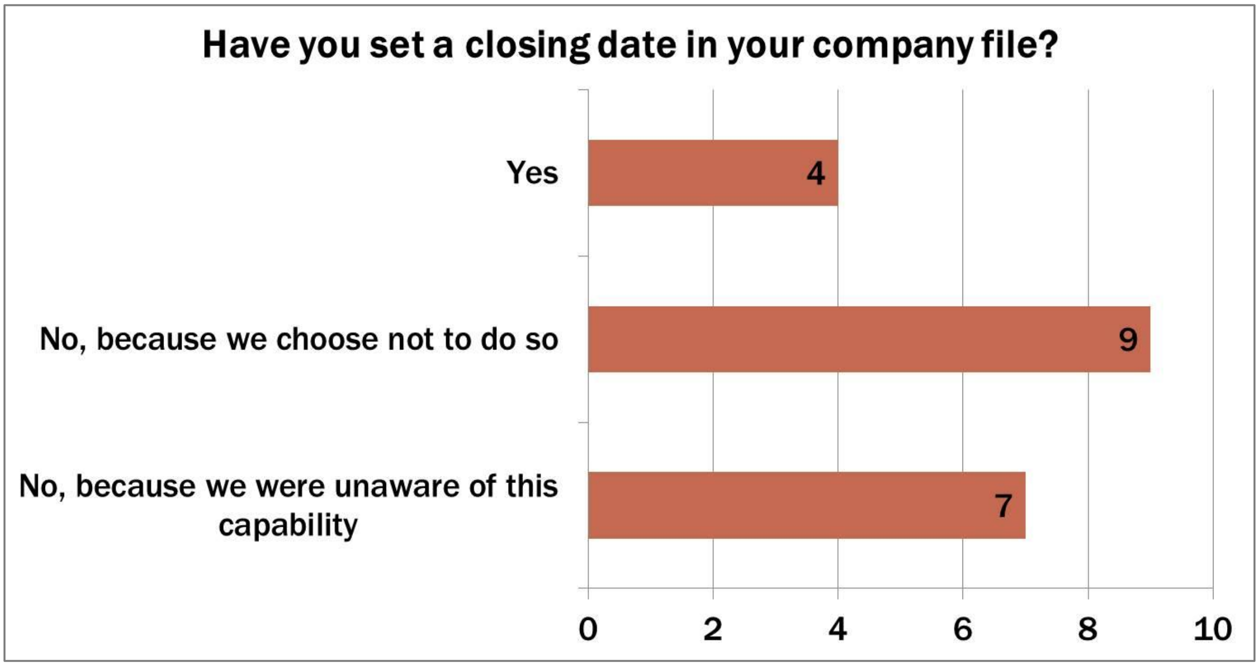


The next control is a valuable extension and improvement on locally saved backups. An "online" backup is one saved on a QuickBooks server maintained by Intuit. Such a practice corrects the limitations of local backups because Intuit servers are obviously in a different geographic location than an individual company's office. Moreover, the reliability of a backup file is further protected because Intuit most likely employs similar controls to further reduce risk, whereby company backup files are saved on multiple servers in multiple locations. Considering the limitations of local backups, the relatively low level of utilization of this control activity is of great concern; the concern is especially great considering that 12 companies elect to forgo this control even with knowledge of its availability. However, the use of online backups through Intuit requires either a monthly or annual fee, which may discourage some companies.

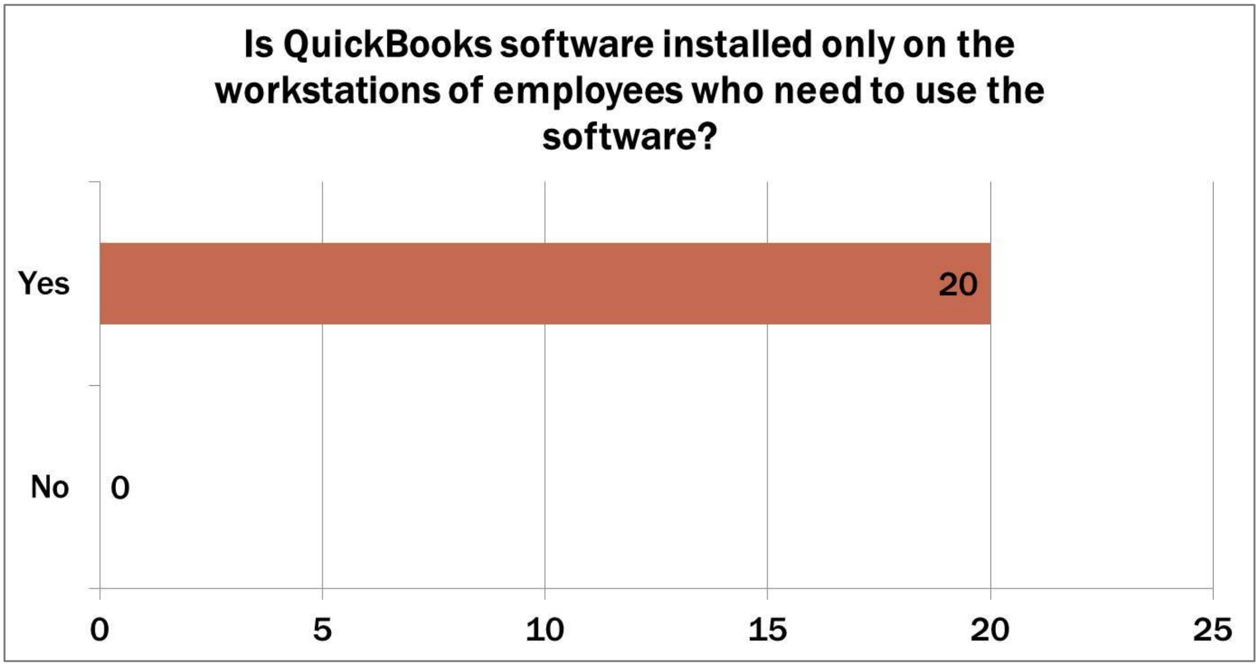
According to Intuit's support website for QuickBooks, the fee is $4.95 per month or $49.95 annually for five gigabytes of online storage, $14.95 per month or $149.95 annually for 25 gigabytes of online storage, or $24.95 per month or $219.95 annually for 75 gigabytes of online storage (Intuit, Inc., 2009b).



The next control tested relates to restricting the dates for which transactions may be entered in a company file. Using what the software calls a closing date, the entering of new transactions and the modification or deletion of previously entered ones can be restricted to only very recent periods. For example, if the Administrator sets the closing date in the company file to June 30, financial information processed prior to and including June 30 will be read-only (except by the Administrator). Therefore, employees would be unable to manipulate past transactions in an effort to commit or conceal fraud. Setting a closing date may also reduce human errors associated with the entry of new information or the accidental modification or deletion of information from prior periods. Again, the survey responses highlight underutilization of internal control. Perhaps of greater concern is that more than half of those companies (nine of 16) simply elect not to use this valuable control.

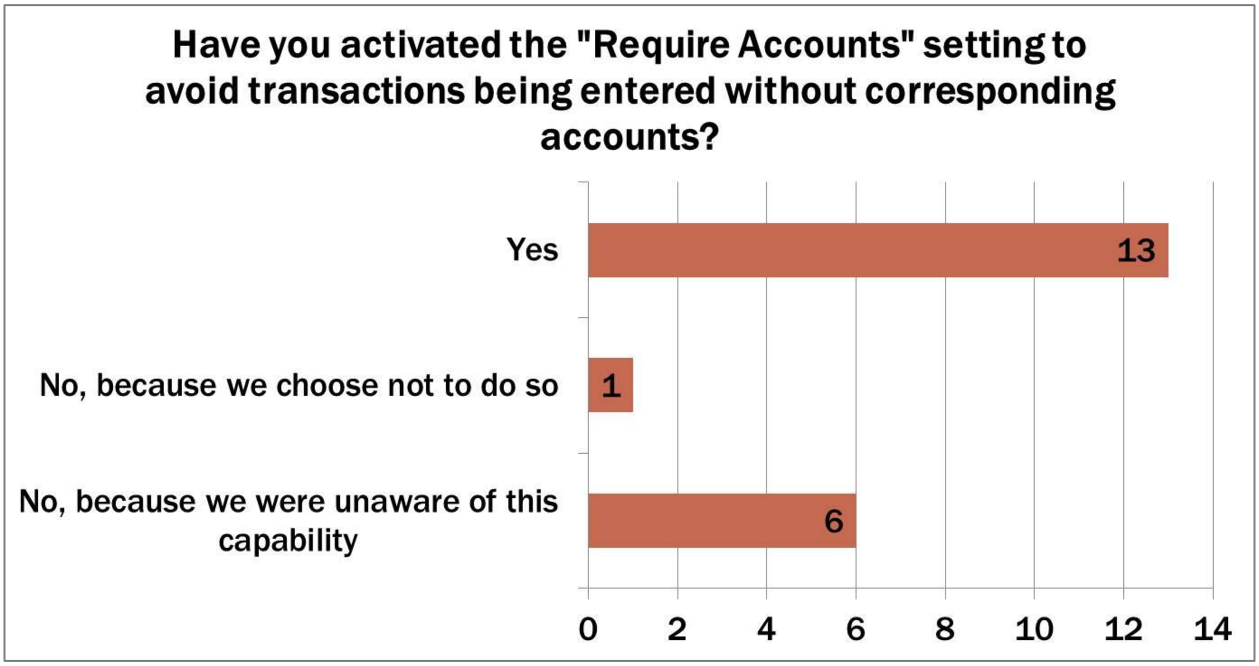


Another preventative control that companies can employ is selective installation of business-related software.



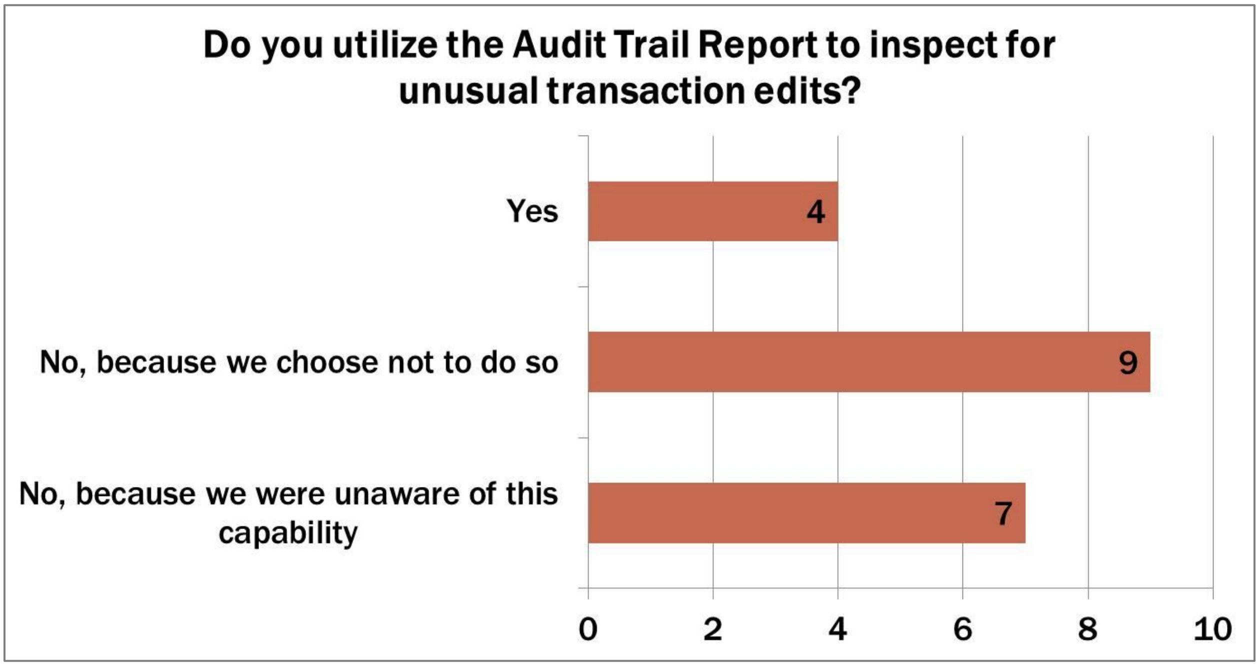
By only installing QuickBooks on the computers of employees that need to use the software, another barrier to unauthorized access to the company file is established. As it relates to this particular control, the survey respondents showed full utilization.

Companies may also utilize a setting in the QuickBooks software called “Require Accounts” to minimize the frequency of human error during data entry. By activating this particular setting, software users are not allowed process and save transactions in the company file unless accounts have been designated to receive the entry (the debits and credits).



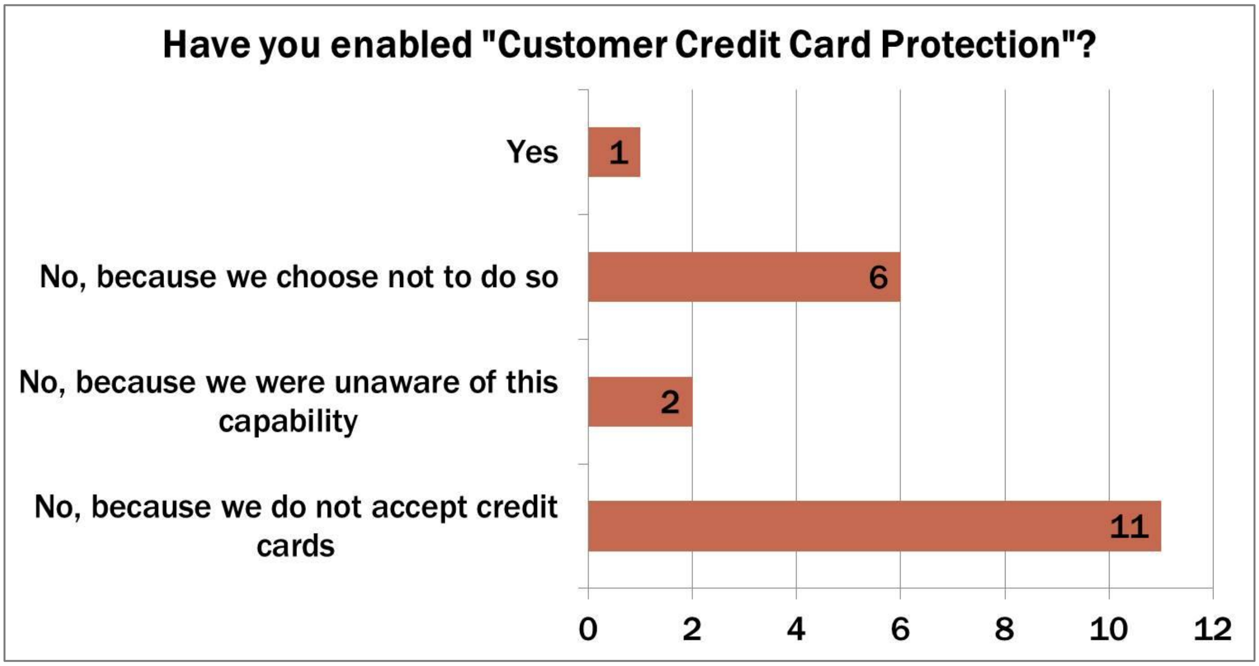
While this control does little in the way of preventing fraud, it does reduce the incidence of human error in the company file and thereby can serve to increase the accuracy of financial information. For this particular control, the survey sample demonstrated a moderate level of utilization. Moreover, a large majority of those failing to employ this control (six of seven) did so due to a lack of information.

In addition to preventative internal controls, companies can employ various detective control measures. Detective controls involve an examination of already processed transactions to discover errors and discrepancies or verify the integrity of previously processed data. While preventative controls are generally preferred to detective controls because it is less costly to prevent errors or fraud than it is to detect and then correct them, any strong internal control structure must employ some detective control activities. One such feature available in the QuickBooks software is the Audit Trail Report. The report is essentially a transaction log, showing all new entries as well as the editing or deleting of previous ones. The report also includes a date and time stamp for each activity and identifies the user account responsible.



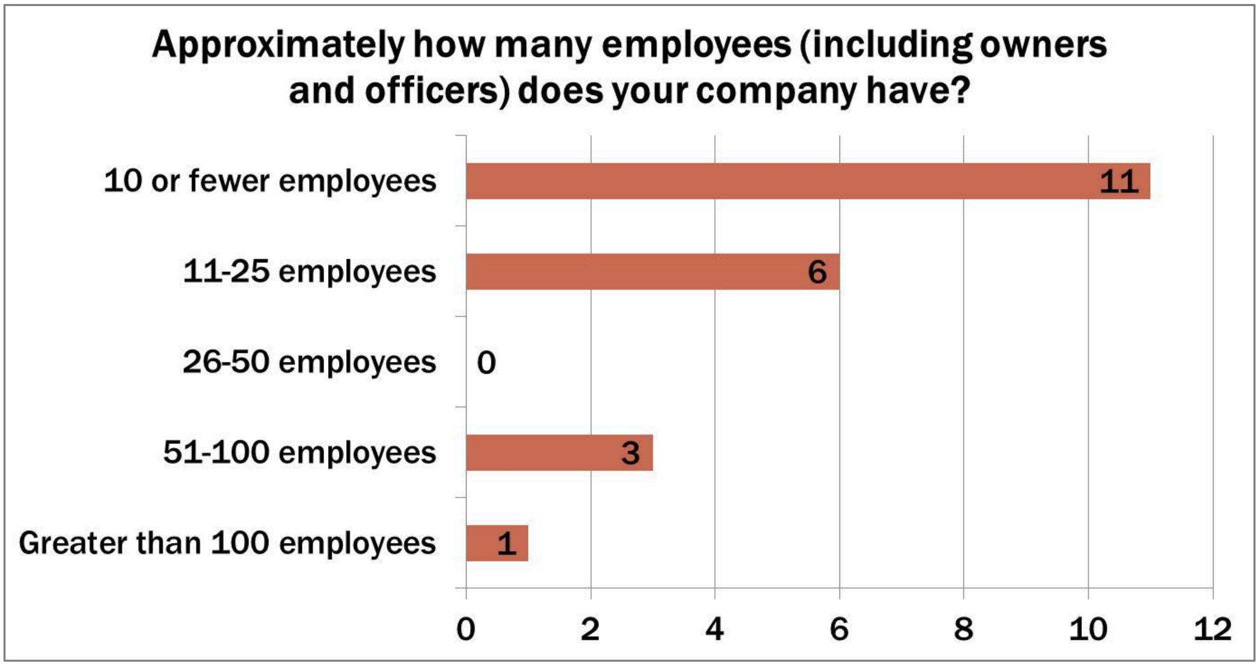
The sample demonstrated a very low level of utilization for this control (20 percent), and again more than half (nine of 16) of the companies failing to use this control simply elect not to do so.

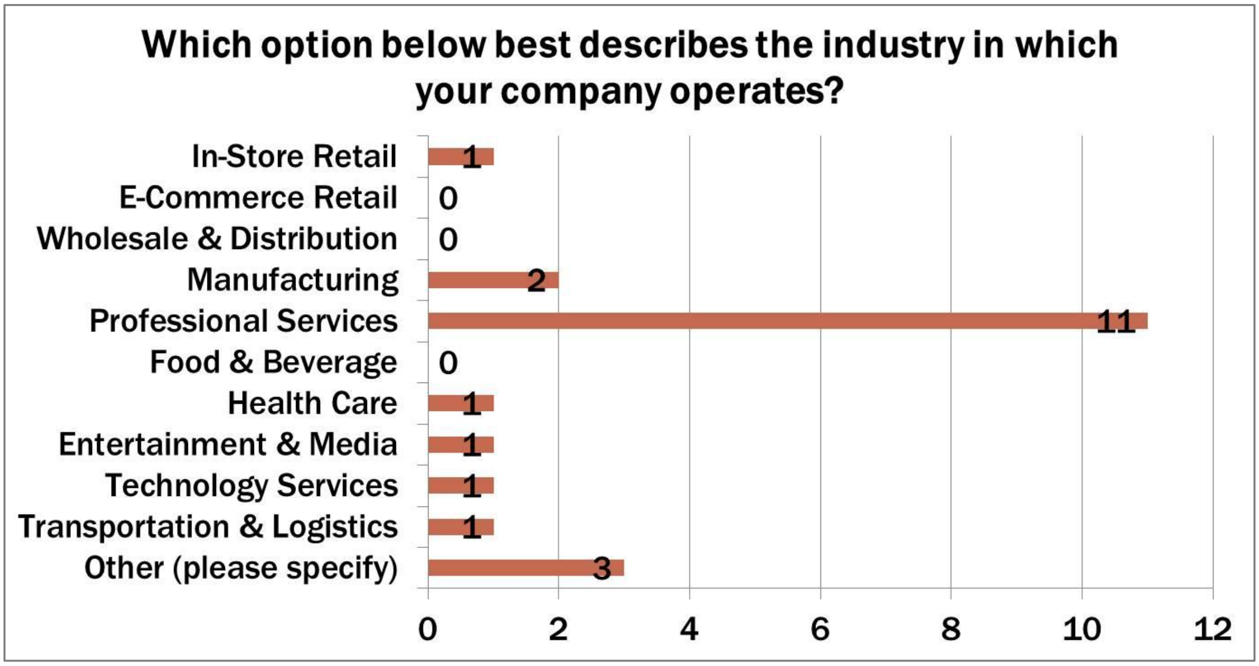
The final control feature tested related to customer information from payment cards. The QuickBooks software contains a feature called “Customer Credit Card Protection.” When this feature is enacted, the software does not show full customer credit card numbers, but rather shows only the final four digits. As previously discussed, controls related to the protection and security of customer payment card data are of extreme importance given the legal and regulatory requirements of businesses.



As a result, the immense neglect of this control by the sample is especially disconcerting – two-thirds (six of nine) of the respondents who accept credit cards elect not to do so.

The final two survey items were intended to collect basic demographic information regarding the relative size of responding firms and the industries in which they participate. As the graph below shows, the survey was effective in garnering responses from small businesses; 17 of the 21 total QuickBooks-user respondents had 25 or fewer employees. The industry-related data show a significantly disproportionate amount of responses from the professional services, with a relatively broad range captured otherwise.





Conclusions, Limitations, and Suggestions for Future Research

The results of my study indicate that, taken as a whole, QuickBooks internal control features are underutilized. Especially when considered in light of a cost-benefit relationship, companies using QuickBooks should employ all available control-related features unless other controls outside of QuickBooks can compensate for forgoing their use. Unfortunately, my study did not investigate for the presence of such compensating controls if respondents indicated not using a QuickBooks control.

An obvious limitation of my study is its small sample size. A larger sample would allow for a greater likelihood that the sample results represent the condition of the actual population. However, given the difficulties encountered in generating survey responses, this study at least provides preliminary results and indications relating to the level of utilization of QuickBooks internal control features. Moreover, my study can guide further, more analytical research to this end.

It is beneficial to examine the data pertaining to each control individually in order to better understand where weaknesses do exist in the internal control structures of small businesses. Moreover, survey respondents elected to forgo the use of a control-related feature in the QuickBooks software at a surprisingly high rate. An interesting avenue for further research would be to investigate management's reasoning for electing to forgo use of these controls. For example, management may not employ the controls due to a poor understanding of the software, a failure to appreciate the risks associated with fraud or regulatory requirements, an undervaluing of the impact and significance of sound financial records, or time constraints.

Another avenue for further research involves determining the level of education and accounting-related expertise possessed by the party or parties responsible for maintaining the QuickBooks company file. Internal control concepts are seldom, if ever, introduced in introductory accounting courses, so even non-accounting business majors may not understand the purpose and value of controls. Such research would go far in efforts to explain why areas of internal control weakness may exist in small business environments.

References

Association of Certified Fraud Examiners. (2010). *Report to the Nations on Occupational Fraud and Abuse*. Retrieved from http://www.acfe.com/rttn/rttn-2010.pdf

Committee of Sponsoring Organizations of the Treadway Commission. (1992). *Internal Control – Integrated Framework Executive Summary*. Retrieved from http://www.coso.org/IC-IntegratedFramework-summary.htm

DiVito, T. (2008). *QuickBooks and Internal Controls*. Retrieved from http://www.rehmann.com/pdfs/News/BWD/Spring2008/QuickBoo.pdf

Intuit, Inc. (2008, June 19). *Intuit Hits 50,000-member Milestone with QuickBooks ProAdvisor Program*. Retrieved from http://about.intuit.com/about_intuit/press_room/press_release/2008/0619qb.jsp

Intuit, Inc. (2009a). *Internal Controls for Small Businesses to Reduce the Risk of Fraud*. Retrieved from http://learn.intuit.com/files/pdf/GoodInternalControls.pdf

Intuit, Inc. (2009b). *Sign Up for QuickBooks Online Backup Service*. Retrieved from http://support.quickbooks.intuit.com/support/Articles/INF12514

Intuit, Inc. (2010, May 12). *QuickBooks Payment Card Industry Data Security Standard (PCI DSS) Implementation Guide*. Retrieved from http://support.quickbooks.intuit.com/OpenCms/sites/default/QBSupportSite/PDFs/PCI_PADSS_QB2010_Implementation_Guide.pdf

K2 Enterprises. (2006). *Internal Control Procedures for QuickBooks Users*. Hammond, LA: K2 Enterprises.

Nagayama, B. (2008). *Improving QuickBooks Internal Control with Passwords*. Retrieved from http://www.bcidot.org/qbb/0647-99.html

National Conference of State Legislatures. (2010, October 12). *State Security Breach Notification Laws*. Retrieved from http://www.ncsl.org/IssuesResearch/TelecommunicationsInformationTechnology/SecurityBreachNotificationLaws/tabid/13489/Default.aspx

National Institute of Standards and Technology. (2011). *The NIST Definition of Cloud Computing (Draft): Recommendations of the National Institute of Standards and Technology*. Retrieved from http://csrc.nist.gov/publications/drafts/800-145/Draft-SP-800-145_cloud-definition.pdf

PCI Security Standards Council, LLC. (2010). *Payment Card Industry (PCI) Data Security Standard: Requirements and Security Assessment Procedures Version 2.0*. Retrieved from https://www.pcisecuritystandards.org/documents/pci_dss_v2.pdf

QBalance, LLC. (2008). *QuickBooks E-Newsletter Volume 2*. Retrieved from http://www.qbalance.com/QuickBooks_newsletter_for_small_business_2.htm

Sleeter, D. (2010). Are Your QuickBooks Clients PCI Compliant? *CPA Technology Advisor*, *20*(4), 31. Retrieved from http://www.cpatechnologyadvisor.com/print/The-CPA-Technology-Advisor/Are-Your-QuickBooks-Clients-PCI-Compliant/1$2917

Stephens, T. (2006). *QuickBooks Internal Control*. Retrieved from http://www.cpafirmsoftware.com/control.htm

Vetter, A. (2009). *Checklist of 25 Elements of Appropriate Controls with QuickBooks*. Retrieved from http://www.accountingweb.com/item/107716

APPENDIX A: SURVEY ITEMS

Does your company utilize QuickBooks software for its accounting and bookkeeping activities?

- Yes
- No

Does your company use the desktop version of the software, or QuickBooks Online?

- Desktop
- Online

Have you established a unique user name and password for each employee required to use the QuickBooks software?

- Yes
- No

Do you limit each employee's access in QuickBooks to only his or her necessary functions and features?

- Yes
- No, because we choose not to do so
- No, because we were unaware of this capability

Do you allow users other than the "Administrator" to edit or delete transactions?

- Yes
- No

Do you use regularly scheduled local backups of your company file?

- Yes
- No, because we choose not to do so
- No, because we were unaware of this capability

Do you use Online Backups?

- Yes
- No, because we choose not to do so
- No, because we were unaware of this capability

Have you set a closing date in your company file?

- Yes
- No, because we choose not to do so
- No, because we were unaware of this capability

Is QuickBooks software installed only on the workstations of employees that need to use the software?

- Yes
- No

Have you activated the "Require Accounts" setting to avoid transactions being entered without corresponding accounts?

- Yes
- No, because we choose not to do so
- No, because we were unaware of this capability

Do you utilize the Audit Trail Report to inspect for unusual transaction edits?

- Yes
- No, because we choose not to do so
- No, because we were unaware of this capability

Have you enabled "Customer Credit Card Protection"?

- Yes
- No, because we choose not to do so
- No, because we were unaware of this capability
- No, because we do not accept credit cards

Approximately how many employees (including owners and officers) does your company have?

- 10 or fewer employees
- 11-25 employees
- 26-50 employees
- 51-100 employees
- Greater than 100 employees

Which option below best describes the industry in which your company operates?

- In-Store Retail
- E-Commerce Retail
- Wholesale & Distribution
- Manufacturing
- Professional Services
- Food & Beverage
- Health Care
- Entertainment & Media
- Technology Services
- Transportation & Logistics
- Other (please specify)