Information Security Risks and Countermeasures in CPA Practices

Ludwig Slusky[1], Rick Stephan Hayes[1] & Richard Lau[1]

[1] College of Business and Economics, California State University, Los Angeles, USA

Correspondence: Ludwig Slusky, College of Business and Economics, California State University, Los Angeles, 90032, USA Tel: 1-323-343-2922. E-mail: lslusky@calstatela.edu

Received: July 12, 2013 Accepted: August 5, 2013 Online Published: August 7, 2013

doi:10.5430/afr.v2n3p123 URL: http://dx.doi.org/10.5430/afr.v2n3p123

Abstract

With proliferation of computers and accounting software, information security became a significant concern for individual CPA practitioners and CPA practices.

This research is based on a survey conducted by the authors at the Second Accounting and Tax CPA seminar at California State University at Los Angeles (CSULA) in 2011. The purpose of this research is to establish metrics and assess cybersecurity for solo practitioners and small and mid-size CPA practices by surveying and analyzing risks that the practices are facing and the countermeasures they employ.

The survey reveals the perceptions and practices of CPA practitioners and employees of CPA firms, small and medium, related to cybersecurity, associated risks in their professional practices, and the challenges they confront in their efforts to prevent, detect, and respond to such risks. Among our key findings are: profiles of CPA practices; indexes for Weighted Risk Expectancy (WRE) as well as Weighted Countermeasure Expectancy (WCE) based on the risk/countermeasure significance and likelihood of occurrences; and comparative analysis of WRE and WCE for CPA firms of various sizes and their averages.

Keywords: CPA, Accounting, Cybersecurity, Information security, Awareness, Risks, Countermeasures, Survey

1. Introduction

1.1 Cybersecurity threats

It is generally recognized that information systems security is crucial to modern business (Cain, 2010). For instance, The "Symantec 2010 SMB Information Protection Survey Global Data" study, conducted by Applied Research, reveals that 42% of the 2,152 companies surveyed in 28 countries have lost data, and three-quarters were hit by cyberattacks in the past year. In the study of 2,500 executives with responsibility for IT security - half from companies of fewer than 100 employees, and half from companies in the 100-to-499 employee range- researchers found that while the dangers of cyberattacks are greater, so is the awareness of these attacks by small to medium sized businesses (SMBs). Deloitte's 2010 Financial Services Global Security Study (Cain, 2010) indicates that information security compliance and remediation based on audit findings are the surveyed companies' top priority.

For a number of years, CPA firms in the US have migrated toward increasing dependence on digital technologies to conduct their operations. As this dependence has increased, the risks associated with cybersecurity have also increased (SEC Division of Corp Finance, 2011). Cybersecurity is the body of technologies, processes and practices designed to protect networks, systems, computers, programs and data from attack, damage or unauthorized access. Recently, there has been an increased focus by US Security and Exchange Commission and members of the legal and accounting professions on these risks and their related impact on the operations of a business entity.

Cybersecurity is becoming more essential necessitating that small to medium CPA firms consider cybersecurity and data breach incidents when deciding how to fulfill their professional obligations. US law and laws in many states require disclosure of data breaches affecting personal information of specific types. Other security incidents may become public knowledge because of unofficial disclosures or because of their effect (e.g., a denial of service attack).

Cyber incidents can result from deliberate attacks or unintentional events. Cyberattacks include, but are not limited to, gaining unauthorized access to digital systems for purposes of misappropriating assets or sensitive information, corrupting data, or causing operational disruption. The objectives of cyberattacks vary widely and may include theft of financial assets, intellectual property, or other sensitive information belonging to business entities, their customers, or other business partners. Cyberattacks may also be directed at disrupting their operations.

Entities that fall victim to successful cyberattacks may incur substantial costs and suffer other negative consequences, which may include, but are not limited to:

- Remediation costs that may include liability for stolen assets or information and repairing system damage that may have been caused. Remediation costs may also include incentives offered to customers or other business partners in an effort to maintain the business relationships after an attack;
- Increased cybersecurity protection costs that may include organizational changes, deploying additional personnel and protection technologies, training employees, and engaging third party experts and consultants;
- Lost revenues resulting from unauthorized use of proprietary information or the failure to retain or attract customers following an attack;
- Litigation; and
- Reputational damage adversely affecting customer or investor confidence.

Because of its considerable national importance, the internet poses a large and tempting target for criminal activities aimed at illegally extracting economic value from accounting firms and their consumers. There is, therefore, broad business and economic value to the practitioner in identifying policies to reduce: (a) the likelihood of such attempts, (b) the likelihood that such attempts will succeed should they take place, and (c) the expected consequences of such activities. (Cordes, 2011)

1.2 Cybersecurity Principles in CPA Practices

CPA practitioners, in addition to the normal concerns over data security, have ethics considerations which impact their decisions regarding cybersecurity practices. U.S. and international standards assign a duty to follow the ethics principles of confidentiality, professional competence and due care, professional behavior and integrity to professional accountants.

Confidentiality is defined in the IESBA Code of Ethics for Professional Accountants as "to respect the confidentiality of information acquired as a result of professional and business relationships and, therefore, not disclose any such information to third parties without proper and specific authority, unless there is a legal or professional right or duty to disclose, nor use the information for the personal advantage of the professional accountant or third parties." (IESBA, 2010). Confidentiality of electronic data is crucial for a professional accounting firm's reputation and is enforced legally.

Various state and federal statutes and regulations require protection of defined categories of personal information. Some of these are likely to apply to CPAs who possess any specified personal information about their employees, clients, clients' employees or customers, opposing parties and their employees, or even witnesses. (Ries, 2010) US Code of Federal Regulation (FTC, 2004) sets forth requirements for an entity information security programs.

Ethics emphasizes that CPAs maintain professional competence and due care. They must maintain professional knowledge and skill at the level required to ensure that a client or employer receives competent professional services based on current developments in practice, legislation and techniques and act diligently and in accordance with applicable technical and professional standards. (IESBA, 2010) This means that as new accounting, communication and security software becomes available that impacts the CPAs work, she should keep current. For instance, encryption is already required for most developed country government agencies that have information about individuals on laptops and portable media. As encryption becomes a security standard, it is likely to become the standard of what is reasonable for CPAs.

Other applicable principles are professional behavior and integrity. Professional behavior is to comply with relevant laws and regulations and avoid any action that discredits the profession. (IESBA, 2010) Some of these laws were discussed above. Integrity is to be straightforward and honest in all professional and business relationships according to the ethics standards. (IESBA, 2010) This ethics principle compels CPAs to be transparent about the information security systems and keep their clients informed.

1.3 Surveys of CPA Practices

Recent surveys have pointed out the needs for security in the financial services and accounting profession. Organizations are starting to recognize the importance of the information security function to business. The increasing sophistication of faceless threats, the change in the threat agents and players, and the decreasing level of

competence required to pose a threat on the internet are all factors that have caused financial services organizations to evolve their security (Cain, 2010)

The AICPA's technology survey from 2008 (Jackson, 2008) until today (AICPA, 2011) found that information security management was the top priority, number one in 2008 and number four in 2011.

Today more than any time in the past a U.S. Certified Public Accountant (CPA) from small to medium firms must understand security policy. As Herrmann (2009) put it, "Virtually every organization must have a written security policy that is based, at a minimum, on the applicable regulations, and be able to demonstrate compliance with that policy." The overriding question is how far along are CPAs today in recognizing and implementing IT security.

CPA firms are just starting to develop strategies for IT. According to a recent *Accounting Today* survey, which polled more than 160 CPA firms, 65 percent of CPA firms revealed that they did not have a dedicated IT partner, while a stunning 82 percent admitted to not even having a formalized or written IT strategy in place. (Fineberg, 2010) Among respondents with a staff of 10 or less, 81 percent were without a dedicated IT person, and usually relied on the managing partner to make IT-related decisions.

The most common software deployed at CPA firms was tax prep (81 percent), with payroll (70 percent) and client write-up (61 percent) rounding out the top three. Business intelligence (13 percent) and customer relationship management (17 percent) were reported as the least-used applications at the surveyed firms.

Another consideration to CPA firm security is the increasing security risk of their own personnel. A recent security awareness report (Clearswift, 2010) found that 44% of office workers report storing data at work on personal memory devices, 39% download software to their computer at work and 23% use personal accounts on social networks to comment about their job. Recent Web 2.0 technology (personal and business internet usage coming together, social media) and its integration into existing IT infrastructures make the requirement for a clear, effective and workable IT security policy more important than ever before. (Turner, 2011) It is clear that, as technology for sharing information becomes more sophisticated and embedded in our lives, it becomes more important for those with access to data in the workplace to understand what is permitted by the business, and which activities may be putting data security at risk.

Employees' compliance with information security policies is reported as a key information security problem for organizations (Ernst & Young, 2008; Puhakainen, 2006). It is estimated that over half of all information systems security breaches are indirectly or directly caused by employees' poor information system (IS) security compliance (Dhillon & Moores, 2001; Stanton et al., 2005). Employee violations of IS security policies are most often due to negligence or ignorance of IS security policies on the part of employees (Vroom & von Solms 2004), even in organizations in which IS security policies and staff are present (Puhakainen 2006).

Disconnect between Information Security practices and awareness has been noticed in various areas. In education, for example, Slusky & Partow (2012) demonstrated that the level of information security awareness of students exceeds their level of information security practices.

Surveys are conducted annually to access global IT security, but there are no surveys of CPAs from small to medium sized enterprises. To fill this gap the authors designed and administered our survey of CPAs who are owners or employees in small to medium sized enterprises.

2. Research Purpose and Hypothesis

The **purpose** of this research is to establish metrics and assess cybersecurity for solo practitioners, small and mid-size CPA practices by surveying and analyzing risks that the CPA practices are facing and the countermeasures they employ.

CPA firms differ significantly by size (number of employees, number of clients), type of services provided to clients, and other factors. It would be expected that they may also differ in terms of cyber maturity (i.e., level of information security practices vs. information security awareness).

The idea that firms differ in cyber maturity led the authors to two research questions:

- Is there a method to measure CPA firm's cyber assurance maturity by analyzing expected risks (loss) and use of countermeasures (protection)?
- Are there any significant differences in cybersecurity risks and use of countermeasures among different types of CPA practices?

3. Cybersecurity Survey Mapping and Administration

3.1 Survey Mapping

Based on the information security vulnerabilities typical for CPA practices, the authors created a survey instrument. This survey instrument underwent a verification test administered at the Second Accounting and Tax CPA seminar at California State University at Los Angeles (CSULA), whose participants made several suggestions about the content and mapping of the questions. With these recommendations, the survey instrument was reorganized and the questions were grouped into three categories: Profile (of practice), Risks, and Countermeasures. The assessment of Risks and Countermeasures objectives of cybersecurity were investigated using dual-focus (paired) questions addressing two aspects of the same risk or countermeasure: likelihood of occurrence in CPA's practice and perceived significance of loss (impact). For example, a question would ask a participant to assess both the likelihood of occurrence of a specific risk in the participant's practice and the loss which is likely to result from a single occurrence of this risk. Countermeasures were surveyed with the same approach: a question would ask a participant to assess in their CPA practice both a likelihood of having a specific countermeasure and the likely impact if their practice used that countermeasure.

Altogether, the survey questions were mapped into three categories and five sub-categories as shown in Figure 1.

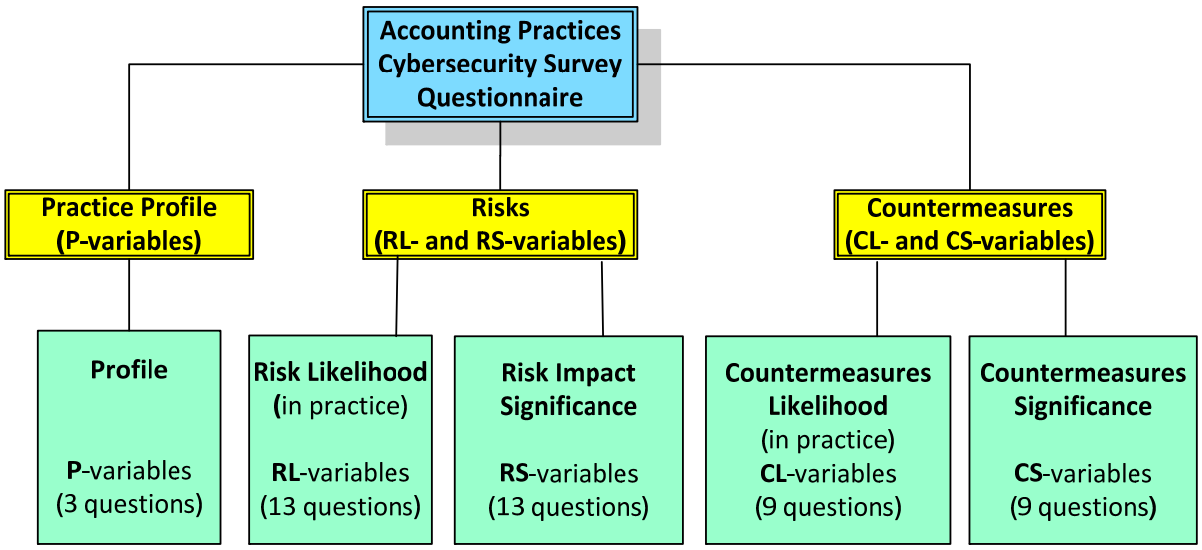

Figure 1. Survey questions mapping (with number of questions)

Because of the logistical constraints for execution of the survey (e.g., the time required for a participant to complete the survey), the authors limited the survey to a single double-sided page, which nevertheless included 47 short questions.

As the survey mapping demonstrates, the survey questions were logically sub-divided into three categories to focus the respondent on (1) a description of the individual CPA practitioner or CPA firm, (2) cyber vulnerabilities of the practice, and (3) what cyber defenses can be employed.

Risks and countermeasures assessed by likelihood and significance are mapped into the RCLS (Risk-Countermeasure-Likelihood-Significance) matrix (see Table 1).

The respondents' perception of the likelihood of risks and countermeasures in practice was investigated with the following two sub-categories of data:

RL The **likelihood** of cyber **risks** that a practitioner perceives in his/her practice

CL The **likelihood** of cyber **countermeasures** that a practitioner employs in his/her practice

The respondents' awareness of potential losses from risks and the protection effect (impact) of countermeasures was investigated with the following sub-categories of data:

RS Participant's perception of **significance** of cyber **risks**; it is also the participants awareness of risks

CS Participant's perception of **significance** (impact) of protection provided by **countermeasures**; it is also the participants awareness of countermeasures

Combined, parameters RL, CL, RS, and CS are characteristics of the participant's cybersecurity maturity level (see Table 1).

Table 1. RCLS Matrix (Risk-Countermeasure-Likelihood-Significance)

	Risks	Countermeasures
Likelihood	RL	CL
Significance	RS	CS

A similar approach was used to assess Information Security practices vs. Information Security awareness among students. (Slusky & Partow, 2012).

3.2 Survey procedure

The survey was administered to CPA practitioners and employees of CPA firms who attended a four-class annual seminar designed for CPAs seeking continuing professional education (CPE) credit on campus at California State University at Los Angeles and one day CPE seminars for the California Society of CPAs in Seattle, Washington and Pasadena, California.

The survey was conducted during a routine CPA training for five groups. The survey was anonymous.

The survey used a non-representative sample of the CPA population under study.

The subjects were asked individually for consent to participate in the survey. If they agreed, they were handed the surveys which they completed before the end of the class.

It was interviewer-administered using a paper form with closed-end questions; no incentives were offered to participants for completing the survey.

The participants were given 30 minutes to complete and submit the survey. The collected survey forms were validated for completeness. Altogether, 99 CPAs participated in the survey, but after review for accuracy and omissions, only 82 completed survey forms were accepted for further analysis.

The survey instructions clearly outlined the purpose of the survey and explained how to answer the questionnaire. The questionnaire form was designed for maximum efficiency having the constraint of time (10-20 minutes) and length (a single double-sided page).

The survey used interval type measurement scales: a three-point scale (e.g., not significant, marginally significant, and very significant), a four-point scale (e.g., unlikely, moderate, likely, very likely), and seven-point scale (e.g., numerical intervals).

4. Profiles of CPA Practices

After the collected survey results were validated for any missing data, they were analyzed using SPSS Statistics software, were each survey item was represented as a variable of one of three categories:

Px for profile items

RxL and RxS for risk's likelihood and significance items

CxL and CxS for countermeasure's likelihood and significance items

where x is a sequential number within a category.

In total, there were 52 variable types collected from 82 respondents' forms resulting in 4264 data items.

The first 3 questions in the survey were designed to collect information about participant's practices:

P1 type of practice

P2 number of employees

P3 number of clients

The type of practice (P1) defines person's work responsibilities and, consequently, involvement in cybersecurity practices. Distribution of the participants by practice type is illustrated in Figure 2. The statistical breakdown is as follows: Tax 67%, Compilation 50%, Bookkeeping 49%; Consulting 33%, Audit 27% and Other 21%. Some participants were involved in multiple CPA activities types, therefore, the total in this distribution is not 100%. About 40% of participants indicated a single work type. Among those respondents who shared responsibilities in several areas, the largest group of practitioners primarily engaged in tax preparations, consulting, bookkeeping and compilation (11%).

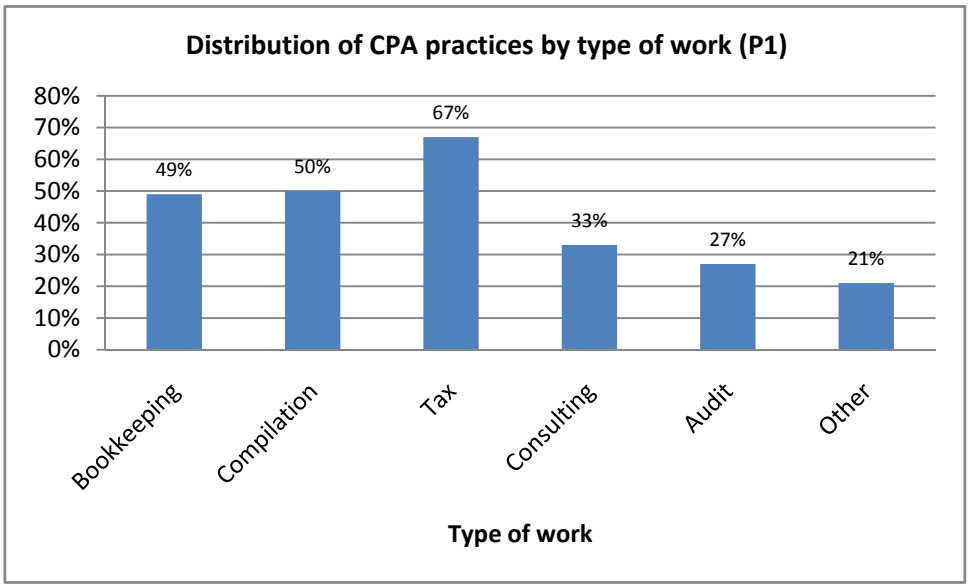

Figure 2. Distribution of respondents by type of work (P1)

Although the authors did not survey the type of data with which the respondents operated in each activity type, this information was gathered during the focus group sessions. The type of data that forms the basis of the small to medium CPA practices are financial accounting records (source documents, journals and ledgers), tax information, consulting work papers, contracts, and review or audit work papers. The users of this data, other than the CPAs and their staff, are their clients which include individuals, corporation, organizations, and federal/state agencies.

The survey participants represented diverse organizations of various sizes (P2). Some of the participants were solo-proprietors while others came from small and medium (25+ employees) accounting firms. (One person was not a practicing accountant.) As Figure 3 shows, the majority of the surveyed participants represented small practices consisting of only 1-10 employees and the firms with 25+ employees. This distribution is not indicative of the CPA practices in the USA (see www.statista.com for general data on number of employees by sectors in the USA).

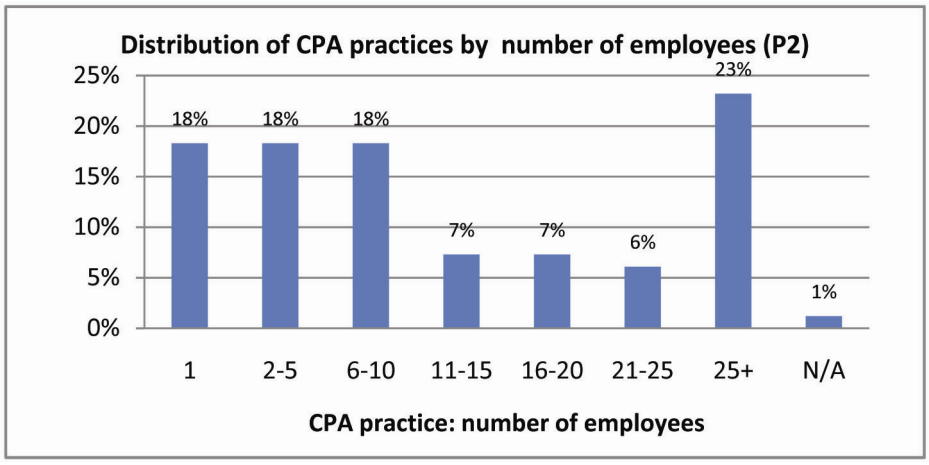

Figure 3. Number of employees in CPA practices

The firms also significantly differ by the number of clients they served, ranging from 0 to 200+. Figure 4 shows the distribution of the respondents representing firms of various sizes as measured by number of clients. The larger firms with 200 and more clients were represented by 43% of participants. Other firms were represented evenly by about 10% of the participants for each client number bracket.

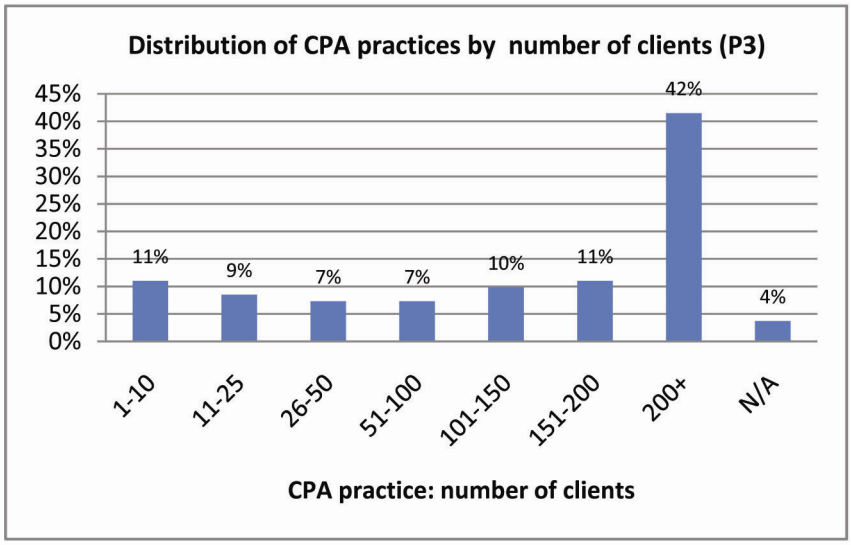

Figure 4. Number of clients

Analysis of the CPA user functions and information flows in CPA practice as well as the collected survey data showed that the size of the CPA practice (P2) has a greater impact on its cyber maturity than the remaining two factors (P1 and P3).

5. Risks and Countermeasures

5.1 Average risks likelihood and significance

The average likelihood of risk losses for each category of the risks is illustrated in Figure 5.

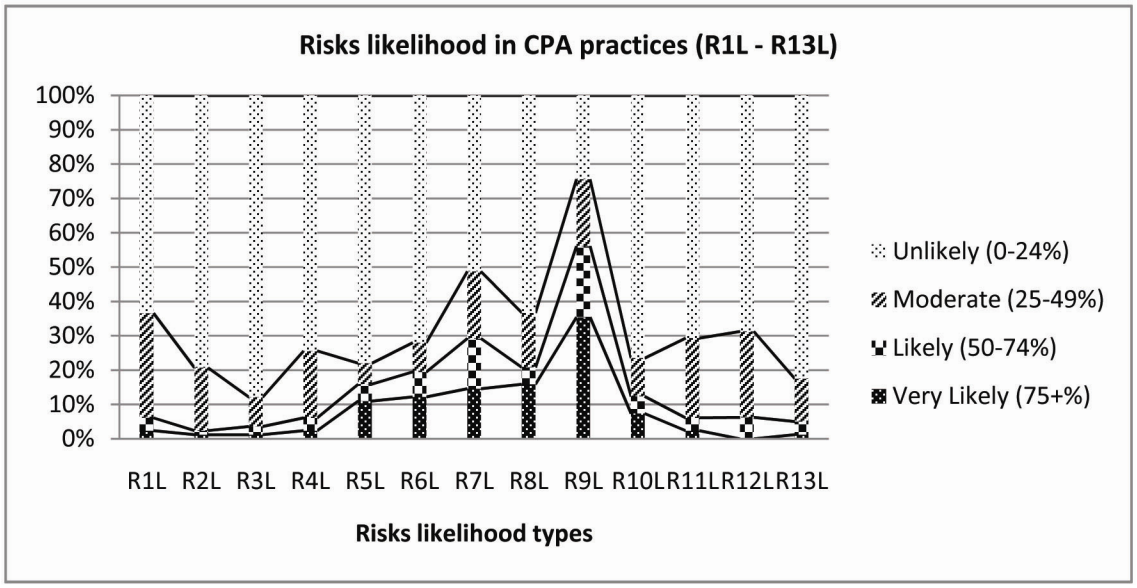

Figure 5. Risks' Likelihood (R#L) in CPA practices

Legend of risks likelihood:

R1L Human errors resulting in accidental destruction of client's data

R2L Accidental, unintentional disclosure of client's sensitive data

R3L Malicious, deliberate breaches of security of client's sensitive data

R4L Employees' dishonesty theft

R5L Employees being unrestricted from changing security settings for Web

R6L Employees sharing login passwords for computer applications

R7L Employees taking home clients' data on a removable storage device

R8L Access to client's data over the Web (today or in the future)

R9L Firm's computers used for personal needs (email, etc.)

R10L Employees installing unauthorized software or hardware on the firm's computers

R11L Disgruntled employee or dissatisfied client damaging firm's computers data

R12L Firm's legal losses from a lack of confidentiality protection of clients' data

R13L Firm's legal losses from a lack of confidentiality protection of employees' data

The three highest risk likelihoods in Figure 5 include the firm's computers being used for personal needs (R9), employees taking home clients' data on a removable storage device (R7), and human errors resulting in accidental destruction of client's data (R1L).

The average significance of risks for each category of the risks is illustrated in Figure 6.

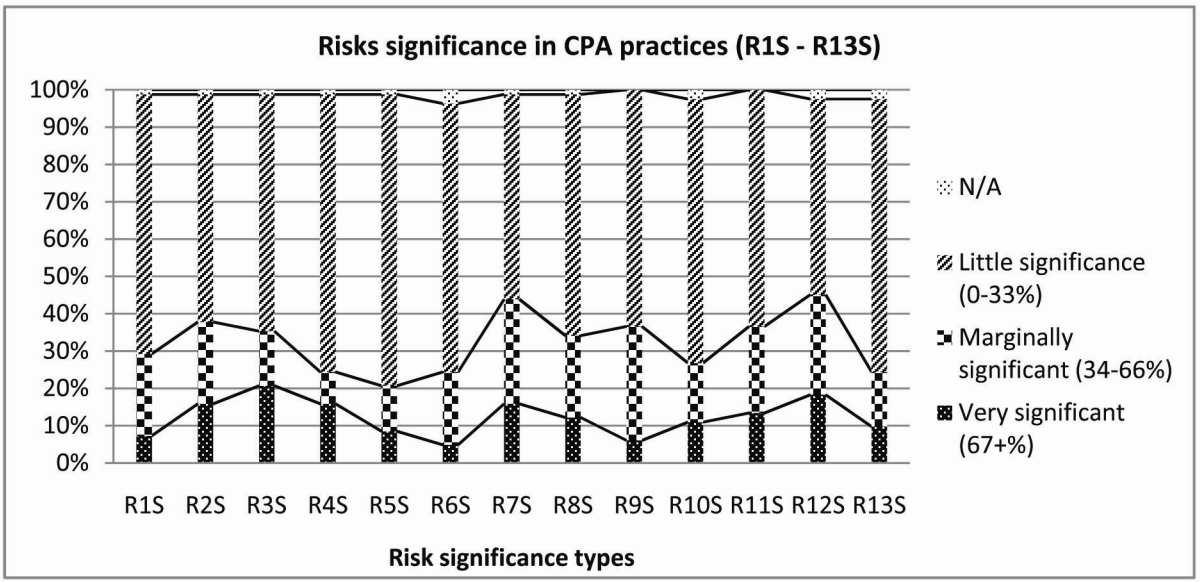

Figure 6. Risks' Significance (R#S) in CPA practices

Legend of risks impact significance:

R1S Human errors resulting in accidental destruction of client's data

R2S Accidental, unintentional disclosure of client's sensitive data

R3S Malicious, deliberate breaches of security of client's sensitive data

R4S Employees' dishonesty theft

R5S Employees unrestricted from changing security settings for the Web

R6S Employees sharing login passwords for shared computer applications

R7S Employees taking home clients' data on a removable storage device

R8S Access to client's data over the Web

R9S Firm's computers being used for personal needs (email, etc.)

R10S Employees installed unauthorized software or hardware on the firm's computers

R11S Disgruntled employee or dissatisfied client damaging firm's computers data

R12S Lack of confidentiality protection of clients' data

R13S Lack of confidentiality protection of employees' data

Figure 6 indicates three greatest risks (the highest significance) arise from: employees taking home clients' data on a removable storage device (R7), accounting firm's legal losses from a lack of confidentiality protection of clients' data (R12), and accidental, unintentional disclosure of client's sensitive data (R2S).

Note that the distribution of likelihood and significance variables (RL and RS) are not similar to each other and that each taken independently might lead to misleading conclusions about security of the practice.

5.2 Average Countermeasures Likelihood and Significance

Nine countermeasures (C1 – C9) were analyzed for both likelihood and significance:

C1 Anti-virus software protection against viruses in the computer clients' files, programs, and e-mail attachments

C2 Protection by insurance and a Disaster Recovery Plan in case of major natural disasters

C3 Protected by insurance and Data Recovery procedures in case of human-caused incidents such as burglary and public disturbances

C4 Protection with regular data backup at least weekly

C5 Protection of clients with a Non-Disclosure Contract and written confirmations of the received confidential client's data

C6 Regular security training for employees

C7 Enforcement of strong passwords that require a combination of upper/lower case, numbers, and special characters

C8 Requirement to change passwords periodically

C9 Placement of a firm's computer system in a secured location

The data for the first six of them (C1 – C6) were collected on the Likert scale and summarized for likelihood and significance (see Figure 7 and Figure 8).

For the remaining three countermeasures (C7 – C9), the data were collected using different scales of measurement and are analyzed separately.

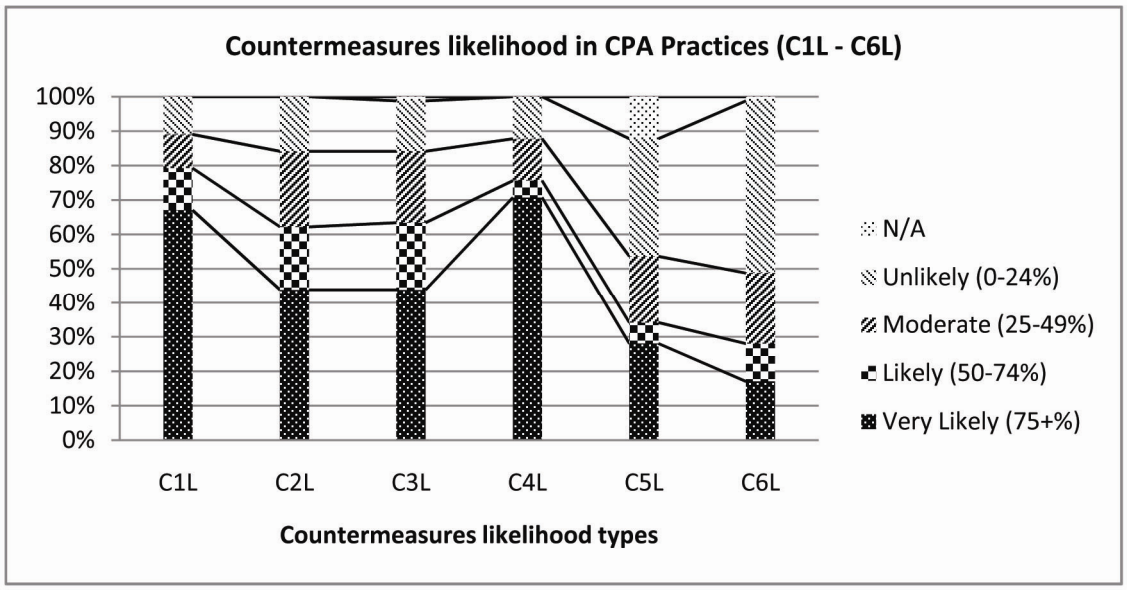

Figure 7. Likelihood of countermeasures use in CPA practices

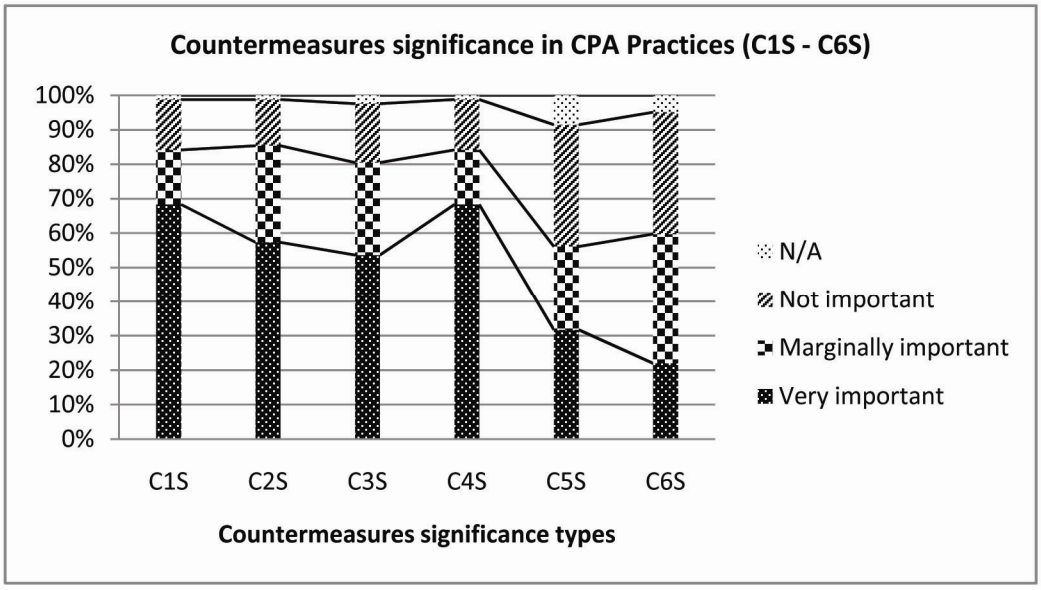

Figure 8. Awareness of countermeasures significance in CPA practices

Note that, as was the case for the risks, the distribution of likelihood and significance of countermeasures (CL and CS) are not similar and that each taken independently might lead to misleading conclusions about security of the practice.

The remaining three countermeasures help to reveal some shortcomings in both implementation of countermeasures and realization of their significance. For example, 40% of practices do not require password change, while significance of that is almost equally distributed between the respondents who view it as very important, marginally important, and unimportant. At least 20% of practices have a server installed in on-site common area, but 55% of the respondents view it as very or marginally important.

5.3 Weighted (Average) Risk Impact Expectancies

Risk impact expectancy from risks plays a fundamental role in cybersecurity risk assessment for CPA practices.

We will define Risk Impact Expectancy (RIE) as a per cent of loss of the business value during the business's life and calculate it as follows:

$$\text{Risk Impact Expectancy} = [\text{Risk Likelihood expectancy}] * [\text{Risk Significance expectancy}] \quad (1)$$

where

[Risk Likelihood expectancy] is the likelihood expectancy of a specified risk (or rate of occurrence).

[Risk Significance expectancy] is the significance of loss (impact) from a specified risk (or exposure factor)

The risk likelihood is measured in four categories and the risk significance is measured in three categories. The percent bracket for each category of the risk likelihood is shown in Figure 5 and the percent bracket for each risk significance category is shown in Figure 6.

To calculate risk expectancies we assign a single value for each bracket group; the average value for a group is appropriate for that purpose. Then, the average values representing likelihood categories will be as follows: very likely - 87%, likely - 62%, moderate - 37%, unlikely - 12%. For example, if risk likelihood is in the "likely" category (which is between 74% and 50%.), then the average for this risk likelihood is 62%.

Similarly, the values representing risk significance categories will be as follows: very significant - 83%, marginally significant - 50%, low significance - 17%.

To calculate average risk expectancy across all categories of likelihood and significance, we need to operate with Weighted (average) Risk Likelihood (WRL) and Weighted (average) Risk Significance (WRS):

$$WRL = \sum (RL_x * Q_x)/4 \quad (2)$$

where RL_x is the average value for the bracket group number X, and Q_x is the number of occurrences in that bracket group,

$$WRS = \sum (RS_x * Q_x)/3 \quad (3)$$

where RS_x is the average value for the bracket group number X, and Q_x is the number of occurrences in that bracket group.

Finally, the Weighted Risk Expectancy (WRE) can be calculated as

$$WRE = WRL * WRS \quad (4)$$

The results are summarized in Figure 9.

The WRE signifies risk impact (loss) expected from a defined risk and its likelihood in a CPA practice.

A high WRE points to higher losses from the risks identified in the survey, and a low WRE signifies a better controlled CPA practices with lower possible losses from the risks identified in the survey.

The WRE is subjective and abstract. It is *subjective* because its indices are based on personal experience and observations of the respondents. It is also *abstract* because it does not take in account the specificities of the risks (like scope, interdependency, others)

Although the WRE is an abstract characteristic, it offers some measure of vulnerability of critical functions of a CPA firm.

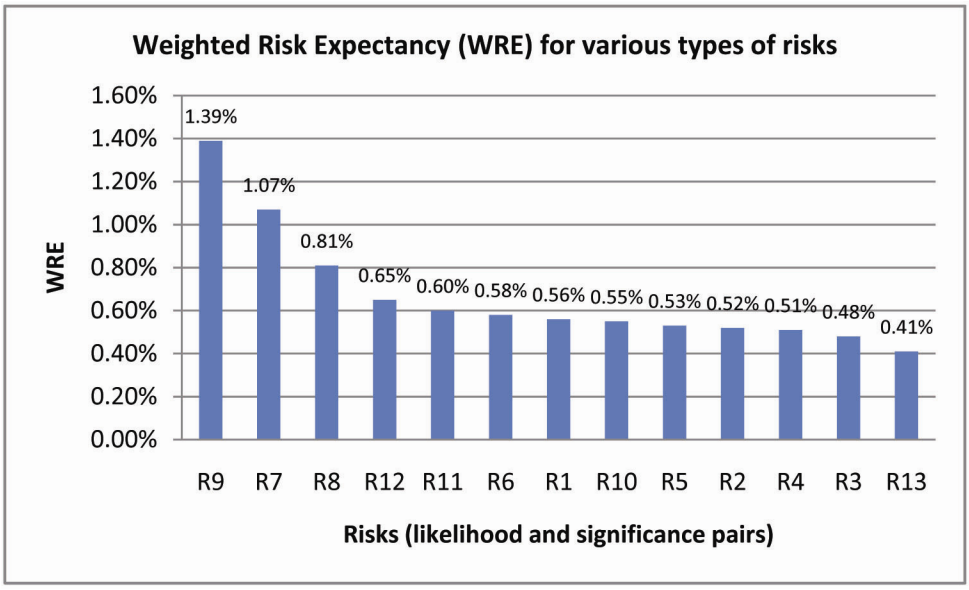

Figure 9. Weighted (average) Risk Expectancy (WRE), sorted and cross-referenced with P2

Figure 9 shows that the five most significant Weighted (average) Risk Expectancies arise from (in order of significance) : the firm's computers being used for personal needs (R9), employees taking home clients' data on a removable storage device (R7), online access to client's data over the Web – now or in the future (R8), firm's legal losses from a lack of confidentiality protection of clients' data (R12), and the risk that a disgruntled employee or dissatisfied client may damage firm's computers data (R11).

5.4 Weighted (Average) Countermeasure Expectancies

We will define the Weighted Countermeasure (protection) Expectancy (WCE) similar to how we defined WRE. Accordingly, the WCE is calculated based on the countermeasure likelihood weighted in four categories and countermeasure significance weighted in three categories. The average values representing four likelihood categories and three significance categories remain the same as for the risk assessment described above:

1. Likelihood categories: very likely - 87%, likely - 62%, moderate - 37%, unlikely - 12%.
2. Significance categories: very significant - 83%, marginally significant - 50%, low significance - 17%.

The Weighted Countermeasure Expectancy (WCE) can be calculated using Weighted (average) Countermeasure Likelihood (WCL) and Weighted (average) Countermeasure Significance (WCS) as follows:

$$WCE = WCL * WCS \quad (5)$$

$$WCL = \sum (CL_x * Q_x)/4 \quad (6)$$

where CL_x is the average value for the bracket group number X, and Q_x is the number of occurrences in that bracket group,

$$WCS = \sum(CS_x * Q_x)/3 \quad (7)$$

where CS_x is the average value for the bracket group number X, and Q_x is the number of occurrences in that bracket group.

The results are summarized in Figure 10.

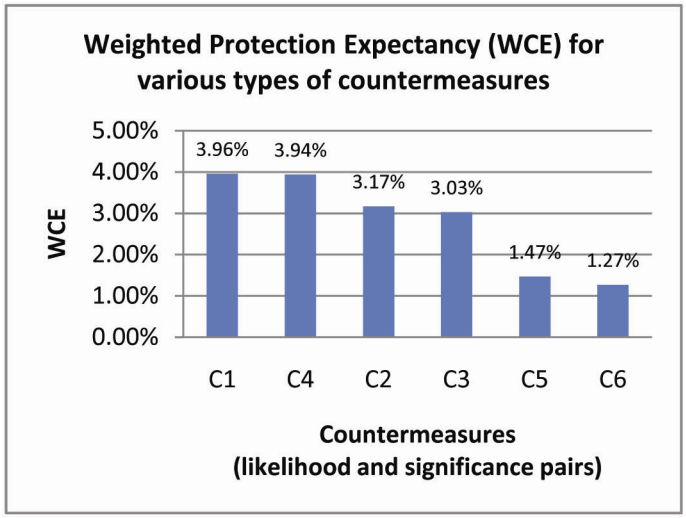

Figure 10. Weighted Countermeasure (protection) Expectancy SCE sorted and cross-referenced with P2

Figure 10 illustrates that the four higher Weighted Countermeasure Expectancies arise from (in order of significance): anti-virus software (C1), data backup (C4), protection by insurance and a Disaster Recovery Plan in cases of major natural disasters (C2) and in cases of human-caused incidents such as burglary and public disturbances (C3).

The WCE indicates protection expected from a defined countermeasure and the degree of its implementation in a CPA practice.

A high WCE points to higher protection from a defined countermeasure (like those identified in our survey), and low WCE signifies less secure CPA practices with lower countermeasure protection.

Just like WRE, the WCE is also subjective and abstract. It is *subjective* because its indices are based on personal experience and observations of the respondents. It is *abstract* because it does not take in account the specificities of the countermeasure (like scope, interdependency, others)

The ultimate goal for both WRE and WCE is to move in opposite directions: to raise WCE (reaching 100% as maximum) and to lower WRE (dropping to 0% as minimum).

5.5 Benchmarking of Risks and Countermeasures

CPA cybersecurity benchmarking is the process of comparing cybersecurity metrics of a CPA practice to the best practices in the industry. This survey does not identify the best cybersecurity practices among CPA firms; the "best" survey form would not be statistically significant.

Therefore, for comparison of cybersecurity of CPA practices, we will identify benchmarking averages for risks and countermeasures. The accuracy of these benchmarks will improve as more surveys of various type risks and countermeasures are performed in the future.

Based on the data shown in Figure 9, the Weighted (average) Risk Expectancy Benchmark (WREB) is 0.67%. Thus, WREB defines the weighted average loss (risk impact) expectancy for all risks analyzed in our survey. Thus, individual WRE for a specific risk that is lower than WREB is assumed to be better than the benchmark.

In practical terms the WREB means, that there is a 0.67% chance that a CPA practice will lose its critical functions and its sustainability will be threatened during its business life span. WRE for any risk type that reaches 100% points to the risk that will certainty occur and will disrupt critical functions of a practice.

Based on the data shown in Figure 10, the Weighted (average) Countermeasure Expectancy Benchmark (WCEB) is 2.81%. The WCEB defines the weighted average protections (countermeasure impact) expectancy for six

countermeasures presented in our survey. Thus, individual WCE for a specific countermeasure that is higher than WCEB is assumed to be better than the benchmark.

In practical terms, the WCEB means, that there is a 2.81% countermeasure protection of critical functions and sustainability of CPA practices during its business life span. WCE for any countermeasure type that reaches 100% indicates that this countermeasure will completely protect the CPA practice from a defined and related vulnerability.

6. Cross-Reference of Risks and Countermeasures with CPA Practice Size

WRE and WCE in Figure 9 and Figure 10 do not reveal differences among various CPA practice types characterized by number of employees (P2). Calculation of expectancies for individual risks and countermeasures provides a more specific picture of threats and protections for a CPA practice.

We will define these individual risk and countermeasure assessments as:

WRE/PT Weighted Risk Expectancy for a Practice Type

WCE/PT Weighted Countermeasure Expectancy for a Practice Type

Examples below illustrate distribution of four selected WRE/TPs for risks and four selected WCE/TP for countermeasures by the CPA Practice size (number of employees).

Four selected risk types are:

R1 accidental human errors in client's data

R7 My firm's employees take home clients' data on a removable storage device

R9 Firm's computers are used for personal needs

R11 Disgruntled employee or a dissatisfied client may damage firm's computers/data

Four selected countermeasure types are:

C1 A firm is well protected by Anti-virus software against viruses in the computer clients' files, programs, and e-mail attachments

C2 A firm is well protected by insurance and a Disaster Recovery Plan in case of major natural disasters

C3 A firm is well protected by insurance and Data Recovery procedures in case of human-caused incidents

C5 A firm protects clients with a Non-Disclosure Contract and written confirmations of the received confidential client's data

7. Weighted Risk Expectancy by CPA Practice Size

7.1 Accidental Data Destruction (R1)

Human errors that are likely or very likely to result in accidental destruction of client's data were reported by 37% of the respondents. The gap between likelihood of this threat in practices and the employee's awareness of potential loss resulting from such destruction is noticeable: on average, only 29% of respondents perceived such potential loss as marginally or very significant.

Distribution of the WRE/TP for the risk R1 (accidental human errors in client's data) by practice size is shown in Figure 11.

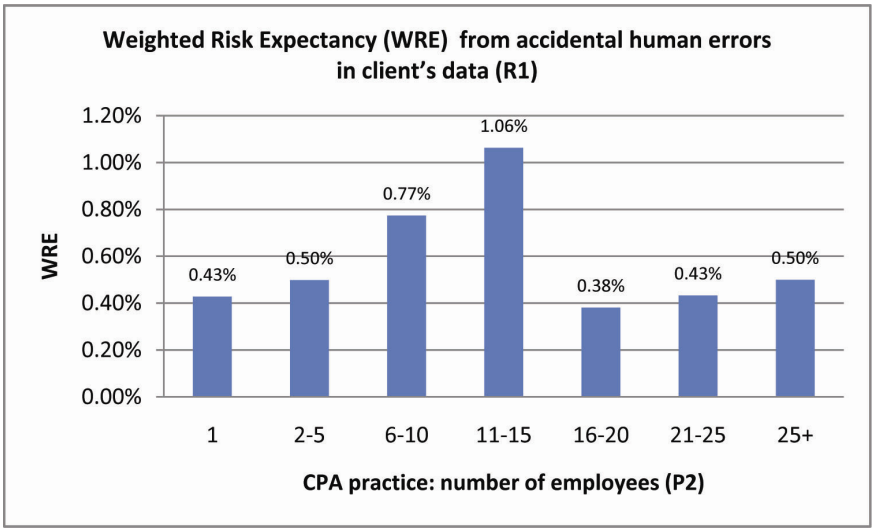

Figure 11. Weighted Risk Expectancy (WRE) from client's data destruction resulted from human errors (R1)

It appears that the mid-size CPA practices (6-15 employees) may experience greater accidental client's data destruction resulting from human errors than other practices.

7.2 Clients' data taken home (R7)

Distribution of the WRE/TP for the risk R7 (employees taking home clients' data on a removable storage device) by practice size is shown in Figure 12.

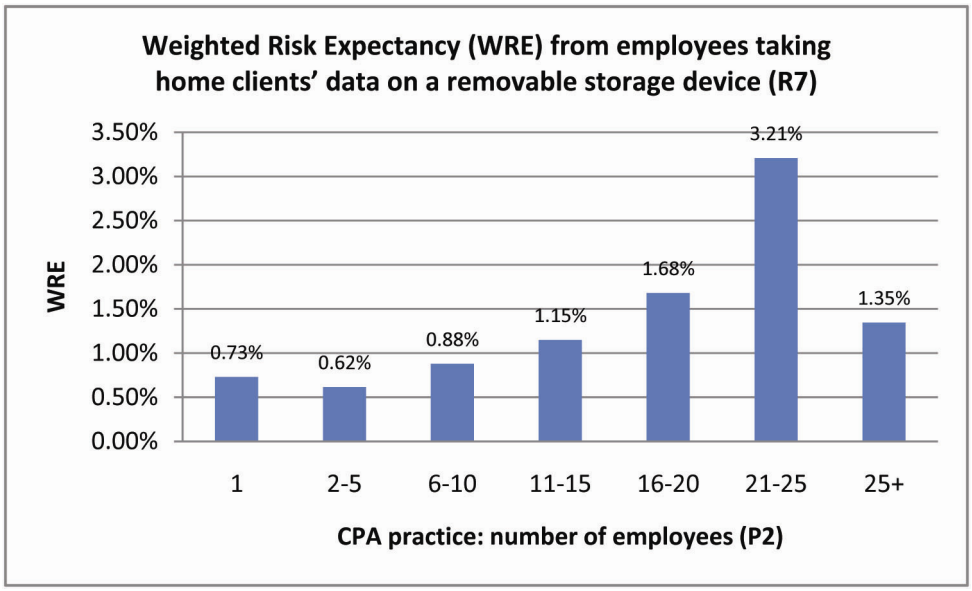

Figure 12. Weighted Risk Expectancy (WRE) from employees taking home clients' data (R7)

The greatest risk of this kind appears for the larger CPA practices (practices with 21-25 employees are on the top).

7.3 Use of firms' computer for personal needs (R9)

Distribution of the WRE/TP for the risk R9 (use of firm's computers for personal needs) by practice size is shown in Figure 13.

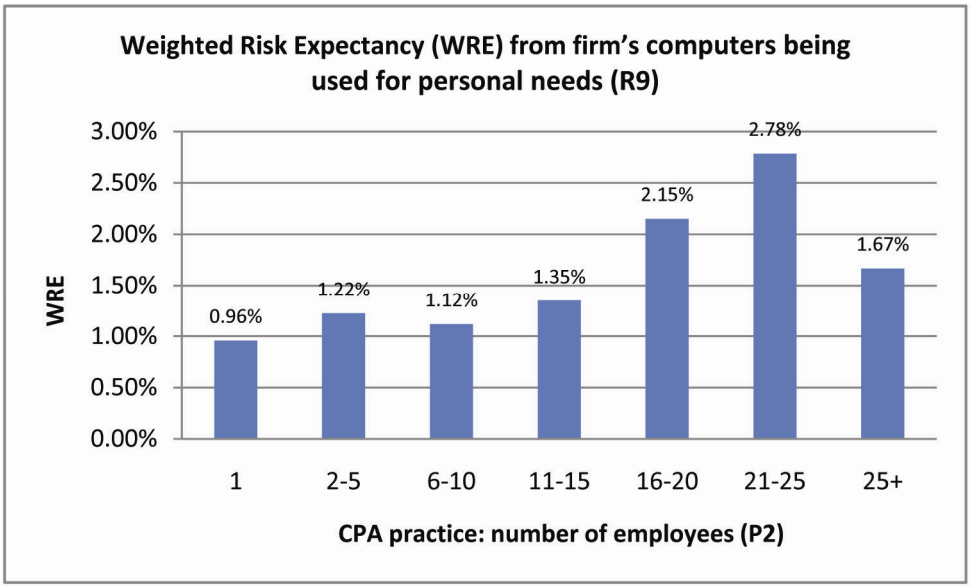

Figure 13. Weighted Risk Expectancy (WRE) from firm's computers being used for personal needs (R9)

As with the previous risk assessment, the greatest risk of this kind (R9) appears for the larger CPA practices (practices with 21-25 employees are the most likely).

7.4 Firm's Computers/Data Damaged by Employees (R11)

Distribution of the WRE/TP for the risk R11 (employees damaging firm's computers) by practice size is shown in Figure 14.

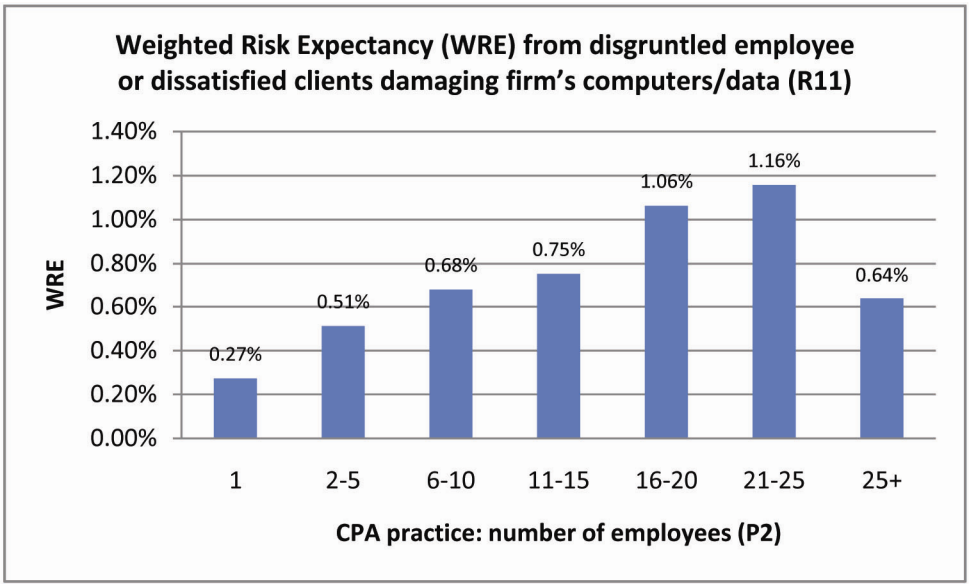

Figure 14. Weighted Risk Expectancy (WRE) from employees damaging firm's computers/data (R11)

Again, the larger CPA practices are subjected to more risk than smaller practices.

8. Weighted Countermeasure Protection Expectancy by CPA Practice Size

8.1 Anti-Virus software

Distribution of the WCE/TP for the countermeasure C1 (use of anti-virus software) by practice size is shown in Figure 15.

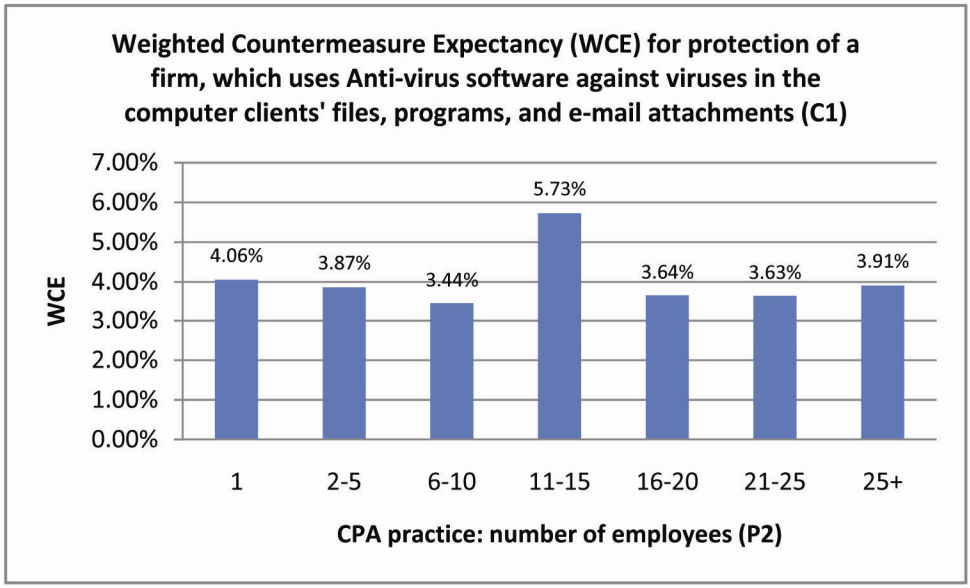

Figure 15. Weighted Countermeasure Expectancy (WCE) from use of anti-virus software (C1)

Except for the group of practices with 11-15 employees, this distribution does not reveal significant differences.

8.2 Insurance and Disaster Recovery Plan for Natural Disasters

Distribution of the WCE/TP for the countermeasure C2 (use of Insurance and Disaster Recovery Plan for Natural Disasters) by practice size is shown in Figure 16.

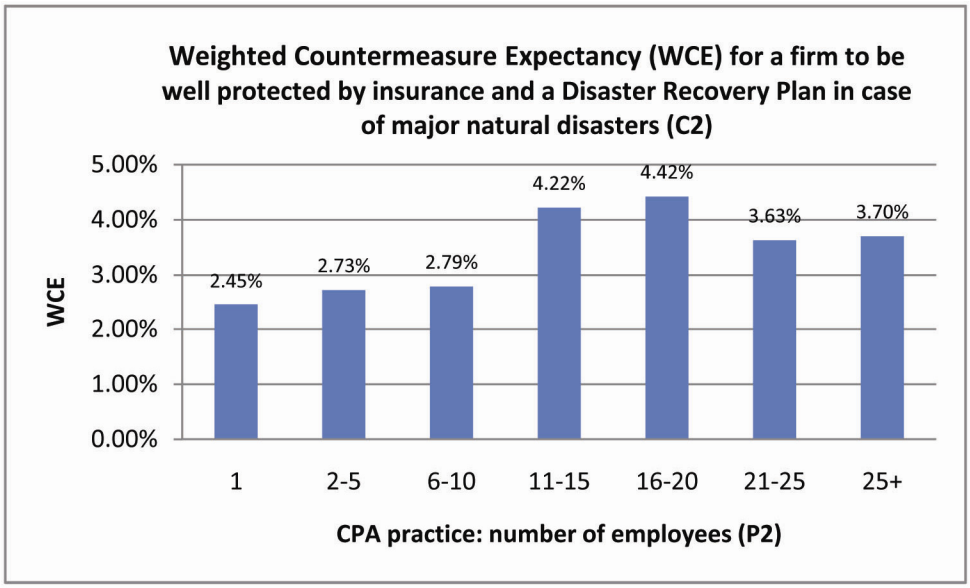

Figure 16. Weighted Countermeasure Expectancy (WCE) for a firm to be well protected by insurance and a Disaster Recovery Plan in case of major natural disasters (C2)

Mid-size and larger CPA practices are using this kind of countermeasure slightly more often and have better awareness of it than smaller practices.

8.3 Insurance and Disaster Recovery Plan for Human-Caused Incidents

Distribution of the WCE/TP for the countermeasure C2 (use of Insurance and Disaster Recovery Plan for Human-Caused Incidents) by practice size is shown in Figure 17.

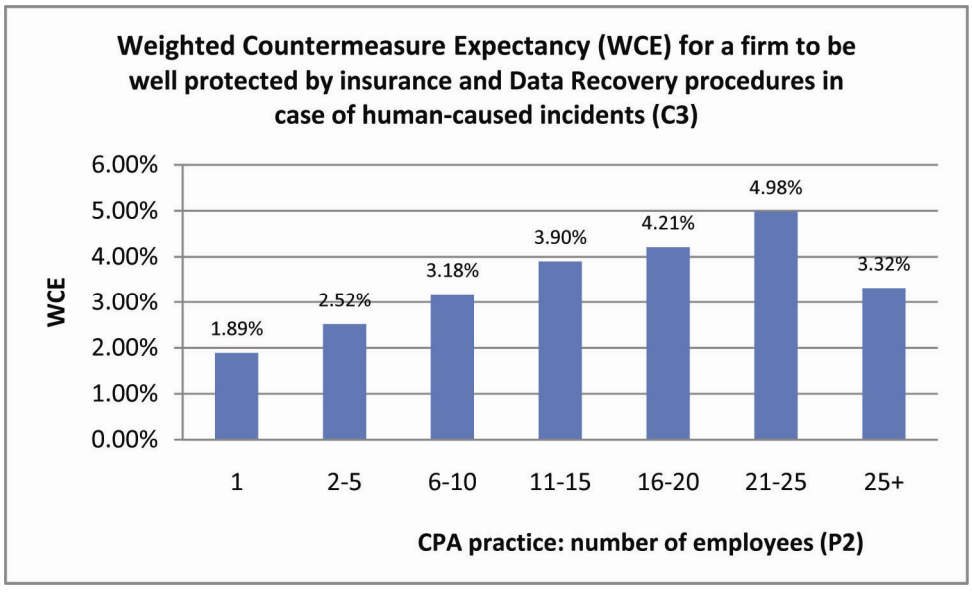

Figure 17. Weighted Countermeasure Expectancy (WCE) for a firm to be well protected by insurance and a Disaster Recovery Plan in case of for Human-Caused Incidents (C3)

Again, the mid-size and larger CPA practices are using insurance and data recovery countermeasures slightly more and have better awareness of it than smaller practices.

8.4 Non-Disclosure Contract for Confidential Client's Data

Distribution of the WCE/TP for the countermeasure C5 (use of non-disclosure contract and written confirmations of the received confidential client's data) by practice size is shown in Figure 18.

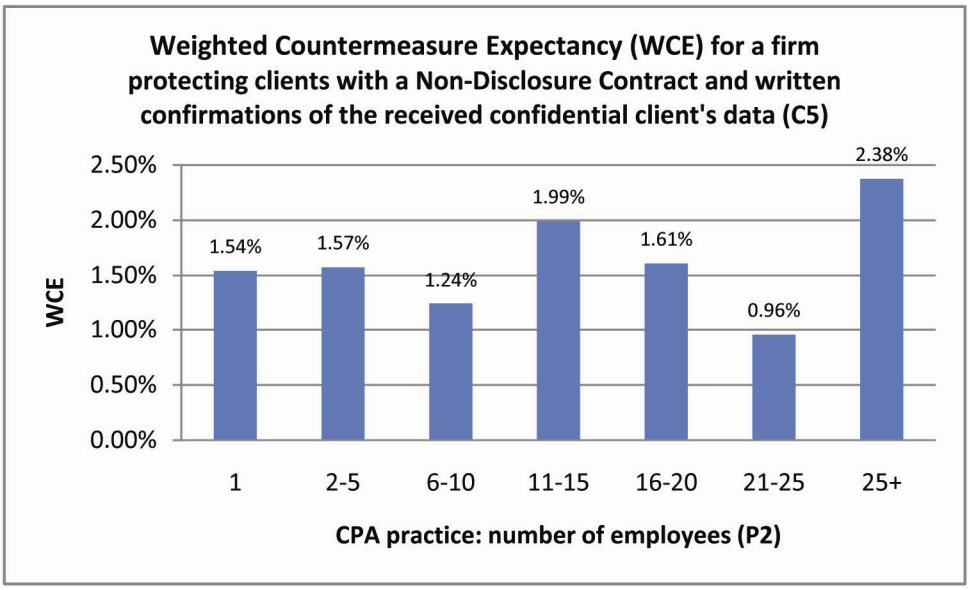

Figure 18. Weighted Countermeasure Expectancy (WCE) for a firm protecting clients with a Non-Disclosure Contract and written confirmations of the received confidential client's data (C5)

The larger practices (25+ employees) employ this countermeasure to a greater extent than other practices.

9. Conclusion

Principles of cybersecurity are applied universally to all areas of business, government and society. They include confidentiality, integrity, availability, and non-repudiation. However, in each of these areas the cybersecurity risks and countermeasures (resulting of awareness of risks) must be context-aware, i.e., considered and assessed in the context of the application areas. Both risks and countermeasures must be assessed in two dimensions - likelihood and significance. The aggregate assessment of a risk or a countermeasure will depend on likelihood and significance, so both risks and countermeasures must be assessed in these two dimensions. Previously, the researchers typically attempted to assess the risks as likelihood and significance and estimate awareness as a degree of knowledge of the risk. (Slusky & Parviz, 2012)

In this article the authors view *building awareness as a countermeasure*, whether it is implemented through technical or organizational means or remains as knowledge at the personal level. Consequently, countermeasures are assessed the same way as risks – through likelihood (of implementation) and significance. Furthermore, the authors attempted to define a benchmark for aggregate assessments of risks and countermeasures that characterize a CPA practice.

The authors constructed the Weighted Risk Expectancy (WRE) index that signifies the risk impact (loss) expected from a defined risk and its likelihood in a CPA practice. Since assessment of a risk's impact and likelihood is often subjective, the WRE index is both subjective and abstract. It is *subjective* because its indices are based on personal experience and observations of the respondents. It is also *abstract* because it does not take in account the specificities of the risks. Despite being an abstract characteristic, the WRE offers some measure of vulnerability of critical functions of a CPA firm.

Similarly, the authors defined the Weighted Countermeasure Expectancy (WCE) index, which signifies protection expected from a defined countermeasure and the degree of its implementation in a CPA practice. Just like the WRE, the WCE is also subjective and abstract. It is *subjective* because its indices are based on personal experience and observations of the respondents. It is *abstract* because it does not take in account the specificities of the countermeasure. It does, however, offer some metric for countermeasure protection for CPA practice security risk.

The risk reduction targets for WRE and WCE are in opposite direction: raising WCE (up to 100% as maximum) and lowering WRE (down to 0% as minimum) both indicate better security.

To compare cybersecurity metrics among CPA practices, the authors proposed the Weighted (average) Risk Expectancy Benchmark (WREB) index and the Weighted (average) Countermeasure Expectancy Benchmark (WCEB) index, both calculated as WRE and WCE averages across all defined risks and countermeasures and across all CPA practice types. WREB and WCER are measured at 0.67% and 2.81% accordingly.

In practical terms the WREB means, that there is a 0.67% chance that a CPA practice will lose its critical functions and its sustainability will be threatened during its business life span; and *the WCEB means that there is a 2.81% countermeasure protection of critical functions and sustainability of CPA practices during its business life span*.

It is important to use both indexes in relative terms for comparison between different practices, not as absolute indexes of cyber assurance.

The research has also showed that there are significant differences in cybersecurity risks and use of countermeasures among different types of CPA practices. For example, the data shows that the mid-size CPA practices (6-15 employees) may experience twice as much accidental client's data destruction resulting from human errors than other practices. Even greater distortion is measurements of risk from employees taking home clients' data and using a CPA firm's computer for personal needs. It appears that CPA practices with 21-25 employees are two to three times more likely than others to have these vulnerabilities.

The defined indexes provide an experimental assessment of risks and vulnerabilities in CPA practices. The authors intend to repeat the surveys with a larger pool of respondents and an updated survey instrument while retaining the methods for weighted risks and countermeasure expectancy defined to identify the trends over a period of time and among various types of CPA practices. The WRE and WCE and their benchmark indexes are experimental; their accuracy can be improved as more practices, more participants, and more risks and countermeasures are surveyed.

Cybersecurity is just one aspect of reliance of CPA practices on Information Technology; which should be among top issues of CPA firms. However, a recent survey (AICPA, 2013) showed that IT, which was in a list of top issues in 2011, dropped from that list in 2013 despite of frequent well-publicized security breaches at financial firms. (DTTL, 2012) That could be an indication of slipping cybersecurity awareness among CPA firms.

The proposed method of cybersecurity survey of CPA practices is intended to provide assessment of status and improvements over a period of time of exposure to risks and countermeasures expectancies vs. benchmark indexes.

References

AICPA. (2011). *2011 Top Technology Initiatives Survey.* [Online] Available: http://www.aicpa.org/interestareas/informationtechnology/resources/toptechnologyinitiatives/pages/2011toptechinitiatives.aspx

AICPA. (2013). *The PCPS CPA Firm 2013 Top Issues Diagnostic Report.* [Online] Available: http://www.aicpa.org/InterestAreas/PrivateCompaniesPracticeSection/StrategyPlanning/FirmStrategyandPlanning/pages/pcps%20top%20issues%20survey.aspxCain, A. (2010). Leading Security Concerns for 2010. *The Internal Auditor*, v. 67 no. 4 (August 2010) p. 16-17. ISSN 0020-5745

Clearswift. (2010). *Security Awareness Report*. November 2010. [Online] Available: http://www.clearswift.com/blog/2010/11/10/security-awareness-research

Cordes, J. (2011). An Overview of the Economics of Cybersecurity and Cybersecurity Policy. Report GW-CSPRI-2011-6. *Cyber Security Policy and Research Institute: Thoughtful Analysis of Cyber Security Issues*. The George Washington University. [Online] Available: http://www.cspri.seas.gwu.edu/uploads/2/1/3/2/21324690/2011-6_economics_and_cybersecurity_cordes.pdf

Dhillon, G., & Moores, S. (2001). Computer Crimes: Theorizing About the Enemy Within. *Computers and Security* (20:8), pp.715-723. ISSN:0167-4048.

DTTL. (2012). *2012 DTTL Global Financial Services Industry Security Study.* [Online] Available: http://www.deloitte.com/view/en_GX/global/industries/financial-services/42a6436f82559310VgnVCM2000001b56f00aRCRD.htm#

Ernst & Young. (2008). *Ernst & Young 2008 Global Information Security Survey.* [Online] Available: http://faisaldanka.wordpress.com/2008/10/20/ernst-young-2008-global-information-security-survey/

Fineberg, Seth. (2010). Too few firms have IT strategy. *Accounting Today*, 10/25/2010, Vol. 24 Issue 14, p1-44, 2p. ISSN 1044-5714.

FTC. (2004). *Federal Trade Commission. 16 C.F.R. Part 314—Standards For Safeguarding Customer Information: Title 16 - Commercial Practices.* OCLC:4989392. [Online] Available: http://law.justia.com/cfr/title16/16-1.0.1.3.38.html

Herrmann, Mimi. (2009). Security Strategy: From Soup to Nuts. *Information Security Journal: A Global Perspective*. Jan2009. Vol. 18 Issue 1, p26-32, 7p. ISSN: 1939-35551939-3547.

IESBA. (2010). International Ethics Standards Board of Accountants (IESBA). Introduction – Objectives, para.100.5, *Handbook of the Code of Ethics for Professional Accountants 2010 Edition*, International Federation of Accountants, New York. ISBN: 9781608150618.

Jackson, R. A. (2008). Top Technology Priorities. *The Internal Auditor*, v. 65 no. 4 (August 2008) p. 38-43. ISSN: 0020-5745.

Puhakainen, P. (2006). *A Design Theory for Information Security Awareness*, Oulu, Finland: University of Oulu. ISBN: 9514281136. [Online] Available: herkules.oulu.fi/isbn9514281144/isbn9514281144.pdf

Ries, David G. (2010). Safeguarding Confidential Data: Your Ethical and Legal Obligations. *Law Practice Journal*. July/August. Volume 36 Number 4. Page 49. ISSN:0959-7689.

SEC Division of Corporation Finance. (2011). *CF Disclosure Guidance: Topic No. 2. Cybersecurity.* October 13, 2011. [Online] Available: http://www.sec.gov/divisions/corpfin/guidance/cfguidance-topic2.htm

Slusky, L. & Partow, P. (2012). Students Information Security Practices and Awareness. *Journal of Information Privacy & Security (JIPS)*. Vol. 8, Issue 4, pp. 3-26. ISSN: 1553-6548.

Stanton, J., Stam, K., Mastrangelo, P., & Jolton, J. (2005). Analysis of End User Security Behaviors. *Computers and Security* (24:2), pp. 124-133. ISSN:0167-4048.

Turner, Richard. (2011). A new focus for IT security. *Computer Fraud & Security*. Feb2011, Vol. 2011 Issue 2, p7-11, 5p. ISSN:1873-7056.

Vroom, C. & von Solms, R. (2004). Towards Information Security Behavioural Compliance. *Computers and Security* (23:3), pp. 191-198. ISSN: 0167-4048.